



10B GESTORA DE RECURSOS LTDA.

MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

OUTUBRO DE 2022



ÍNDICE

1.1.	Sumário	4
1.2.	Aplicabilidade do Manual	5
1.3.	Ambiente Regulatório	5
1.4.	Termo de Recebimento e Compromisso	5
POLÍTICA DE COMPLIANCE		7
1.	INTRODUÇÃO	7
1.1	Responsabilidades e Obrigações	7
1.2	Dúvidas ou ações contrárias aos princípios e normas do Manual	9
1.3	Garantia de Independência	10
1.4	Acompanhamento das Políticas descritas neste Manual	10
1.5	Dever de Reportar	11
1.6	Investigações Sobre Suspeitas de Infração.....	11
1.7	Sanções (“Enforcement”).....	12
2.	POLÍTICA DE CONFIDENCIALIDADE	12
2.1.	Sigilo e Conduta	12
3.	POLÍTICA DE PROTEÇÃO E BOM USO DOS BENS DA EMPRESA	15
3.1.	Proteção dos Bens da 10b.....	15
3.2.	Propriedade Intelectual.....	15
4.	POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES	17
4.1	Objetivo e Definição	17
5	POLÍTICAS DE TREINAMENTO.....	18
5.1	Treinamento e Processo de Reciclagem.....	18
5.2	Implementação e Conteúdo	18
6	POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA.....	19
6.1	Objetivo.....	19
6.2	Identificação de Riscos (risk assessment)	20
6.3	Colaboração.....	21
6.4	Ações de Prevenção e Proteção.....	21
6.5	Monitoramento e Testes	26
6.6	Plano de Identificação e Resposta.....	27

6.7	Arquivamento de Informações	28
6.8	Treinamento	28
6.9	Revisão da Política	28
7	VANTAGENS, BENEFÍCIOS E PRESENTES	28
7.1	Vantagens e Benefícios proibidos	28
7.2	Soft Dollar	29
8	POLÍTICA DE ANTICORRUPÇÃO.....	31
8.1	Introdução	31
8.2	Abrangência das Normas de Anticorrupção.....	31
8.3	Definição	32
8.4	Normas de Conduta.....	33
8.5	Proibição de Doações Eleitorais.....	33
8.6	Relacionamentos com Agentes Públicos.....	33
	POLÍTICA DE CERTIFICAÇÃO	35
1.1.	Introdução	35
1.2.	Atividades Elegíveis e Critérios de Identificação.	35
1.3.	Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA.....	37
1.4.	Rotinas de Verificação	37
1.5.	Processo de Afastamento	39
	VIGÊNCIA E ATUALIZAÇÃO	39
	ANEXO II.....	41
	ANEXO III.....	45
	ANEXO IV.....	46
	ANEXO V	48



INTRODUÇÃO

1.1. Sumário

Este Manual de Regras, Procedimentos e Controles Internos (“Manual”) da **10b Gestora de Recursos Ltda.** (“10b” ou “Gestora”) foi elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, na Resolução da Comissão de Valores Mobiliários (“CVM”) nº 21, de 25 de fevereiro de 2021 (“Resolução CVM 21”), em demais orientações da CVM a respeito, no Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“ANBIMA”) de Administração de Recursos de Terceiros (“Código de ART”), no Código da ANBIMA de Certificação (“Código de Certificação”) e no Código da ANBIMA de Distribuição de Produtos de Investimento (“Código de Distribuição”), e tem por objetivo estabelecer regras, normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança que seja recorrente com a 10b (“Colaboradores”), empresa integrante do Grupo de Gestoras Tarpon, abaixo definido.

O “Grupo de Gestoras Tarpon” é formado pelas seguintes empresas: **(i)** Tarpon Gestora de Recursos Ltda.; **(ii)** TPE Gestora de Recursos Ltda.; **(iii)** 10b; e **(iv)** Niche Partners Gestora de Recursos Ltda.

Na busca incessante da satisfação dos clientes, a 10b atua com total transparência, respeito às leis, normas e aos participantes do mercado financeiro e de capitais.

Assim sendo, este Manual reúne as diretrizes que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando ao atendimento de padrões éticos cada vez mais elevados. Este documento reflete a identidade cultural e os compromissos que a 10b assume nos mercados em que atua.

A 10b e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, etnia, religião, classe social, sexo, deficiência física ou qualquer outra forma de preconceito que possa existir.

A 10b mantém versões atualizadas deste Manual em seu website (<https://10b.com.br>), juntamente com os seguintes documentos: (i) Formulário de Referência, cujo conteúdo deve refletir o Anexo E da Resolução CVM 21; (ii) Política de Gestão de Risco; (iii) Política de Investimentos Pessoais; e (iv) Política de Rateio e Divisão de Ordens entre as Carteiras de Valores Mobiliários.



1.2. Aplicabilidade do Manual

Este Manual aplica-se a todos os Colaboradores que, por meio de suas relações com ou funções na 10b, possam ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

1.3. Ambiente Regulatório

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

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à 10b bem como do completo conteúdo deste Manual. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da 10b foram apontadas no **Anexo III** deste Manual.

1.4. Termo de Recebimento e Compromisso

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

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos neste Manual ou das demais normas aplicáveis às atividades da 10b, deverá ser levado ao conhecimento da Área de Compliance e Risco. Competirá ao Diretor de Compliance (abaixo definido) aplicar as sanções decorrentes de tais desvios, nos termos deste Manual, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar o Diretor de Compliance sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da 10b, bem como zelar pela reputação da empresa. Caso a



violação ou suspeita de violação recaia sobre o próprio Diretor de Compliance, o Colaborador deverá informar diretamente os demais administradores da 10b.



POLÍTICA DE COMPLIANCE

1. INTRODUÇÃO

1.1 Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos, conforme indicado no Formulário de Referência e no Contrato Social da 10b (“Diretor de Compliance”), nos termos da Resolução CVM 21.

São obrigações do Diretor de Compliance:

- (i) Acompanhar as políticas descritas neste Manual;
- (ii) Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade da 10b para apreciação dos administradores da 10b;
- (iii) Atender prontamente todos os Colaboradores;
- (iv) Identificar possíveis condutas contrárias a este Manual;
- (v) Centralizar informações e revisões periódicas dos processos de compliance, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;
- (vi) Assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a CVM e outros organismos congêneres;
- (vii) Encaminhar aos órgãos de administração da 10b, **até o último dia útil do mês de abril de cada ano**, relatório referente ao ano civil imediatamente anterior à data de entrega, contendo: **(a)** as conclusões dos exames efetuados; **(b)** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e **(c)** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das



deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; devendo referido relatório permanecer disponível à CVM na sede da 10b;

- (viii) Appreciar 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;
- (ix) Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
- (x) Aplicar as eventuais sanções aos Colaboradores, conforme definido pelo Comitê de Compliance e Risco; e
- (xi) Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:
 - Investimentos pessoais;
 - Transações financeiras com clientes fora do âmbito da 10b;
 - Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
 - Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
 - Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou
 - Participações da 10b e/ou de seus Colaboradores em alguma atividade política.

Todo e qualquer Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da 10b, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Manual, deverá informar o Diretor de Compliance, para que sejam tomadas as providências cabíveis.



O Diretor de Compliance poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de compliance e o Diretor de Risco para as rotinas de risco, com as atribuições a serem definidas caso a caso, a depender da necessidade da 10b em razão de seu crescimento e de acordo com a senioridade do Colaborador (“Área de Compliance e Risco”).

Ademais, a Gestora possuirá também um Comitê de Compliance e Risco, que será composto pelo Diretor de Compliance, pelo Diretor de Risco, pelo Diretor de Investimentos (abaixo definido) e pelos demais membros da Área de Compliance e Risco, e deverá e averiguar e debater possíveis falhas e oportunidades de aprimoramento nos controles internos da Gestora, entre outros assuntos relacionados à área conforme descrito abaixo, além dos demais assuntos pertinentes à gestão de risco das carteiras, conforme Política de Gestão de Risco da 10b.

São atribuições do Comitê de Compliance e Risco da 10b relacionadas a este Manual:

- Analisar eventuais situações reportadas pelo Diretor de Compliance sobre as atividades e rotinas de compliance;
- Revisar as metodologias e parâmetros de controle existentes; e
- Analisar eventuais casos de infringência das regras descritas neste Manual, nas demais políticas e manuais internos da 10b, das regras contidas na regulamentação em vigor, ou de outros eventos relevantes e definir sobre as sanções a serem aplicadas.

As reuniões do Comitê de Compliance e Risco serão realizadas **trimestralmente**, ou sob demanda, e suas deliberações serão registradas por e-mail.

1.2 Dúvidas ou ações contrárias aos princípios e normas do Manual

Este Manual possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano da 10b, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de compliance e princípios que orientam as ações da 10b.

A Área de Compliance e Risco da 10b está disponível para responder as dúvidas em relação a quaisquer das matérias constantes deste Manual, aconselhar e receber relatos de suspeitas de infração.



Mesmo que haja apenas a suspeita de uma potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses da 10b, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da 10b e reforçar os seus princípios éticos.

Para os fins do presente Manual, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da 10b, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de Compliance, exclusivamente pelo endereço eletrônico compliance@tarpon.com.br. Todos os questionamentos serão, na medida do possível, tratados de forma confidencial.

1.3 Garantia de Independência

Os Colaboradores que desempenharem as atividades de compliance, sob a coordenação do Diretor de Compliance e os Colaboradores que desempenharem as atividades de risco, sob a coordenação do Diretor de Risco, formação a Área de Compliance e Risco, sendo certo que estes exercem suas atividades de forma independente das outras áreas da 10b e poderão exercer seus poderes e autoridade com relação a qualquer Colaborador.

1.4 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 10b, que cheguem ao conhecimento do Diretor de Compliance, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de Compliance utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pelo Diretor de Compliance, caso haja necessidade. Arquivos pessoais salvos em cada computador serão acessados caso o Diretor de Compliance julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela 10b.



Adicionalmente, será realizado um monitoramento **anual**, a cargo do Diretor de Compliance, sobre uma amostragem dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, 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, tal como Política de Investimentos Pessoais e participações da 10b e/ou de seus Colaboradores em atividades políticas.

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

A 10b realizará inspeções com periodicidade **anual**, a cargo do Diretor de Compliance, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da 10b, sendo tal inspeção realizada de forma aleatória. O Diretor de Compliance deverá ainda verificar periodicamente os níveis de controles internos e compliance junto a todas as áreas da 10b, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas da 10b, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções, sendo certo que as correções e os monitoramentos aplicáveis serão feitos pelo Departamento de Tecnologia de Informação e reportadas ao Diretor de Compliance.

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

1.5 Dever de Reportar

Caso um Colaborador tome conhecimento ou suspeite de uma infração de leis ou regulamentos aplicáveis, deste Manual, ou de quaisquer políticas da 10b, tal Colaborador deverá imediatamente reportar tal infração para seu supervisor ou representante da Área de Compliance e Risco. Ninguém estará sujeito à retaliação em virtude de um relato de boa-fé sobre suspeita de infração.

1.6 Investigações Sobre Suspeitas de Infração

Todas as infrações relatadas serão prontamente investigadas e tratadas de forma



confidencial, na medida do possível. É essencial que as pessoas que relatem infrações não conduzam sua própria investigação preliminar. Investigações sobre infrações alegadas poderão envolver questões jurídicas complexas, e agir por conta própria poderá comprometer a integridade da investigação e afetar adversamente tanto você quanto a 10b.

1.7 Sanções (“Enforcement”)

A 10b pretende empregar todas as medidas razoáveis para evitar a ocorrência de condutas em violação a este Manual e interromper tal conduta, caso eventualmente venha a ser observada, o mais breve possível após sua verificação. Pessoas que violarem este Manual ou outras políticas e procedimentos da 10b, inclusive supervisores que deixem de detectar ou reportar uma infração, poderão estar sujeitos a sanções disciplinares, incluindo a extinção de seu vínculo com a 10b.

São exemplos de conduta que poderão resultar na imposição de sanções disciplinares:

- violação, ou solicitação para que terceiro viole, de política prevista neste Manual ou qualquer lei ou regulamento;
- ausência de relato imediato sobre uma infração conhecida ou suspeita de política prevista neste Manual ou qualquer lei ou regulamento;
- ausência de cooperação em investigações de possível infração de política prevista neste Manual ou qualquer lei ou regulamento; e
- retaliação contra pessoa que tenha realizado um relato de boa-fé sobre possível infração de política prevista neste Manual ou qualquer lei ou regulamento.

2. POLÍTICA DE CONFIDENCIALIDADE

2.1. Sigilo e Conduta

As disposições do presente Capítulo se aplicam aos Colaboradores que, por meio de suas funções na 10b, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

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

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da 10b. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo



com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no **Anexo III** deste Manual) e de compliance da 10b.

São consideradas informações confidenciais, reservadas ou privilegiadas (“Informações Confidenciais”), para os fins deste Manual, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a 10b, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da 10b, incluindo:

- a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela 10b;
- c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela 10b;
- d) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- e) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da 10b e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da 10b e que ainda não foi devidamente levado à público;
- f) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
- g) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
- h) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da 10b ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

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

Sem prejuízo da colaboração da 10b com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada ao Diretor de Compliance, para que esta decida sobre a forma mais adequada



para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

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

Insider Trading e “Dicas”

Insider Trading significa o uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores), não sendo, necessariamente, sobre uma operação de compra ou venda na bolsa.

“Dica” é a transmissão, a qualquer terceiro, estranho às atividades da 10b, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running

Front-running significa a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antecipadamente às operações principais, ou seja, se considerarmos literalmente significa sair correndo na frente. Nesse sentido, antes de uma operação de compra ou venda que o Colaborador sabe que vai acontecer, ele se antecipa e executa a ordem.

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a 10b, mas também após o seu término.

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

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



comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance anteriormente mencionada.

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

3. POLÍTICA DE PROTEÇÃO E BOM USO DOS BENS DA EMPRESA

3.1. Proteção dos Bens da 10b

O desvio, o descuido e o desperdício têm um impacto direto na rentabilidade da 10b. Nesse sentido, os Conselheiros, os Diretores e Colaboradores da 10b têm o dever de zelar pelos bens da 10b e assegurar seu uso eficiente. Os bens da 10b deverão ser utilizados somente para fins legítimos.

3.2. Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à 10b, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da 10b, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na 10b, devendo todos os documentos permanecer em poder e sob a custódia da 10b, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da 10b, salvo se autorizado expressamente pela 10b e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à 10b documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à 10b, o Colaborador deverá assinar declaração nos termos do **Anexo IV** ao presente Manual, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações,



atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da 10b, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da 10b, exceto se aprovado expressamente pela 10b.



4. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

4.1 Objetivo e Definição

Atualmente, a 10b desempenha exclusivamente atividades voltadas para a administração de carteiras de valores mobiliários, esta representada pela gestão de fundos de investimento e carteiras administradas, e distribuição de cotas de fundos de investimento que é gestora, nos termos permitidos pela Resolução CVM 21, as quais são exaustivamente reguladas pela CVM.

A atividade de gestão de recursos exige credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de gestão de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas (com exceção da distribuição de cotas de fundos de investimento que é gestora, conforme regulamentação em vigor) pela 10b ou empresas controladoras, controladas, ligadas ou coligadas, bem como prestadores de serviços.

Neste sentido, a 10b, quando necessário, assegurará aos Colaboradores, seus clientes e às autoridades reguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais objetivando a segregação física de instalações entre a 10b e empresas responsáveis por diferentes atividades prestadas no mercado de capitais.



5 POLÍTICAS DE TREINAMENTO

5.1 Treinamento e Processo de Reciclagem

A 10b possui um processo de treinamento inicial de todos os seus Colaboradores, especialmente aqueles que tenham acesso a 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.

Trimestralmente será realizado um processo de treinamento para todos os Colaboradores que tenham sido contratados pela 10b no referido trimestre, a fim de adquirir conhecimento sobre as atividades da 10b e esclarecer dúvidas relacionadas a tais princípios e normas.

Nesse sentido, todos os Colaboradores devem participar do programa de reciclagem anual, à medida que as normas, princípios, conceitos e valores contidos neste Manual sejam atualizados, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

5.2 Implementação e Conteúdo

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da 10b, seus princípios éticos e de conduta, as normas de compliance, as políticas de segregação, quando for o caso, e as demais procedimentos e controles internos previstos neste Manual (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e negociações pessoais), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo III** deste Manual.

Os programas de treinamento devem ser norteados pela clareza, acessibilidade e simplicidade na transmissão de informações. O conteúdo e datas dos programas de treinamento serão definidos pelo Diretor de Compliance.

A Área de Compliance e Risco arquivará os materiais e Termos assinados pelos Colaboradores nos treinamentos realizados no **trimestre** de ingresso do Colaborador e na reciclagem **anual**.

Os Colaboradores que atuarem na distribuição de cotas dos fundos de investimento sob gestão da 10b participarão de um treinamento específico, em que receberão instruções



sobre os materiais comerciais, principais normas aplicáveis e outros temas relacionados à distribuição de cotas, conforme políticas e manuais próprios da 10b ligados ao assunto.

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

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

6 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

6.1 Objetivo

As medidas de segurança da informação têm por finalidade preservar o sigilo, a integridade e a disponibilidade das informações da 10b contra uma série de riscos, como fraude, violação da privacidade e interrupção de serviço e assim minimizar as ameaças aos negócios da 10b e às disposições deste Manual, buscando, principalmente, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da 10b são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

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

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela 10b.

O ora descrito envolve diretamente o Analista de Tecnologia da 10b, e a coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Área de Compliance e Risco, sendo que o Diretor de Compliance será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.



6.2 Identificação de Riscos (risk assessment)

No âmbito de suas atividades, a 10b identificou os seguintes principais riscos internos e externos que precisam de proteção:

- **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria 10b, suas afiliadas, dos Fundos, das companhias investidas, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- **Sistemas:** informações sobre os sistemas utilizados pela 10b e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio da 10b;
- **Governança da Gestão de Risco:** a eficácia da gestão de risco pela 10b quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a 10b identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: *Vírus*, *Cavalo de Troia*, *Spyware* e *Ransomware*);
- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);
- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a 10b avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.



6.3 Colaboração

A segurança da informação exige a participação e o apoio de todos os funcionários da 10b, que receberão orientações suficientes para permitir que eles protejam e administrem adequadamente as informações a que venham a ter acesso no exercício de suas atribuições.

O funcionário que violar qualquer dos controles de segurança da informação estará sujeito às sanções, que pode incluir a rescisão do vínculo empregatício.

6.4 Ações de Prevenção e Proteção

Após a identificação dos riscos, a 10b adota as medidas a seguir descritas para proteger suas informações e sistemas.

- Regra Geral de Conduta:

Os recursos de computação, rede e telecomunicações da 10b são fornecidos para dar apoio às suas atividades comerciais e administrativas. Esses recursos são operados dentro de uma série de sistemas, procedimentos e protocolos de segurança. O uso desses recursos é um privilégio concedido pela 10b e seus usuários devem realizar suas atividades de acordo com as restrições e políticas gerais da 10b.

Todas as atividades realizadas pelos funcionários no âmbito da rede e sistema de telecomunicações da 10b são monitoradas pelo Departamento de Tecnologia de Informação.

O uso impróprio de equipamentos de computação, *software*, equipamentos de telecomunicações, sistemas de rede, recursos e outros equipamentos da 10b incluem, dentre outras hipóteses:

- (a) roubo, danos ou destruição de equipamentos de computação, equipamentos de telecomunicações, programas ou dados;
- (b) instalação, remoção ou outra modificação de qualquer hardware ou software com a finalidade de burlar, evitar ou destruir quaisquer medidas de filtragem, monitoramento ou outras medidas de segurança que o Departamento de Tecnologia da Informação da 10b tenha implementado, bem como o uso ou instalação de qualquer software ou hardware distinto dos padrões disponibilizados



pela 10b, exceto quando for aprovado com antecedência pelo Analista de Tecnologia da Informação;

(c) reprodução ou permissão para reprodução de material de software com direitos autorais em qualquer forma, sem autorização adequada, ou não cumprimento das licenças de software, leis e regulamentações de direitos autorais, sejam elas federais ou estaduais;

(d) inutilização intencional de sistemas de computadores, equipamentos de telecomunicações, redes ou outros recursos (por exemplo, causar “pane” no sistema ou na rede);

(f) uso de sistemas de computador, equipamentos de telecomunicações, redes ou outros recursos, incluindo sistemas de e-mail, para uso comercial fora do âmbito das atividades da 10b; e

(g) uso de sistemas de computadores, equipamentos de telecomunicações, redes ou outros recursos, incluindo sistemas de e-mail, para cometer abusos, difamar, importunar ou ameaçar outro indivíduo ou grupo, cometer fraude ou distribuir outras mensagens ilegais.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da 10b e circulem em ambientes externos à 10b 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 10b. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

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

Neste sentido, os Colaboradores não deverão manter expostos, em qualquer hipótese, em suas respectivas estações de trabalho ou em outro espaço físico da 10b documentos que contenham Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.



Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da 10b.

A 10b mantém um arquivo físico e cada Colaborador é o responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

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

Em consonância com as normas internas acima, a utilização de pen-drivers, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na 10b e que não tenham sido fornecidos pela 10b, deverá ser autorizada pelo Departamento de Tecnologia da Informação.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da 10b.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da 10b.

O Departamento de Tecnologia da Informação e a Área de Compliance e Risco irão monitorar o uso da internet em todos os computadores e dispositivos móveis conectados à rede corporativa. Para todo o tráfego, o sistema de monitoramento deve registrar o endereço IP da fonte, data, hora, protocolo e o site ou servidor de destino.

Além disso, o Gerente de Tecnologia da Informação bloqueará o acesso aos sites *blogs*, *fotologs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida e/ou que forem considerados inapropriados para o ambiente corporativo da 10b. Os protocolos



e categorias de sites da web bloqueados são determinados periodicamente pelo Analista de Tecnologia da Informação em conjunto com a Área de Compliance e Risco.

A Área de Compliance e Risco e a administração da 10b terão acesso a todos os dados e relatórios mantidos pelo Analista de Tecnologia de Informação.

- Acesso Escalonado do Sistema

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

A 10b mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da 10b necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da 10b em caso de violação

- Senha e Login

As senhas são parte essencial da política de segurança de rede da 10b. Assim, todos os funcionários deverão adotar as medidas aqui descritas ao selecionar suas senhas.

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. Todas as senhas no nível de sistema (por exemplo, raiz, habilitação, administrador de servidor, contas de administração de aplicativos e outras) e de usuário (por exemplo, e-mail, Web, computador desktop) devem ser trocadas a cada 90 (noventa) dias, conforme aviso fornecido pelo responsável pela área de informática. Os dispositivos móveis também contarão com proteção por senha.

Todas as senhas no nível de sistema de produção devem fazer parte do serviço de administração de senha global administrado pela 10b. Todos os Colaboradores deverão manter absoluta confidencialidade quanto a suas senhas.

Os funcionários deverão evitar senhas óbvias ou relacionadas à 10b. As senhas de acesso à rede deverão observar os seguintes parâmetros: (i) tamanho mínimo de 8 caracteres; e



(ii) ter três dos seguintes quatro tipos de caracteres: caracteres especiais, letras maiúsculas, números e letras minúsculas.

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

- Uso de Equipamentos e Sistemas

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

A utilização dos ativos e sistemas da 10b, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

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

- Acesso Remoto

A 10b permite o acesso remoto pelos Colaboradores e dará direito aos mesmos acessos verificados no escritório da 10b.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de Compliance qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da 10b e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

- Controle de Acesso

O acesso de pessoas estranhas à 10b a áreas restritas somente é permitido com a autorização expressa de Colaborador autorizado pelos administradores da 10b.



Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a 10b monitora a utilização de tais meios.

- Firewall, Software, Varreduras e Backup

A 10b utiliza um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance é responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

A 10b mantém proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *virus*, *worms*, *spyware*). Serão conduzidas varreduras semanalmente para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da 10b.

A 10b utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance é responsável por patches regulares nos sistemas da 10b.

A 10b mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance. As informações da 10b são atualmente objeto de backup **diário** com o uso de computação na nuvem.

6.5 Monitoramento e Testes

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

- (i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e
- (ii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

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



6.6 Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da 10b (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração da 10b e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, a Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

- Procedimentos de Resposta

Mediante o fornecimento de informações do Departamento de Tecnologia de Informação, o Diretor de Compliance responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da 10b de acordo com os critérios abaixo:

- (i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
- (ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
- (iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
- (iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
- (v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
- (vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais



de fundo de investimento sob gestão da 10b, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

- (vii) Determinação do responsável (ou seja, a 10b ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

6.7 Arquivamento de Informações

De acordo com o disposto neste Manual, os Colaboradores deverão manter arquivada toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 18 da Resolução CVM 21.

6.8 Treinamento

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

6.9 Revisão da Política

O Diretor de Compliance realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética anualmente, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da 10b e acontecimentos regulatórios relevantes.

7 VANTAGENS, BENEFÍCIOS E PRESENTES

7.1 Vantagens e Benefícios proibidos

Os Colaboradores não devem, direta ou indiretamente, nem para si nem para terceiros, solicitar, aceitar ou admitir dinheiro, benefícios, favores, presentes, promessas ou quaisquer outras vantagens que possam influenciar o desempenho de suas funções ou como recompensa por ato ou omissão decorrente de seu trabalho.



Os Colaboradores somente poderão aceitar, presentes, refeições ou outros benefícios, sem prévia autorização do Diretor de Compliance, nos seguintes casos:

- (a) Refeição, que não possua valor suficientemente alto a ponto de influenciar o bom desempenho das funções do Colaborador;
- (b) Material publicitário ou promocional até um valor de USD100 (cem dólares americanos) distribuídos no curso normal dos negócios;
- (c) Qualquer presente ou benefício com valor não superior a USD100 (cem dólares americanos) habitualmente oferecidos na ocasião de um aniversário ou outra ocasião semelhante, que não seja incomum;
- (d) Qualquer presente ou benefício com valor de até USD100; (cem dólares americanos);
- (e) Presente da família ou amigos não ligados com os deveres e responsabilidades profissionais.

Caso o benefício ou presente não se enquadrar nos dispostos acima, o Colaborador somente poderá aceitá-lo mediante prévia autorização do Diretor de Compliance.

7.2 Soft Dollar

Em termos gerais, *Soft Dollar* pode ser definido como sendo o benefício econômico, de natureza não pecuniária, eventualmente concedido à 10b por corretoras de títulos e valores mobiliários ou outros fornecedores (“Fornecedores”), em contraprestação ao direcionamento de transações dos fundos de investimento e carteiras geridos pela 10b, para fins de auxílio no processo de tomada de decisões de investimento em relação aos respectivos fundos e carteiras.

Tais benefícios não devem apresentar caráter pecuniário e devem ser utilizados pelos representantes da 10b exclusivamente em benefício dos clientes, como ferramentas de auxílio da avaliação, seleção e decisão de investimento e suporte à gestão dos fundos de investimento e carteiras de valores mobiliários geridos pela 10b.

A 10b não deverá selecionar seus Fornecedores considerando somente os benefícios recebidos por meio de acordos de *Soft Dollar*, mas deverá levar em consideração, primordialmente, a eficiência, produtividade ou menores custos oferecidos por tais Fornecedores.

A 10b, por meio de seus representantes, deverá observar os seguintes princípios e regras de conduta ao firmar acordos de *Soft Dollar*:



- (i) Colocar os interesses dos clientes acima de seus próprios interesses;
- (ii) Definir de boa-fé se os valores pagos pelos clientes e, conseqüentemente, repassados aos Fornecedores, são razoáveis em relação aos serviços de execução de ordens ou outros benefícios que esteja recebendo;
- (iii) Ter a certeza de que o benefício recebido auxiliará diretamente no processo de tomada de decisões de investimento em relação ao veículo que gerou tal benefício, devendo alocar os custos do serviço recebido de acordo com seu uso, se o benefício apresentar natureza mista;
- (iv) Divulgar amplamente a clientes, potenciais clientes e ao mercado os critérios e políticas adotadas com relação às práticas de *Soft Dollar*, bem como os potenciais conflitos de interesses oriundos da adoção de tais práticas;
- (v) Cumprir com seu dever de lealdade, transparência e fidedignidade com os clientes;
- (vi) Transferir à carteira dos clientes qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de 10b de carteira de valores mobiliários.

Os acordos de *Soft Dollar* devem ser transparentes e mantidos por documento escrito. A 10b deverá manter registros dos benefícios recebidos, identificando, se possível, a capacidade de contribuir diretamente para o processo de tomada de decisões de investimento, visando comprovar o racional que levou a firmar tais acordos de *Soft Dollar*.

Ao contratar os serviços de execução de ordens, a 10b não buscará somente o menor custo, mas o melhor custo-benefício, em linha com os critérios de *best execution* estabelecidos no mercado internacional, devendo ser capaz de justificar e comprovar que os valores pagos aos Fornecedores com que tenha contratado *Soft Dollar* são favoráveis aos fundos de investimento e carteiras sob sua gestão comparativamente a outras corretoras, considerados para tanto não apenas os custos aplicáveis, mas também a qualidade dos serviços oferecidos, que compreendem maior eficiência na execução de transações, condições de segurança, melhores plataformas de negociação, atendimento diferenciado, provimento de serviço de análise de ações e qualidade técnica dos materiais correspondentes, disponibilização de sistemas de informação, entre outros.

Caso o benefício seja considerado de uso misto, os custos deverão ser alocados de forma razoável, de acordo com a utilização correspondente.

Quaisquer benefícios não relacionados ao processo de tomada de decisão de investimentos, tais como pagamento de despesas de escritório, viagens, entretenimento, entre outros, não devem ser objeto de acordos de *Soft Dollar*.



Os acordos de *Soft Dollar* não devem gerar qualquer vínculo de exclusividade ou de obrigação de execução de volume mínimo de transações os Fornecedores, devendo a 10b manter a todo tempo total independência para selecionar e executar com quaisquer Fornecedores operações em nome dos fundos de investimento sob gestão e carteiras sob sua administração, sempre de acordo as melhores condições para seus clientes.

8 POLÍTICA DE ANTICORRUPÇÃO

8.1 Introdução

A 10b está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 11.129/22 (“Normas de Anticorrupção”).

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a 10b e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

8.2 Abrangência das Normas de Anticorrupção

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.

8.3 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.

8.4 Normas de Conduta

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

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.

8.5 Proibição de Doações Eleitorais

A 10b não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, a 10b e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente e notificar o Diretor de Compliance, podendo ter que dar maiores explicações se assim por requerido por esse.

8.6 Relacionamentos com Agentes Públicos



Quando se fizer necessária a realização de reuniões e audiências (“Audiências”) com agentes públicos, sejam elas internas ou externas, a 10b será representada por, ao menos, 2 (dois) Colaboradores, salvo no caso de procurações específicas com poder individualizado que permitem a atuações isolada, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a 10b contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a 10b deverão elaborar relatórios de tais Audiências, e apresentá-los ao Diretor de Compliance imediatamente após sua ocorrência.



POLÍTICA DE CERTIFICAÇÃO

1.1. Introdução

A 10b aderiu e está sujeita às disposições do Código de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

1.2. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da 10b como gestora de recursos de terceiros e distribuidora dos seus próprios fundos, a 10b 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, bem como que a certificação profissional ANBIMA série 20 (“CPA-20”) é a certificação pertinente para os Colaboradores que realizam a distribuição dos fundos de investimento diretamente junto a investidores.

Nesse sentido, apenas o Colaborador com poder para realizar a distribuição dos fundos de investimento diretamente junto a investidores é elegível ao CPA-20, ao passo que somente o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Investimentos, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e CGE, a depender do investimento gerido, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em carteiras administradas, fundos de renda fixa, fundos de ações, fundos multimercado, fundos cambiais e/ou fundos de índice e a CGE é aplicável aos profissionais que atuam em fundos de investimento em participações, fundos de investimento em direitos creditórios não padronizados, fundos de índice, fundos de investimento em direitos creditórios, fundos de investimento em cotas de fundos de investimento em direitos creditórios e/ou fundos de investimento imobiliário.

Em complemento, a 10b destaca que a CGA, a CGE e a CPA-20 são pessoais e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Diretor de Compliance:

- (i) caso o Colaborador esteja exercendo a atividade elegível de CGA ou CGE na 10b e a certificação não esteja vencida, a partir do vínculo do Colaborador com a 10b, o prazo de validade da certificação CGA e CGE será indeterminado, enquanto perdurar o seu vínculo com a 10b e a sua atuação na atividade elegível. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível da CGA ou CGE na 10b, 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; e

- (ii) com relação ao Colaborador certificado pela CPA-20 que se vincular a 10b para exercer atividade elegível, e desde que a sua certificação não esteja vencida na data do vínculo, terá o prazo de vencimento de sua certificação equivalente a 5 (cinco) anos, contados a partir da data da aprovação no exame ou da conclusão do procedimento de atualização, conforme o caso. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CPA-20 na 10b, a validade da certificação será de até 3 (três) anos, contados da data de aprovação no exame ou da conclusão do procedimento de atualização, conforme o caso, ou, ainda, no caso de o Colaborador já ter atuado na atividade elegível anteriormente, o prazo será contado a partir da data de desligamento comunicada à ANBIMA, respeitado o prazo máximo de 5 (cinco) anos.

A 10b irá assegurar que seus 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 de Certificação.

Colaboradores certificados pela CPA-20 e que atuem em atividade elegível de CPA-20 na 10b, deverão, para fins de atualização de sua certificação:

- (i) participar de programa de treinamento oferecido pela ANBIMA com este propósito específico, desde que a conclusão do programa de treinamento e aprovação na avaliação final do curso ocorram até a data de vencimento da certificação, observado os prazos mínimos para realização dos cursos disponíveis no site da ANBIMA na internet; ou
- (ii) participação em programas de treinamento, oferecidos ou validados pela 10b, baseados no programa de atualização divulgado pela ANBIMA com este propósito específico, desde que a conclusão do programa de treinamento ocorra até a data do vencimento da certificação.

A atualização da certificação CPA-20, quando realizada por meio de programas de treinamento oferecidos pela 10b, deve ser informada pela instituição no Banco de Dados da ANBIMA até o último dia do mês subsequente à data da conclusão do treinamento.

Colaboradores certificados pela CPA-20, mas que não atuem em atividade elegível de CPA-20 na 10b, deverão, para fins de atualização de sua certificação, participar de



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

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

Antes da contratação ou admissão de qualquer Colaborador, o Diretor de Compliance 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.

Os Diretores de Investimentos e de Distribuição deverão esclarecer ao Diretor de Compliance se os Colaboradores que integrarão os departamentos técnicos terão ou não alçada/poder discricionário de decisão de investimento ou realizarão a distribuição dos fundos de investimento diretamente junto a investidores, conforme o caso.

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

O Diretor de Compliance também deverá checar se Colaboradores que estejam se desligando da 10b estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à 10b.

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

1.4. Rotinas de Verificação

Mensalmente, o Diretor de Compliance 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 de Certificação.



Ainda, o Diretor de Compliance deverá, mensalmente, contatar os Diretores de Investimentos e Distribuição que deverão informar o Diretor de Compliance se houve algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e distribuição dos fundos, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso, bem como que possam realizar a distribuição dos fundos de investimento diretamente junto a investidores, se for o caso.

Colaboradores que não CPA-20 estão impedidos de realizar a distribuição dos fundos de investimento diretamente junto a investidores, assim como aqueles 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 sem a aprovação prévia do Diretor de Investimentos, tendo em vista que não possuem alçada/poder final de decisão para tanto.

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

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

Por fim, serão objeto do treinamento anual de *compliance* assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da 10b, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos e distribuição de cotas dos fundos sob gestão, reforçando que (a) somente os Colaboradores com CGA e/ou CGE, a depender do caso, podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da 10b, devendo os demais buscar aprovação junto ao Diretor de Investimentos e (b) somente os Colaboradores com CPA-



20 poderão realizar a distribuição dos fundos de investimento diretamente junto a investidores; e (iii) treinamento direcionado aos Colaboradores da Área de Compliance e Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

1.5. Processo de Afastamento

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

Os profissionais já certificados, caso deixem de ser Colaboradores da 10b, deverão assinar a documentação prevista no **Anexo V** a este Manual denominado “Termo de Afastamento”, comprovando o seu afastamento da 10b. O mesmo procedimento de assinatura do Anexo aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

VIGÊNCIA E ATUALIZAÇÃO

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

Histórico das atualizações deste Manual		
Data	Versão	Responsáveis
Maio de 2020	1ª	Diretor de Compliance
Outubro de 2022	2ª e Atual	Diretor de Compliance



ANEXO I
TERMO DE RECEBIMENTO E COMPROMISSO

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

- (i) Ter recebido, na presente data, o Manual de Regras, Procedimentos e Controles Internos (“Manual”) da **10b GESTORA DE RECURSOS LTDA.**, inscrita no CNPJ/ME sob o nº 35.098.686/0001-80 (“SOCIEDADE”);
- (ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual;
- (iii) Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da SOCIEDADE, incorporando-se às demais regras internas adotadas pela SOCIEDADE; e
- (iv) Estar ciente do meu compromisso de comunicar ao Diretor de Compliance da SOCIEDADE qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas no Manual.

[local], [data].

[COLABORADOR]



ANEXO II TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, doravante denominado Colaborador, e **10b GESTORA DE RECURSOS LTDA** inscrita no CNPJ/ME sob o nº 35.098.686/0001-80 (“SOCIEDADE”).

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

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

- a) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela SOCIEDADE;
- c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela SOCIEDADE;
- d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da SOCIEDADE ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da SOCIEDADE e que ainda não foi devidamente levado à público;
- e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
- f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
- g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da SOCIEDADE 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 SOCIEDADE, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à SOCIEDADE, 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 SOCIEDADE, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, “Insider Trading”, “Dicas” e “Front Running”, seja atuando em benefício próprio, da SOCIEDADE ou de terceiros.

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

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a SOCIEDADE, 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.

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

4. O Colaborador reconhece e toma ciência que:

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

avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na SOCIEDADE são e permanecerão sendo propriedade exclusiva da SOCIEDADE 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 SOCIEDADE, devendo todos os documentos permanecer em poder e sob a custódia da SOCIEDADE, salvo se em virtude de interesses da SOCIEDADE for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da SOCIEDADE;

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

(iii) Nos termos da Lei nº 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da SOCIEDADE, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

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

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



5.2. A obrigação de notificar a SOCIEDADE 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 contratual e/ou societária do Colaborador com a SOCIEDADE, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

7. 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 SOCIEDADE.

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

[local], [data].

[COLABORADOR]

10b GESTORA DE RECURSOS LTDA

Testemunhas:

1. _____

Nome:

CPF:

2. _____

Nome:

CPF:



ANEXO III
PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS
ATIVIDADES DA 10b GESTORA DE RECURSOS LTDA

1. Resolução CVM 21.
2. Resolução da CVM nº 30, de 11 de maio de 2021.
3. Resolução da CVM nº 35, de 26 de maio de 2021.
4. Resolução da CVM nº 50, de 31 de agosto de 2021.
5. Instrução da CVM nº 578, de 30 de agosto de 2016, conforme alterada.
6. Instrução da CVM nº 555, de 17 de dezembro de 2014, conforme alterada.
7. Ofício-Circular/CVM/SIN/Nº 05/2014.
8. Código de ART.
9. Código de Certificação.
10. Código de Distribuição.
11. Lei nº 9.613/98, conforme alterada.

Data Base: Outubro/2022¹

¹ **Atenção:** Todo Colaborador deve checar a vigência e eventuais alterações dos normativos contidos neste Anexo previamente à sua utilização.



ANEXO IV

TERMO DE PROPRIEDADE INTELECTUAL

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

(i) que a disponibilização pelo Colaborador à **10b GESTORA DE RECURSOS LTDA.** (“SOCIEDADE”), nesta data, dos documentos contidos no *pen drive* da marca [==], número de série [==] (“Documentos”), bem como sua futura utilização pela SOCIEDADE, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;

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

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

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

[•], [•] de [•] de [•].

[COLABORADOR]



Apêndice
Lista dos Arquivos Gravados nos *Pen Drives*



ANEXO V
TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/ME sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de [gestão de recursos de terceiros/distribuição dos fundos geridos] da **10b GESTORA DE RECURSOS LTDA.** (“SOCIEDADE”) por prazo indeterminado:

até que me certifique pela CGA e CGE;

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;

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

até que me certifique pela CPA-20, no caso das atividades de distribuição dos fundos de investimento diretamente junto a investidores;

tendo em vista que não sou mais Colaborador da SOCIEDADE.]

São Paulo, [•] de [•] de [•].

[COLABORADOR]

10b GESTORA DE RECURSOS LTDA.

Testemunhas:

1. _____

2. _____

Nome:

Nome:

CPF:

CPF: