GESTÃO DE RECURSOS
Rua Dias Ferreira, 175/503, Leblon
CEP: 22431-050, Rio de Janeiro – RJ

CÓDIGO DE ÉTICA, CONDUTA E POLÍTICAS INTERNAS DA RIO PERFORMANCE GESTÃO DE RECURSOS LTDA.

("Sociedade")

Versão vigente: maio/2023

Sumário

Introdução

1.1. O presente Código de Ética, Conduta e Políticas Internas ("Código") da Sociedade estabelece regras e princípios norteadores das condutas dos colaboradores da Sociedade, bem como políticas internas atinentes à Soft Dollar e de Presentes; Anticorrupção; Propriedade Intelectual; Utilização de Bens e Equipamentos; Plano de Continuidade de Negócios; Tratamento de Informações Confidenciais; Proteção de Dados Pessoais, Segurança da Informação e Segurança Cibernética; Tratamento de Conflitos de Interesses e Segregação de Atividades e Funções; Contratos; Reembolso de Despesas; Programa de Treinamento; Responsabilidade Socioambiental; e Seleção, Contratação e Monitoramento de Prestadores de Serviços.

1.2. Para fins deste Código é entendido como colaboradores os (i) sócios, (ii) funcionários, (iii) diretores, (iv) estagiários e (v) quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Sociedade, tenham acesso a informações confidenciais sobre a Sociedade, seus negócios, suas estratégias de investimento ou investidores, ou ainda, aqueles que participem do processo de decisão de investimentos.

1.3. Os princípios aqui definidos deverão ser compulsoriamente observados pelos colaboradores da Sociedade. Para tanto, será coletado Termo de Adesão e Confidencialidade, nos termos do Anexo, através do qual os colaboradores declaram estar cientes de todas as regras, políticas internas e princípios aqui expostos, que lhes foram previamente apresentados pelo responsável pelo Compliance da Sociedade e em relação aos quais não existe qualquer dúvida, comprometendo-se a observá-los a todo tempo no desempenho de suas atividades.

1.4. O Termo de Adesão e Confidencialidade deve ser coletado até o último dia do mês subsequente à contratação de novo colaborador e arquivado na sede da Sociedade em meio físico ou digital.

1.5. O inteiro teor deste Código, bem como dos demais manuais e políticas internas adotadas pela Sociedade, deverá ser apresentado a todo novo colaborador que ingressar na Sociedade, bem como periodicamente, nos termos do Programa de Treinamento abaixo descrito, colocando-se o responsável pelo Compliance à disposição para o esclarecimento de dúvidas.

Princípios Norteadores das Condutas

2.1. Todos os colaboradores da Sociedade devem:

I – desempenhar suas atividades e pautar suas condutas em conformidade com os valores da boa-fé, transparência, diligência, lealdade e veracidade, evitando quaisquer práticas que possam ferir a relação fiduciária mantida com seus clientes/investidores;

II – empregar, no exercício de suas atividades, o cuidado que toda pessoa prudente e diligente costuma dispensar a administração de seus próprios negócios, respondendo por quaisquer infrações ou irregularidades que venham a ser cometidas; e

III - adotar condutas compatíveis com os princípios da idoneidade moral e profissional.

2.2. Todos os esforços em prol da eficiência na gestão dos fundos devem visar à obtenção de melhor retorno aos investidores, com base na análise e interpretação de informações divulgadas ao mercado, e jamais no acesso a informações privilegiadas.

2.3. Os colaboradores da Sociedade devem estar conscientes de que a informação transparente, precisa e oportuna constitui o principal instrumento à disposição do público investidor para que lhes seja assegurado o indispensável tratamento equitativo. As informações prestadas ao investidor não devem, de forma efetiva ou aparente, assegurar a existência de resultados futuros ou a isenção de riscos do investimento.

2.4. O relacionamento dos colaboradores da Sociedade com os participantes do mercado e com os formadores de opinião deve dar-se de modo ético e transparente, evitando a adoção de qualquer prática caracterizadora de concorrência desleal e/ou condições não equitativas.

2.5. A Sociedade transferirá às carteiras sob gestão qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de gestora de carteiras de valores mobiliários, observadas as exceções previstas em norma específica.

2.6. Os colaboradores deverão informar ao Compliance sempre que se verifique, no exercício de suas atribuições, a ocorrência de violação à legislação ou às normas internas de conduta.

2.7. Sem prejuízo do acima estabelecido, os colaboradores deverão atentar-se aos seguintes padrões de conduta no desempenho das suas atividades:

a) não fazer propaganda garantindo níveis de rentabilidade, com base em desempenho histórico da carteira ou de valores mobiliários e índices do mercado de valores mobiliários;

b) não fazer quaisquer promessas quanto a retornos futuros;

c) não negociar títulos e valores mobiliários com a finalidade de gerar receitas de corretagem ou de rebate para si ou para terceiros; e

d) não negligenciar, em qualquer circunstância, a defesa dos direitos e interesses do cliente/investidor.

Atendimento aos Parceiros e Clientes/Investidores

2.8. Todas as informações solicitadas e as consultas efetuadas por parceiros e clientes/investidores devem ser respondidas de forma ágil, completa, objetiva e precisa, observadas eventuais barreiras da informação, a confidencialidade desta, o devido tratamento equitativo entre os investidores e o conceito "*need to know*", pelo qual as informações devem ser repassadas apenas àqueles colaboradores que necessitem da informação para o desenvolvimento das suas respetivas funções.

2.9. Os colaboradores da Sociedade devem atentar para os prazos solicitados e a cordialidade no relacionamento.

Relacionamento com a Imprensa

2.10. Visando o resguardo dos interesses da Sociedade em face ao volume de informações com as quais precisa lidar diariamente, somente os sócios da Sociedade, ou pessoas por estes prévia e expressamente autorizadas, podem manter qualquer tipo de comunicação, em nome da Sociedade, com jornalistas, repórteres ou agentes da imprensa falada ou escrita ("Imprensa").

2.11. Considera-se comunicação, para os fins da vedação estabelecida na cláusula anterior, a revelação à Imprensa de qualquer informação, principalmente as relacionadas a investidores, carteiras sob gestão e operações realizadas ou em desenvolvimento, obtidas no exercício das atividades da Sociedade, bem como de qualquer item sujeito à propriedade intelectual da Sociedade

2.12. Os colaboradores autorizados a participar de entrevistas e assemelhados deverão restringir-se a tecer comentários estritamente técnicos, evitando-se o uso de juízos de valor desnecessários, devendo pautar suas declarações na cautela.

2.13. É vedado, sob qualquer circunstância, conceder declaração à Imprensa que possa aparentar ou ter conteúdo discriminatório em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei, assim como a utilização de expressões de baixo calão ou não condizentes com a melhor educação.

2.14. É vedado, sob qualquer circunstância, conceder declaração à Imprensa que possa aparentar ou possuir orientação político-partidárias são vedadas sob qualquer circunstância.

Políticas Internas

3.1. Em complemento aos princípios norteadores de conduta geral estabelecidos acima, a Sociedade adota uma série de políticas internas com a finalidade de orientar suas atividades e a de seus colaboradores no que compete ao cuidado com as informações aos quais possuem acesso; contato com terceiros, inclusive clientes, dentre outros assuntos.

3.2. O presente Código e suas políticas internas não possuem o objetivo de esgotar todos os controles adotados internamente, tendo em vista que a Sociedade adota outros normativos complementares ao presente Código.

I. Política de *Soft Dollar* e de Presentes

3.1.1 A Sociedade adota uma postura conservadora no tratamento de *Soft Dollar*, somente permitindo a sua aceitação caso não haja influência na independência da tomada de decisão de investimento, escolha de parceiros, tratamento desigual entre os investidores e/ou qualquer tipo de compromisso do colaborador em contrapartida.

3.1.2. É estritamente proibido o recebimento ou o oferecimento de entretenimento, presentes ou benefícios de qualquer valor a/de funcionários públicos, pessoas ou organizações, particulares ou públicas, excetuando-se os casos de pessoas ou entidades que possuam relacionamento comercial com a Sociedade e desde que em valor de até US$ 100 (cem dólares americanos).

3.1.3. Brindes promocionais são permitidos desde que contenham a identificação do fornecedor ou cliente. Em caso de dúvida, o colaborador deve aconselhar-se com o Compliance.

3.1.4. O recebimento de presentes ou quaisquer outros benefícios em valor superior ao estipulado deve ser autorizado pela área de Risco e Compliance.

II. Política Anticorrupção

3.2.1. É terminantemente proibido aos colaboradores, atuando por si ou por meio de terceiros, praticar atos lesivos contra a administração pública, nacional ou estrangeira, 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 na legislação e regulamentação que tratam da responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública ("Normas 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.

3.2.2. É terminantemente proibido ao colaborador agindo em seu nome ou em nome da Sociedade, dar, oferecer, pagar, prometer pagar, ou autorizar o pagamento de, direta ou indiretamente, qualquer dinheiro ou qualquer coisa de valor a qualquer servidor público, autoridade governamental, consultores, representantes, parceiros, ou quaisquer terceiros, com a finalidade de influenciar qualquer ato ou decisão do agente ou do governo, ou para assegurar qualquer vantagem indevida, ou direcionar negócios para, qualquer pessoa, e que violem as regras das Normas Anticorrupção.

3.2.3. O colaborador deverá atentar, ainda, que qualquer valor oferecido a agentes públicos, por menor que seja e independentemente da aceitação pela agente público, poderá ensejar a aplicação das penalidades previstas nas Normas Anticorrupção à Sociedade, hipótese em que o colaborador estará sujeito a indenizar a Sociedade, por meio das medidas legais cabíveis.

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

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

3.2.6. A Sociedade e seus colaboradores devem ainda verificar constantemente se terceiros prestadores de serviços e parceiros comerciais estão sendo processados ou já foram condenados por práticas corruptivas, devendo abster-se de manter relacionamento ou contratar terceiros se houver sérios indícios ou condenação em casos de corrupção ativa ou passiva. Esta previsão se aplica especialmente para contrapartes que tenham sido recomendadas à Sociedade por quaisquer autoridades, servidores públicos, funcionários ou executivos de empresas ou órgãos públicos.

III. Política de Propriedade Intelectual

3.3.1. Todos os documentos, arquivos, modelos, metodologias, fórmulas, cenários, projeções, análises e relatórios produzidos pelos colaboradores da Sociedade,

desenvolvidos na realização das atividades da Sociedade ou a elas relacionadas, têm sua propriedade intelectual atribuída à Sociedade.

3.3.2. Ressalvada autorização expressa e por escrito do Diretor de Risco e Compliance da Sociedade, a exportação, o envio a terceiros, a cópia, descrição, utilização ou adaptação fora do ambiente da Sociedade, em qualquer circunstância, de qualquer item sujeito à propriedade intelectual da Sociedade são vedados, e sujeitos à apuração de responsabilidades nas esferas cível e criminal

3.3.3. Uma vez rompido o vínculo com a Sociedade, o ex-colaborador permanece obrigado a observar as restrições mencionadas acima, estando sujeito à responsabilização pela via judicial.

IV. Política de Utilização de Bens e Equipamentos

3.4.1. O patrimônio da Sociedade deverá ser utilizado exclusivamente para a consecução do seu objeto social, sendo dever de todos os colaboradores a sua preservação e utilização adequada.

3.4.2. Os colaboradores deverão utilizar os telefones fixos e celulares disponibilizados pela Sociedade exclusivamente para assuntos corporativos. Para fins de controle e segurança, todas as ligações poderão ser monitoradas e até mesmo gravadas.

3.4.3. Ligações telefônicas particulares são permitidas, desde que observado o bom-senso, sendo recomendada a ligação para telefones fixos, prioritariamente. A utilização de telefones celulares particulares é permitida, devendo ser mantida ao mínimo necessário.

3.4.4. Os colaboradores deverão utilizar os recursos de acesso à internet e serviço de correio eletrônico (e-mail) apenas para assuntos corporativos, sendo a utilização para fins particulares tratadas como exceção. Para preservar esses recursos, a Sociedade se reserva o direito de controlar e monitorar seus conteúdos e formas de utilização.

3.4.5. O uso da rede para armazenar os arquivos pessoais é permitido, desde que a pasta seja corretamente identificada, ficando o colaborador ciente de que não será assegurada privacidade às informações armazenadas, as quais poderão ser acessadas por quaisquer colaboradores que possuam acesso à rede.

3.4.6. Em nenhuma hipótese os colaboradores poderão utilizar os ativos da Sociedade para discriminação em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e

mental ou de qualquer outra forma não autorizada expressamente em lei. Ademais, é estritamente vedada a utilização destes para:

(i) visitar sites na internet que contenham materiais obscenos, lascivos, preconceituosos ou outro tipo de material repreensível;

(ii) enviar ou receber material obsceno ou difamatório ou cujo objetivo seja aborrecer, assediar ou intimidar terceiros;

(iii) objetivar fins ilícitos; e

(iv) apresentar opiniões pessoais como se fossem da Sociedade.

V. Plano de Continuidade de Negócios

3.5.1. O Plano de Continuidade de Negócios da Sociedade tem como objetivo assegurar a continuidade das operações na eventualidade de uma indisponibilidade prolongada dos recursos essenciais (pessoas, dados, sistemas de informação, equipamentos e instalações).

3.5.2. Este Plano deverá ser de conhecimento de todos os colaboradores, observado o procedimento disposto na Introdução deste Código, sendo que sua implementação será coordenada pelo departamento de Compliance.

Plano de Continuidade Operacional

3.5.3. O Plano de Continuidade Operacional da Sociedade é composto pelas seguintes fases:

a) Identificação das atividades essenciais à consecução da atividade de gestão profissional de recursos de terceiros:

As atividades essenciais ao objeto social da Sociedade são todas aquelas que compõem o processo de análise e seleção de ativos, bem como de tomada de decisão de investimentos e desinvestimentos.

b) Identificação e análise dos riscos em potenciais:

Os incidentes mais comuns que podem resultar em descontinuidade operacional são incêndios, enchentes, quedas de energia, roubos, greves, ataques de *hackers*, vírus de computador, sabotagem e erros humanos, bloqueios ou impossibilidade de acesso ao

edifício, falha grave no link de internet e sua redundância, hardware ou software, bem como questões relacionadas à saúde pública.

c) Identificação da interrupção do funcionamento dos recursos:

Uma situação de emergência é configurada sempre que houver uma descontinuidade operacional, assim entendida como o impedimento à execução de qualquer atividade essencial da Sociedade, ou processo do qual dependa uma atividade essencial.

Uma vez identificada a interrupção de quaisquer dos recursos essenciais, o Diretor de Risco, Compliance e PLD/FTP deve ser imediatamente comunicado e ativará o Plano de Continuidade de Negócios, orientando os colaboradores sobre a postura e providências cabíveis, de acordo com a natureza e gravidade da contingência.

Todos os colaboradores devem possuir os contatos telefônicos e e-mail do responsável pelo Compliance, de modo a possibilitar a comunicação da contingência ocorrida.

Para que seja caracterizada uma situação de emergência, o impedimento à execução da atividade essencial deve ser por tempo prolongado ou indeterminado. Considera-se tempo prolongado sempre que o tempo transcorrido desde a interrupção da atividade alcance 3 horas, a expectativa de tempo até a solução da interrupção for superior a 3 horas, quando o tempo remanescente para a conclusão da atividade for insuficiente para sua execução no mesmo dia ou se a não execução imediata da atividade puder provocar prejuízo para os fundos sob gestão.

d) Comunicação aos colaboradores

Compete ao Diretor de Risco, Compliance e PLD/FTP, ou colaborador por ele designado, a comunicação da contingência aos demais colaboradores, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e gravidade da contingência, sendo responsável pela implementação da ativação e operacionalização do Plano abaixo apresentado no prazo máximo de 2 horas da identificação da interrupção do funcionamento normal dos recursos, conforme item acima.

e) Ativação do Plano e acesso às informações para continuidade das operações críticas:

A ativação do Plano de Continuidade consiste no acesso pelos colaboradores aos dados e informações necessárias ao desempenho das respectivas atividades através de

local diverso da sede social, podendo tal acesso ser realizado remotamente pela internet.
Todos os sistemas e veículos de informação contratados para auxiliar no processo de análise e gestão das carteiras são passíveis de serem acessados de qualquer localidade, bastando apenas a conexão com a rede mundial de computadores. Estes sistemas possuem mecanismos próprios de redundância e segurança.

A continuidade das atividades essenciais é garantida mediante o arquivamento das informações relacionadas a estes processos em ambiente seguro, com acesso restrito aos integrantes da equipe da Sociedade, e objeto de backup diário em tempo real em nuvem mantida por plataforma profissional, possibilitando o acesso às citadas informações de qualquer outro computador através da senha de acesso, bem como a redundância de armazenamento para salvaguarda em caso de eventual sinistro.

f) Testes Periódicos:

Anualmente, são realizados testes de ativação do referido Plano pelo Diretor de Compliance. Nesta oportunidade, o responsável deverá trabalhar ao menos por um dia com os laptops destinados para esse fim.

Plano de Recuperação

3.5.4. Este Plano tem o propósito de definir um guia de recuperação e restauração das funcionalidades afetadas que suportam o processo de tomada de decisões de investimentos e desinvestimentos, bem como as atividades de gestão de riscos e Compliance, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível.

3.5.5. Assim, cabe ao Compliance desenvolver relatórios acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tal relatório deverá ser submetido à Diretoria da Sociedade para que sejam promovidas as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

3.5.6. Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a Sociedade estudará procedimentos preventivos a serem implementados e incluídos neste Plano de Continuidade de Negócios.

VI. Política de Tratamento das Informações Confidenciais

3.6.1. Consideram-se informações de natureza confidencial todas as informações às quais os colaboradores venham a ter acesso em decorrência do desempenho de suas funções na

Sociedade, inclusive por meio dos sistemas e arquivos disponibilizados pela Sociedade para tanto, que não sejam notória e comprovadamente de domínio público.

3.6.2. São consideradas confidenciais ainda as informações reservadas ou privilegiadas de que trata o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, devendo ser observados para estas os mesmos princípios de conduta e controle definidos neste Código.

3.6.3. Portanto, todos os colaboradores da Sociedade, conforme definido no item 1.1. deste Código, podem, eventualmente, ter acesso a informações de cunho confidencial ou privilegiado, devendo observar as diretrizes definidas pela Sociedade, neste Código e demais manuais e políticas internas, a fim de garantir o adequado tratamento destas informações e evitar o seu acesso por terceiros não autorizados.

3.6.4. Os colaboradores da Sociedade deverão:

a) abster-se de utilizar informação privilegiada para obter, em benefício próprio ou de outrem, vantagem mediante negociação de títulos e/ou valores mobiliários;

b) abster-se de recomendar ou de qualquer forma sugerir que qualquer pessoa compre, venda ou retenha títulos e/ou valores mobiliários se a informação a que tenha acesso privilegiado puder, em tese, influenciar a tomada de qualquer uma dessas decisões;

c) advertir, de forma clara, àqueles em relação a quem se verificar a necessidade de revelar informação privilegiada, sobre a responsabilidade pelo cumprimento do dever de sigilo e pela proibição legal de que se utilizem de tal informação para obter, em benefício próprio ou alheio, vantagem mediante negociação com tais títulos e/ou valores mobiliários;

d) guardar sigilo sobre qualquer informação a que tenham acesso e que ainda não tenha sido divulgada ao público em geral, ressalvada a revelação da informação quando necessária para a Sociedade conduzir seus negócios de maneira eficaz e, ainda, somente se não houver motivos ou indícios para presumir que o receptor da informação a utilizará erroneamente.

3.6.5. Os colaboradores da Sociedade deverão guardar absoluto sigilo sobre toda e qualquer informação de natureza confidencial a que tenham acesso ou conhecimento no desempenho de suas funções, inclusive por meio dos sistemas e arquivos disponibilizados pela Sociedade para tanto. Tal determinação se aplica igualmente às informações obtidas/repassadas verbal ou informalmente, assim como às escritas ou impressas.

3.6.6. O fornecimento de informações confidenciais a pessoas externas à Sociedade será realizado somente nos casos estritamente necessários a fim de cumprir as normas atinentes à atividade desenvolvida pela Sociedade, proteção contra fraudes ou qualquer outra atividade ilegal suspeita, mediante contratos de confidencialidade, quando for o caso.

3.6.7. Os colaboradores comprometem-se à manutenção da confidencialidade das informações que tenha acesso mediante a assinatura do Termo de Adesão e Confidencialidade. Já os terceiros contratados que tiverem acesso a informações confidenciais deverão assinar Termo de Confidencialidade específico, caso o próprio Contrato de Prestação de Serviço não possua cláusula para este fim.

3.6.8. Sob nenhuma circunstância os colaboradores da Sociedade poderão utilizar informações confidenciais para obter vantagens pessoais, tampouco poderão fornecê-las para terceiros, inclusive familiares, parentes e amigos, ou mesmo a outros colaboradores da Sociedade que não necessitem de tais informações para executar suas tarefas.

3.6.9. Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o colaborador deve, previamente à sua divulgação, procurar o responsável pelo Compliance para obter orientação adequada, o qual deverá atribuir interpretação extensiva ao conceito de informação confidencial definido acima.

3.6.10. A revelação dessas informações a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada ao diretor responsável pela atividade de gestão desenvolvida pela Sociedade para que este decida, em conjunto com o Diretor de Risco e Compliance, sobre a forma mais adequada para tal revelação.

VII. Política de Proteção de Dados Pessoais, Segurança da Informação e Segurança Cibernética

Proteção de Dados Pessoais

3.7.1. A Sociedade zela pela observância, implementação e cumprimento de regras, políticas e procedimentos relacionados à Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais. Sem prejuízo das diretrizes contidas neste Código e com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, a Sociedade adota regras e procedimentos para a coleta e tratamento de dados pessoais e, eventualmente, dados sensíveis, inclusive nos meios digitais, em linha com a Lei Geral de

Proteção de Dados e com a Política de Privacidade e de Tratamento de Dados adotada internamente e segregada deste Código.

3.7.2. Para os fins dispostos neste Código e na Política de Privacidade e de Tratamento de Dados adotados, consideram-se:

(i) "**Dados Pessoais**" qualquer informação relacionada a pessoa natural identificada ou identificável. Deste modo, sujeitam-se à tutela deste Código e da Política de Privacidade todos os Dados Pessoais de colaboradores, investidores, parceiros, prestadores de serviço ou quaisquer terceiros com os quais a Sociedade mantenha relacionamento de qualquer natureza.

São considerados, ainda, Dados Pessoais aqueles utilizados para formação de perfil comportamental de determinada pessoa natural, se identificada.

(ii) "**Dados Pessoais Sensíveis**" os Dados Pessoais que versem sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.

3.7.3. Todos os Dados Pessoais ou Dados Pessoais Sensíveis são informações confidenciais e devem ser tratados como tal para os fins desta Política e demais manuais e políticas internas adotadas pela Sociedade.

3.7.4. As atividades de tratamento de Dados Pessoais e Dados Pessoais Sensíveis deverão observar a boa-fé e os seguintes princípios:

(i) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(ii) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

(iii) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

(iv) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;

(v) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vi) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(vii) segurança: utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

(viii) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;

(ix) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

(x) responsabilização e prestação de contas: demonstração, pela Sociedade, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

3.7.5. As formas de coleta, tratamento e processamento de Dados Pessoais e Dados Pessoais Sensíveis encontram-se regulamentadas no Capítulo IV da Política de Privacidade e de Tratamento de Dados adotada pela Sociedade.

3.7.6. A Sociedade manterá registro das operações de tratamento de Dados Pessoais e Dados Pessoais Sensíveis que realizar, especialmente quando baseado no seu legítimo interesse.

3.7.7. A Autoridade Nacional de Proteção de Dados poderá determinar que a Sociedade elabore um relatório de impacto à proteção de Dados Pessoais, inclusive Dados Pessoais Sensíveis, referente às operações de tratamento de dados. Este relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise da Sociedade sobre estas medidas, salvaguardas e mecanismos de mitigação de risco adotados.

3.7.8. O encarregado pelo tratamento de Dados Pessoais e Dados Pessoais Sensíveis será o Diretor de Compliance da Sociedade. As informações para contato do encarregado estarão

disponíveis no site da Sociedade e na Política de Privacidade e de Tratamento de Dados adotada internamente nos itens 3.3. 3.4.

Procedimentos de Segurança da Informação

a. Acesso Restrito

3.7.9. 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 deve ser acionada previamente à revelação.

3.7.10. Os colaboradores da Sociedade que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos mesmos, devendo salvaguardar as senhas e outros meios de acesso.

3.7.11. O acesso controlado aos computadores da Sociedade e às pastas e arquivos se dá mediante outorga de senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

3.7.12. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores utilizados pela Sociedade permitem a identificação do seu remetente/receptor.

3.7.13. O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se àqueles fornecidos pela Sociedade.

3.7.14. A outorga e cancelamento de senha é de responsabilidade do TI sempre mediante orientação do Diretor de Compliance, a quem compete a verificação da estrutura de governança da Sociedade, a fim de evitar a transgressão de barreiras de informação e potenciais conflitos de interesse. Este procedimento deverá ser observado ainda na hipótese de mudança de atividade/área de um determinado profissional dentro da Sociedade.

3.7.15. As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança, devendo ser desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

3.7.16. Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Sociedade expiram, usando um protetor de tela protegido por senha que exige que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticado novamente.

3.7.17. No caso do desligamento ou saída de algum colaborador, o acesso aos arquivos será automaticamente bloqueado e a respectiva senha revogada. Para sistemas externos, a Sociedade deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

3.7.18. O controle de acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros da Sociedade, não sendo o espaço físico compartilhado com outras empresas ou atividades.

b. Backup

3.7.19. Todos os documentos arquivados nos computadores da Sociedade são objeto de *back-up* diário na nuvem com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

c. Cópia de Arquivos e Instalações

3.7.21. Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de TI. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

3.7.22. A cópia de arquivos e instalação de programas em computadores da Sociedade deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

3.7.23. É terminantemente proibido que os colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

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

interno da Sociedade. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copiadoras.

d. Descarte de Informações

3.7.25. O descarte de informações confidenciais deve observar as seguintes diretrizes:

(i) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;

(ii) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;

(iii) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada; e

(iv) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Sociedade devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

e. Redundância

3.7.26. Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe poderá acessar as informações na nuvem de qualquer local.

3.7.27. Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a um equipamento do tipo no-break, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvem seus arquivos. A manutenção do mesmo é feita anualmente pela empresa terceirizada de TI.

f. Suporte e Monitoramento

3.7.28. Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à área de TI, que assegurará o suporte interno ou providenciará que seja acionado o suporte externo necessário.

3.7.29. O sistema eletrônico utilizado pela Sociedade está sujeito à revisão, monitoramento e gravação a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

3.7.30. Nesse sentido, 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 Sociedade também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos colaboradores.

3.7.31. Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

g. Tratamento de casos de vazamento de informações confidenciais

3.7.32. No caso de vazamento de informações confidenciais relacionadas a investidores, ou de qualquer outro Dado Pessoal ou Dado Pessoal Sensível tratado pela Sociedade, ainda que oriundo de ação involuntária, o Diretor de Compliance notificará os interessados sobre o ocorrido. Em se tratando de Dado Pessoal ou Dado Pessoal Sensível, a Autoridade Nacional de Proteção de Dados também deverá ser comunicada, além do titular do dado. Esta comunicação observará os parâmetros exigidos pela Lei Geral de Proteção de Dados.

3.7.33. Sem prejuízo, a Sociedade acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e responsabilização do causador. Ademais, será elaborado um Relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

3.7.34. Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

h. Firewall

3.7.35. A Sociedade faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas.

i. Rede Wireless

3.7.36. A Sociedade possuí 2 (duas) redes WIFI distintas, uma para uso interno e outra para uso dos visitantes. Jamais deve ser divulgada a senha de acesso interno para os visitantes. Os visitantes devem sempre solicitar a senha de acesso para a recepcionista. Nesse sentido, a rede WIFI para visitantes é bloqueada para acessar recursos internos.

j. Testes de Segurança

3.7.37. São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real
Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Monitoramento de Hosts e serviços	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 30 min
Backup Online	Tempo real
Backup Firewall	A cada alteração
Verificar status dos logs do Backup	Semanal
Documentação em geral	A cada mudança
Verificar sistema gráficos de consumo de link, visão diária, semanal e mensal	Semanal
Troca da senha dos usuários	Semestral

<u>Procedimentos de Segurança Cibernética</u>

3.7.38. O objetivo das regras sobre segurança cibernética da Sociedade é assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus colaboradores a respeito.

3.7.39. Os processos de segurança de dados e da informação da Sociedade devem assegurar:

(i) a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);

(ii) a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e

(iii) a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Sociedade, observadas as regras de sigilo e confidencialidade.

Responsabilidade

3.7.40. A equipe de TI, em conjunto com o Diretor de Risco e Compliance, é a principal responsável dentro da Sociedade para tratar e responder questões de segurança cibernética ("Responsável pela Segurança Cibernética"), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

3.7.41. São deveres e responsabilidades do Responsável pela Segurança Cibernética:

(i) Testar a eficácia dos controles utilizados e informar à Diretoria os riscos residuais;

(ii) Acordar com a Diretoria o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes;

(iii) Configurar os equipamentos e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

(iv) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

(v) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Sociedade em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros;

(vi) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Sociedade, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Sociedade; e

(vii) Promover a conscientização dos colaboradores em relação à relevância da segurança a informação para o negócio da Sociedade, mediante treinamentos.

3.7.42. Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer colaborador que perceba ou desconfie de tal incidente deverá imediatamente informar o Responsável por Segurança Cibernética que comunicará ao Diretor de Risco e Compliance para que sejam tomadas as devidas providências.

Identificação e Avaliação de Riscos

3.7.43. A Sociedade, a cada 24 (vinte e quatro) meses, deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção, além de revisar o processo de cibersegurança. Esse processo será conduzido pelo Responsável pela Segurança Cibernética e documentado pela área de Compliance, com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Sociedade. A Sociedade poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança Cibernética julgue necessário e mediante aprovação da Diretoria.

3.7.44. Após a condução do referido processo, a Diretoria deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Sociedade, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

3.7.45. A identificação e avaliação de riscos cibernéticos visa evitar a ocorrência de incidentes relevantes de segurança cibernética que afete os processos críticos do negócio da Sociedade, ou dados e informações sensíveis, e que tenham impacto significativo sobre suas atividades.

3.7.46. Diante da possibilidade de invasores utilizarem (i) Malware, (ii) Engenharia social; (iii) Pharming; (iv) Phishing; (v) Vishing; (vi) Smishing; (vii) Acesso pessoal; (viii) Ataques de DDos (distributed denial of services) e botnets; e (ix) Invasões (advanced persistent threats), a Sociedade adota ações de prevenção e proteção descritos a seguir.

Ações de Proteção e Prevenção aos Riscos Cibernéticos

3.7.47. A Sociedade estabeleceu um conjunto de medidas buscando mitigar os riscos identificados que visa impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo.

3.7.48. Os planos de ação e prevenção descritos neste tópico têm por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

3.7.49. Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede.

3.7.50. Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Diretor de Compliance reportados imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

3.7.51. São adotadas as seguintes medidas preventivas para cada risco identificado:

Risco Interno	**Ação de Proteção/Prevenção**
Indisponibilidade dos arquivos na rede	Redundância para assegurar a disponibilidade dos sistemas.
Perda de arquivos de usuários	Backup em nuvem de todos os dados que estão no servidor.
Possibilitar acessos indevidos às aplicações restritas da empresa	Troca periódica das senhas cadastradas com alto nível de criticidade e segurança; Trilha de auditoria habilitada; Política de segurança da informação e Cibernética da empresa acessível aos usuários.

Risco Externo	**Ação de Proteção/Prevenção**
Tentativa de invasão a rede interna	O Firewall instalado na rede analisa todo o tráfego de entrada na rede. Caso um dos acessos seja suspeito o próprio firewall de forma proativa realiza o bloqueio e alerta o TI local do acesso bloqueado.

3.7.52. Todos os novos equipamentos e sistema instalados na Sociedade devem contar com as configurações de proteção acima descritas, sendo realizado teste em ambientes de homologação e de prova antes do início da sua utilização. Sem prejuízo, semestralmente

são realizadas inspeções visando a verificação da atualização dos sistemas operacionais e softwares instalados nos computadores da Sociedade.

3.7.53. Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de TI, sendo vedadas aplicações não autorizadas por meio de controles de execução de processos.

Mecanismos de Supervisão da Segurança Cibernética

3.7.54. Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

3.7.55. São realizados os seguintes testes de verificação para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados:

Rotina	Periodicidade
Backup	Diário
Teste de restauração de dados	Diário
Teste de invasão externa e *phishing*	Semestral
Teste de resposta a incidentes com simulação de cenários	Semestral
Análise de Logs e trilhas de auditoria	Diário

3.7.56. São mantidos inventários atualizados de hardware e softwares utilizados pela Sociedade. Semestralmente são realizadas verificações, a fim de identificar elementos estranhos à Sociedade, tais como computadores não autorizados ou softwares não licenciados.

3.7.57. Sempre que houver alteração relevante na estrutura tecnológica da Sociedade serão realizadas análises de vulnerabilidade.

Resposta a Incidentes Cibernéticos

3.7.58. A Sociedade adota os seguintes procedimentos de resposta a incidentes em função das ameaças identificadas:

(i) Avaliação Inicial: aspectos e decisões fundamentais deverão ser analisadas pelo Responsável pela Segurança Cibernética, em conjunto com a Diretoria e tomadas após o

incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

(ii) Incidente Caracterizado: Se for caracterizado um incidente, devem os Diretores tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à CVM, ANBIMA ou mais alguma autoridade; (ii) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial ao investidor que tenha sido afetado; e (iv) houve prejuízo para a Sociedade, algum veículo de investimento ou investidor específico. Além disso, a Diretoria, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros.

(iii) Recuperação: Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um call ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pela Diretoria, para estabelecer as medidas a serem tomadas, responsabilidades e prazos. Também deverá ser avaliado o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e, caso necessário, tomar as devidas ações, tais como manifestação pública na mídia, enquanto que a Diretoria verificará se todas as informações necessárias ao portfólio estão seguras e a área de Gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por colaboradores da Sociedade, devem ser comunicados à Diretoria. Colaboradores externos relevantes deverão ser mantidos atualizados.

(iv) Retomada: refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao full compliance, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A área de Compliance deverá registrar o histórico em local adequado, como o sistema de gerenciamento Compliasset.

3.7.59. Compete ao Diretor de Compliance e ao Responsável pela Segurança Cibernética a comunicação da contingência aos demais colaboradores da Sociedade, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância do Plano de Continuidade de Negócios.

3.7.60. Cabe à Equipe de Compliance e Risco desenvolver relatórios acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda

medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tais relatórios deverão ser submetidos à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

3.7.61. Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a Sociedade estudará procedimentos preventivos a serem implementados e incluídos neste Plano de Continuidade de Negócios.

Programa de Treinamento

3.7.62. A Sociedade conta com um Programa de Treinamento dos colaboradores que tenham acesso a informações confidenciais, conforme descrito no presente Código de Ética e Conduta. O treinamento levará em consideração o tratamento das informações confidenciais e, no que se refere ao tratamento de Dados Pessoais e Dados Pessoais Sensíveis, abordará aspectos como: (i) natureza; (ii) escopo; (iii) finalidade; (iv) probabilidade e a gravidade de riscos; (v) benefícios decorrentes do tratamento de dados.

VIII. Política de Tratamento de Conflitos de Interesses e Segregação de Atividades e Funções

3.8.1. Consideram-se conflitos de interesse, de forma genérica e não limitadamente, quaisquer interesses pessoais dos colaboradores, em benefício próprio ou de terceiros, contrários ou potencialmente contrários aos interesses da Sociedade ou de seus investidores.

3.8.2. Os colaboradores devem evitar desempenhar outras funções fora da Sociedade que possam gerar conflitos de interesse, ou mesmo aparentar tais conflitos. Também devem evitar defender interesses de terceiros que possam gerar conflitos de interesse na hora da tomada de decisão e implicar em algum tipo de prejuízo para a Sociedade ou seus investidores.

3.8.3. Caso o colaborador resolva exercer outras atividades, sejam elas com ou sem fins lucrativos, além da praticada junto à Sociedade, deve comunicar previamente ao Diretor de Risco e Compliance da Sociedade para a devida aprovação a fim de evitar potenciais conflitos de interesse.

3.8.4. Caberá à área de Risco e Compliance orientar a estrutura de governança da Sociedade, visando garantir a segregação de atividades no âmbito interno e evitando

conflitos de interesse, ainda que potenciais, entre as atividades desenvolvidas pelos colaboradores na instituição.

3.8.5. A fim de evitar potenciais conflitos de interesse no que se refere à organização funcional da Sociedade, todos os colaboradores que atuam na atividade de gestão profissional de recursos de terceiros, participando do processo de análise, seleção e tomada de decisão de investimentos, dedicam-se com exclusividade à esta atividade.

3.8.6. A Sociedade disponibiliza ambiente físico segregado aos seus colaboradores, assim como infraestrutura tecnológica dedicada exclusivamente à consecução da atividade de gestão profissional de recursos de terceiros, os quais são protegidos pelos controles descritos nas Políticas de Proteção de Dados, Segurança da Informação e Segurança Cibernética adotadas pela Sociedade e descritas acima no presente Código de Ética e Conduta.

3.8.7. As atividades de gestão de risco e Compliance são coordenadas pelo Diretor de Risco, Compliance e PLD/FTP, podendo a equipe de risco e Compliance contar com profissionais compartilhados. Neste sentido, as atividades relacionadas à análise e gestão de riscos serão desempenhadas na forma da Política de Gestão de Riscos adotada pela Sociedade, servindo os controles internos para confirmação das ações tomadas para fins de observância da mencionada Política.

IX. Política de Contratos

3.9.1. À exceção de autorização prévia, específica e por escrito, somente a Diretoria da Sociedade podem contrair obrigações, assinar contratos, tratar acordos ou assumir compromissos de qualquer espécie em nome da Sociedade, observado o Contrato Social.

X. Política de Reembolso de Despesas

3.10.1. As notas fiscais ou documentos equivalentes indicando, de forma clara e discriminada, os gastos efetuados, são de apresentação obrigatória para a comprovação das despesas.

3.10.2. Sempre que possível, as notas fiscais ou documentos equivalentes devem ser emitidos em nome da Sociedade.

XI. Programa de Treinamento

3.11.1. A Sociedade conta com um programa de treinamento dos colaboradores e quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Sociedade tenham acesso a informações confidenciais ou participem do processo de decisão de investimento dividido em 02 (duas) etapas distintas.

3.112. A primeira etapa consiste na apresentação pelo Diretor de Compliance, ou colaborador por ele designado, dos normativos internos ao colaborador no ato do seu ingresso na Sociedade, disponibilizando-se para prestar quaisquer esclarecimentos que se façam necessários.

3.11.3. Já a segunda etapa do treinamento ocorre anualmente quando o Diretor de Compliance, colaborador por ele designado, ou terceiro contratado para este fim, abordará rotinas e processos descritos nos manuais e políticas internas, dando ênfase aos casos práticos ocorridos internamente ou no mercado.

3.11.3.1. Dentre os temas a serem tratados no treinamento anual de reciclagem, deverão ser abordados os seguintes assuntos:

- Risco de imagem e risco legal (Descumprimento da legislação/regulamentação).
- *Enforcement* - Implicações da não observância das normas de conduta e ética.
- Boas práticas para manipulação da informação e utilização indevida de informações privilegiadas.
- Barreiras de informação e segregação de atividades de forma a evitar possíveis conflitos de interesses.
- Política de segurança e preservação da Informação, conceito "*need to know*".
- Processo de análise, seleção e tomada de decisão, registro das operações e seus fundamentos.
- Segregação entre a gestão de recursos próprios e de terceiros – política de investimentos pessoais.
- Gerenciamento dos limites operacionais e de risco e enquadramento às políticas de investimento das carteiras sob gestão.
- Plano de Continuidade de Negócios.
- Procedimentos de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento a Proliferação de Armas de Destruição em Massa.
- Certificação e a regras da autorregulação sobre o tema, bem como alertas sobre a incompatibilidade de determinados cargos e funções por profissionais que não sejam certificados.

3.11.4. O Compliance poderá promover treinamentos em periodicidade menor, visando a atualização e ampliação do conhecimento dos colaboradores acerca de novidades normativas e regulatórias, bem como discutir casos concretos ocorridos dentro e fora da instituição.

XII. Política de Seleção, Contratação e Monitoramento de Prestadores de Serviços

3.12.1. A presente Política de Seleção, Contratação e Monitoramento de Prestadores de Serviços tem como objetivo definir as regras e os procedimentos para fins de seleção, contratação e supervisão dos terceiros contratados pela Sociedade em nome dos fundos de investimento sob gestão.

3.12.2. Compete à Diretoria a seleção dos prestadores de serviço, com base na presente Política, sendo coletado Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso a informações confidenciais que digam respeito à Sociedade, seus colaboradores, fundos sob gestão e investidores, salvo se este compromisso já tiver sido firmado entre as partes mediante a assinatura do correspondente Contrato de Prestação de Serviços.

3.12.3. Fica estritamente proibida a contratação em nome da Sociedade de pessoas físicas ou jurídicas com as quais qualquer dos colaboradores da Sociedade ou pessoa a este ligada possua interesse financeiro.

3.12.4. É vedada a contratação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo – GAFI, assim como pessoas politicamente expostas, indivíduos que ocupam ou ocuparam posições públicas, tais como: funcionários do governo, executivos de empresas governamentais, políticos, funcionários de partidos, assim como seus parentes e associados.

3.12.5. É vedada a contratação de prestadores de serviço que estejam envolvidos em investigação, inquérito, ação, procedimento judicial ou administrativo relativos à prática de atos lesivos, infrações ou crimes contra a ordem econômica ou tributária, de "lavagem" ou ocultação de bens, direitos e valores, ou contra o Sistema Financeiro Nacional, o Mercado de Capitais ou a administração pública, nacional ou estrangeira, incluindo, sem limitação, atos ilícitos que possam ensejar responsabilidade administrativa, civil ou criminal.

Processo de Seleção de Prestadores de Serviço (*Due Diligence*)

3.12.6. O processo de due diligence será coordenado pela Área de Compliance. Os terceiros contratados pela Sociedade devem atender as exigências mínimas abaixo especificadas:

(a) Preço: O preço cobrado pelo serviço deve ter um custo benefício atraente, em comparação com a média do mercado. Para esta aferição faz-se necessária, conforme o caso, a comparação dos preços cobrados pelo mesmo serviço por, no mínimo, 02 (duas) instituições diferentes.

(b) Qualidade: Todo prestador de serviço deve ter a qualidade comprovada, mediante a verificação de certificações e comprovantes de qualificação, tais como:

(i) Registros atuais em agências regulatórias e autorreguladoras, se for o caso;

(ii) Litígios passados ou correntes envolvendo a instituição e/ou seus controladores, diretores ou qualquer dos seus colaboradores no exercício das suas atividades profissionais;

(iii) Política de segurança da informação, conforme o caso;

(iv) Plano de continuidade de negócio, conforme o caso.

(c) Envio de documentos: Envio de cópia do contrato social e procuração (se aplicável), cópia da identidade e CPF dos sócios e dos procuradores (se aplicável), contrato para prestação de serviço com a Sociedade, bem como apresentação institucional da empresa, incluindo o currículo e as certificações dos colaboradores que estarão responsáveis pelo atendimento à Sociedade.

(d) Checagem de regularidade da empresa nos órgãos federais: Pesquisa no site da receita Federal do registro do CNPJ, prova de regularidade com o FGTS, Certidão Negativa de Débitos (CND) da empresa e dos sócios, e checagem de regularidade da empresa na CVM quando aplicável.

(e) Questionário Due Diligence da ANBIMA: Apresentar o Questionário de Due Diligence da ANBIMA para Contratação de Corretoras, conforme aplicável.

3.12.7. Para a contratação de Corretoras de Títulos e Valores Mobiliários serão adotados ainda os seguintes critérios visando a busca pelo melhor interesse dos investidores: (i) infraestrutura tecnológica e de recursos humanos adequada; (ii) plano de continuidade de negócios; (iii) política de segurança da informação; (iv) política anticorrupção; (v) política

de prevenção e combate à lavagem de dinheiro; (vi) qualidade dos relatórios de análise recebidos.

3.12.7.1. O eventual recebimento de serviços adicionais não será fator determinante no processo de seleção de corretoras de títulos e valores mobiliários. Qualquer vantagem neste sentido será utilizada em benefício das carteiras sob gestão da Sociedade, sendo outorgada ampla transparência ao investidor sobre os serviços adicionais eventualmente recebidos através do Formulário de Referência da Sociedade.

3.12.7.2. A contratação com corretoras também deve passar pela aprovação do processo de *due diligence* do administrador de cada fundo.

3.12.8. São realizadas consultas em listas restritivas e sites de busca para a conferência de dados e/ou identificação de informações desabonadoras, nos termos da Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo adotada pela Sociedade.

Cadastro

3.12.9. A Sociedade, após aprovação do prestador de serviços, deverá providenciar o cadastro internamente. Nesse sentido, a área de Compliance será responsável pela coleta da seguinte documentação para fins de cadastro do prestador de serviço:

(i) Breve informação sobre o histórico da empresa;

(ii) Cópia do contrato social arquivado no órgão competente;

(iii) Informações sobre a equipe;

(iv) Cópia da procuração, se aplicável; e

(ii) Contrato de Prestação de Serviços em linha com o conteúdo mínimo exigido pelo Código ANBIMA de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros.

3.12.10. A Sociedade poderá solicitar documentos e informações adicionais caso julgue necessário para fins da seleção do prestador do serviço.

Monitoramento e Supervisão Baseada em Risco

3.12.11. A área tomadora do serviço é responsável pelo monitoramento da prestação dos serviços pelos contratados pela Sociedade, indicando à Área de Compliance, anualmente, eventuais não-conformidades e ressalvas identificadas durante a prestação dos serviços contratados, incluindo informações sobre a frequência e o volume de desenquadramentos, não atendimento das solicitações da Sociedade nos prazos definidos, omissão ou intempestividade no fornecimento de informações ou documentos, dentre outros critérios que julgar pertinente.

3.12.12. A Sociedade adota metodologia de supervisão baseada em risco, na qual a instituição contratada é avaliada de acordo com os seguintes critérios: (i) criticidade da atividade desempenhada para a gestão das carteiras dos fundos de investimento; (ii) existência de redundância com relação ao prestador; (iii) existência de pessoa politicamente exposta no quadro societário ou principais executivos da instituição; (iv) identificação de ressalvas no processo de due diligence; (v) ocorrência de não conformidades reportadas pela equipe da Sociedade.

3.12.13. Após a avaliação dos critérios supramencionados o Diretor de Risco, Compliance e PLD/FTP classificará os prestadores de serviço da seguinte forma:

BAIXO RISCO: São classificadas como de baixo risco as instituições que apresentarem todas as informações solicitadas na forma da presente Política. Apesar da criticidade da atividade desempenhada poder ser alta, a instituição é classificada como de baixo risco caso: (i) haja redundância para a atividade desempenhada; (ii) não tenha sido apontada nenhuma ressalva no seu processo de due diligence ou revisão periódica; (iii) reputação ilibada; e (iv) for aderente/associado à ANBIMA, quando aplicável.

MÉDIO RISCO: São classificadas como de médio risco as instituições que tenham apresentado ressalvas em seu processo de due diligence ou de revisão periódica

ALTO RISCO: São classificados como de alto risco os prestadores de serviço que tiverem suas atividades autorreguladas pela ANBIMA e não forem associados ou aderentes aos Códigos ANBIMA de Regulação e Melhores Práticas. Sendo de alto risco a sua contratação só poderá ser feita mediante aceitação do Diretor de Risco, Compliance e PLD//FTP. A análise do prestador de serviço deve ser minuciosa, nos termos dos procedimentos adotados pela PLD/FTP e Código de Ética.

3.12.14. A classificação de que trata o item acima deve ser aplicada apenas àquelas instituições contratadas em nome dos fundos de investimento sob gestão cujas atividades sejam autorreguladas pela ANBIMA.

3.12.15. Tais informações serão objeto de relatórios anuais a serem elaborados pelo Diretor de Risco, Compliance e PLD/FTP à Diretoria, os quais conterão ainda eventuais sugestões de providências a serem tomadas, devendo ser arquivados na Sociedade, em meio físico ou eletrônico, em conjunto com as conclusões da Diretoria.

3.12.16. As informações cadastrais dos prestadores de serviço, bem como a pesquisa de idoneidade acima mencionada deverão ser atualizadas na forma e periodicidade definida na da Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

3.12.17. A reavaliação de que trata acima poderá ocorrer em períodos menores, sempre que houver qualquer fato novo, ou alteração significativa que a critério da Sociedade justifique a referida reavaliação.

3.12.18. A Sociedade deve manter pelo prazo mínimo de 5 (cinco) anos todos os documentos e informações relacionados ao processo de seleção, contratação e monitoramento dos prestadores de serviços, sendo admitido o arquivamento eletrônico.

Considerações Finais e *Enforcement*

4.1. O presente Código prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da Sociedade aos seus termos e condições.

4.2. A título de enforcement, vale notar que a não observância dos dispositivos do presente Código resultará em advertência, suspensão ou demissão/exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais eventualmente cabíveis.

4.3. Este Código será revisado anualmente, sendo mantido o controle de versões. A cada revisão será coletado novo Termo de Adesão e Confidencialidade dos colaboradores, na forma e para fins de atendimento aos itens 1.2 e 1.3. do presente.

4.4. Qualquer suspeita, conhecimento de violação deste Código ou indício de práticas corruptivas por parte de colaboradores deve ser objeto de informação ao Diretor de Compliance através do e-mail fneves@riogestao.com.br que, em seguida, comunicará à Diretoria para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos. A comunicação poderá ser feita de forma identificada ou anônima, sendo garantido o seu sigilo.

4.5. Na ocorrência de quaisquer dúvidas sobre as regras e princípios inerentes ao cumprimento do presente Código de Ética e Conduta, o colaborador deve procurar o Diretor de Compliance para obter orientação adequada, podendo, inclusive, encaminhar um e-mail para fneves@riogestao.com.br.

4.6. Todos os documentos que evidenciem a observância dos dispositivos do presente Código devem ser arquivados na Sociedade, em meio eletrônico ou físico, pelo prazo mínimo de 5 (cinco) anos, para fins de controles internos.

TERMO DE ADESÃO E CONFIDENCIALIDADE

Pelo presente Termo de Adesão e Confidencialidade, **[NOME]**, [nacionalidade], [profissão], portador da carteira de identidade nº [definir], expedida pelo [órgão expedidor], inscrito no CPF sob o nº [definir], na qualidade de colaborador da **RIO PERFORMANCE GESTÃO DE RECURSOS LTDA.** ("Sociedade"), declaro que:

- recebi cópia dos manuais e políticas identificados no quadro infra, tendo sido apresentado o seu teor pelo Diretor de Risco e Compliance, o qual colocou-se à disposição para esclarecer toda e qualquer dúvida porventura existente;

- compreendi a integralidade dos termos e disposições definidos pelos manuais e políticas em questão, comprometendo-se a cumpri-las e observá-las no dia-a-dia das suas atividades.

Manual/Política	**Adesão** X [OU] N/A
Código de Ética, Conduta e Políticas Internas	
Manual de Compliance	
Política de Gestão de Riscos	
Política de Investimentos Pessoais	
Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo	
Política de Rateio e Divisão de Ordens	
Política de Voto	
Política de Distribuição e Suitability	

Comprometo-me a observar todas as regras, manuais e políticas internas definidas pela Sociedade, legislação e regulamentação aplicáveis às minhas atividades e às atividades da Sociedade, e estou ciente de que a não observação dessas regras poderá caracterizar falta grave, passível de punição, inclusive rescisão contratual ou de exclusão por justa causa do quadro societário.

Comprometo-me a informar ao Diretor de Compliance quaisquer violações ou indícios de violação a que tenha ciência às regras internas definidas pela Sociedade, assim como à legislação e regulamentação aplicáveis à minha atividade e às atividades da Sociedade.

Autorizo o Compliance ao tratamento dos meus dados pessoais, sensíveis ou não, para fins de cumprimento das leis e normas que regem a atividade da Sociedade, bem como quando necessário para atendimento dos seus interesses legítimos, proteção da sua reputação e imagem, ou de seus clientes. O consentimento ora outorgado poderá ser revogado, não afetando, entretanto, a legalidade de nenhum tratamento realizado em momento anterior à revogação, bem como o tratamento lícito dispensado da necessidade de consentimento.

Declaro ciência que, durante o exercício das minhas atividades profissionais na Sociedade, poderei ter acesso a informações confidenciais, conforme definido no Código de Ética e Conduta. Na qualidade de colaborador e mesmo após o término do vínculo com a Sociedade, comprometo-me a guardar sigilo em relação às Informações Confidenciais, sendo expressamente vedada sua revelação a terceiros ou a colaboradores não autorizados da Sociedade ou sua utilização para outros fins que não a devida execução das minhas atividades profissionais na Sociedade.

Dessa maneira e por meio deste Termo, comprometo-me a zelar para que Informações Confidenciais permaneçam restritas ao conhecimento de colaboradores autorizados ou que necessitem dessas informações para a devida execução de suas atividades profissionais na Sociedade.

Declaro, ademais, que informarei ao Compliance caso eu seja considerado Pessoa Politicamente Exposta ("PPE"), ou caso possua relacionamento ou ligação com PPE.

Declaro, ainda, que:

a. Possuo reputação ilibada;

b. Nunca estive inabilitado(a) ou suspenso(a) para o exercício de cargo em instituições financeiras e demais entidades autorizadas a funcionar pela CVM, pelo Bacen, pela SUSEP ou pela PREVIC;

c. Nunca fui condenado(a) por crime falimentar, prevaricação, suborno, concussão, peculato, lavagem de dinheiro ou ocultação de bens, direitos e valores, contra a economia popular, a ordem econômica, as relações de consumo, a fé pública ou a propriedade pública, o sistema financeiro nacional, ou a pena criminal que vede, ainda que temporariamente, o acesso a cargos públicos, por decisão transitada em julgado, ressalvada a hipótese de reabilitação;

d. Não estou impedido(a) de administrar seus bens ou deles dispor em razão de decisão judicial ou administrativa;

e. Nunca sofri punição definitiva, nos últimos 05 (cinco) anos, em decorrência da minha atuação como administrador ou membro do conselho fiscal de entidade sujeita ao controle e fiscalização dos órgãos reguladores mencionados acima.

Por fim, declaro que manterei o Compliance atualizado sobre quaisquer mudanças nas informações prestadas neste Termo.

O presente Termo de Adesão e Confidencialidade é firmado, de forma irrevogável e irretratável, em 2 (duas) vias, de igual teor e forma, permanecendo uma das vias arquivada na sede da Sociedade.

Rio de Janeiro, [dia] de [mês] de [ano]

_____

[NOME DO COLABORADOR]