VINO CAPITAL GESTÃO DE RECURSOS LTDA.

CNPJ nº 61.230.735/0001-04

MANUAL DE REGRAS, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

31 de agosto de 2025

OBJETIVO E ABRANGÊNCIA

- Sumário

A **VINO CAPITAL GESTÃO DE RECURSOS LTDA.**, na qualidade de sociedade que atua como administradora de carteira de valores mobiliários na categoria "gestor de recursos" ("Sociedade") desenvolveu o presente Manual de Regras, Procedimentos e Descrição dos Controles Internos ("Manual") observando a regulamentação da Comissão de Valores Mobiliários ("CVM") e autorregulação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de forma a estabelecer diretrizes e princípios que orientem o comportamento ético e profissional dos sócios, administradores, empregados e colaboradores da Sociedade ("Colaboradores"), incluindo as suas condutas internas no âmbito do exercício de suas atividades profissionais, sempre pautadas com base no compliance interno.

Dessa forma, este Manual foi elaborado observando as seguintes principais regras, normas e orientações regulatórias e autorregulatórias:

- Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21");
- Código da ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código de AGRT") e demais disposições acessórias a este Código;
- Código da ANBIMA de Ética ("Código de Ética") e demais disposições acessórias a este Código;
- Código ANBIMA de Certificação Continuada ("Código de Certificação"); e
- Demais documentos divulgados pela regulação e autorregulação que forem aplicáveis às atividades da Sociedade.

O presente Manual foi estruturado de forma proporcional à atual fase pré-operacional da Vino Capital, devendo evoluir em abrangência e detalhamento conforme a expansão da operação e o aumento da complexidade dos fundos sob gestão, preservando sempre a aderência regulatória e autorregulatória.

- Declaração de Recebimento e Compromisso

Este Manual integra as diretrizes que regem a relação entre a Sociedade e os seus Colaboradores. Ao subscreverem a Declaração de Recebimento e Compromisso (Anexo I), os Colaboradores manifestam expressamente ciência e concordância com as normas, princípios e procedimentos nele previstos.

É responsabilidade de todos os Colaboradores compreender as normas aplicáveis à Sociedade e adotar conduta compatível com este Manual. A assinatura da Declaração de Recebimento e Compromisso formaliza a adesão do Colaborador, que se compromete a zelar pelo cumprimento das regras de compliance aqui previstas. Sempre que necessário, a Sociedade poderá solicitar a assinatura de nova declaração, reforçando o compromisso com os termos do Manual.

A violação ou suspeita de violação das normas previstas neste Manual, ou de outras normas aplicáveis às atividades da Sociedade, deverá ser comunicada ao Diretor de Compliance, Risco e PLD, que conduzirá a apuração e aplicará as medidas cabíveis, assegurando ao Colaborador o direito de defesa.

É dever de todos os Colaboradores reportar violações ou indícios de violações de princípios e normas, visando preservar os interesses dos clientes e a reputação da Sociedade. Caso a suspeita envolva o próprio Diretor de Compliance, Risco e PLD, a comunicação deverá ser feita diretamente aos demais administradores da Sociedade.

POLÍTICA DE COMPLIANCE

- Obrigações Internas da Área de Compliance

No atual estágio de constituição e fase pré-operacional da Vino Capital, a área de Compliance é formalmente composta pelo Diretor de Compliance, Risco e PLD, designado no Contrato Social, que acumula integralmente suas atribuições. Embora atualmente não conte com equipe dedicada, a área de Compliance existe e exerce suas funções de forma proporcional à estrutura da Gestora, podendo ser expandida futuramente, à medida que a operação cresça e aumente a complexidade dos fundos sob gestão.

Entre outras atribuições, compete ao Diretor de Compliance, Risco e PLD:

a. acompanhar as políticas descritas neste Manual;
b. assegurar que todos os Colaboradores que desempenhem funções ligadas à administração de carteiras de valores mobiliários atuem com imparcialidade e conheçam este Manual, o código de ética, as normas aplicáveis e as políticas previstas pela Resolução CVM 21;
c. encaminhar pedidos de autorização, orientação, esclarecimento ou relatar ocorrências, suspeitas ou indícios de práticas contrárias às disposições deste Manual e demais normas aplicáveis à atividade da Sociedade para análise dos administradores da sociedade;
d. identificar possíveis condutas em desacordo com este Manual;
e. centralizar informações e realizar revisões periódicas dos processos de compliance, especialmente em casos de alterações nas políticas vigentes ou aumento no número de colaboradores;
f. assessorar a gestão de negócios no entendimento, interpretação e impacto da legislação, monitorando as melhores práticas e analisando periodicamente as normas emitidas por órgãos competentes como a CVM e outros organismos similares;
g. elaborar o Relatório Anual de Compliance, contendo avaliação sobre a adequação das políticas, procedimentos e controles internos da Sociedade, bem como recomendações de aperfeiçoamento;
h. submeter o Relatório Anual de Compliance à Alta Administração, até o último dia útil de abril de cada ano, incluindo (i) conclusões das revisões realizadas; (ii) eventuais deficiências identificadas, com plano de ação e cronograma de saneamento; e (iii) manifestação sobre medidas adotadas em relação a recomendações anteriores;
i. promover a ampla divulgação e aplicação dos preceitos éticos nas atividades de todos os Colaboradores, incluindo treinamentos periódicos conforme previsto neste Manual;
j. avaliar todos os casos relacionados ao potencial descumprimento dos preceitos éticos e de compliance estabelecidos neste Manual ou em outros documentos mencionados, além de analisar situações não previstas;
k. garantir o sigilo de informantes de delitos ou infrações, mesmo quando não solicitado, exceto em casos que demandem testemunho judicial;
l. solicitar, sempre que necessário, o apoio da auditoria interna ou externa ou outros assessores profissionais para análise de questões específicas;
m. aplicar eventuais sanções aos Colaboradores; e

n. analisar situações que cheguem ao seu conhecimento e que possam caracterizar "conflitos de interesse" pessoais e profissionais.

Qualquer Colaborador ciente de informações ou situações em curso que possam afetar os interesses da Sociedade, gerar conflitos ou contrariar os termos deste Manual deve informar o Diretor de Compliance, Risco e PLD para adoção das medidas apropriadas, a fim de administrar e eliminar eventuais conflitos.

O Diretor de Compliance, Risco e PLD pode contar com outros Colaboradores para atividades e rotinas de compliance, com atribuições específicas determinadas conforme a necessidade da Sociedade e a senioridade do Colaborador.

- ❖ Esclarecimentos e formas de contato com o Diretor de Compliance, Risco e PLD

Em caso de dúvidas sobre as disposições deste Manual ou sobre normas aplicáveis às atividades da Sociedade, o Colaborador deverá entrar em contato com o Diretor de Compliance, Risco e PLD para obter a devida orientação.

Da mesma forma, qualquer ocorrência, suspeita ou indício de prática em desacordo com este Manual ou com a legislação vigente deve ser comunicada de forma imediata ao Diretor de Compliance, Risco e PLD, exclusivamente por meio de canais corporativos formais (como e-mail institucional).

Essa conduta garante transparência, segurança e alinhamento das atividades da Sociedade, reforçando a cultura ética e de conformidade.

- ❖ Procedimentos internos de supervisão periódica

Em caso de violação, suspeita ou indício de não conformidade com as diretrizes estabelecidas neste Manual ou com normas aplicáveis às atividades da Sociedade, que cheguem ao conhecimento do Diretor de Compliance, Risco e PLD, este adotará as medidas necessárias para avaliar a conduta envolvida, com base nos registros e controles internos disponíveis.

O Diretor de Compliance, Risco e PLD poderá realizar revisões periódicas dos processos e controles internos, com o objetivo de identificar fragilidades e propor correções, sempre observando os princípios da proporcionalidade, confidencialidade e conformidade com a legislação vigente, inclusive a Lei Geral de Proteção de Dados (LGPD).

Essas revisões poderão incluir a análise de comunicações institucionais realizadas por meios corporativos (como e-mails e sistemas internos), de forma limitada ao necessário e respeitando a privacidade dos Colaboradores. A utilização dessas informações será restrita às finalidades de verificação de conformidade, e seu compartilhamento ocorrerá apenas nos termos da lei ou de determinação de autoridade competente.

Adicionalmente, o Diretor de Compliance, Risco e PLD deverá realizar verificações regulares dos níveis de controles internos e de conformidade em todas as áreas da Sociedade, monitorando a implementação de eventuais medidas corretivas recomendadas.

- Independência na Atuação

Os membros que atuarem nas funções de compliance comporão a Área de Compliance, que estará sob a supervisão do Diretor de Compliance, Risco e PLD. É importante destacar que a Área de Compliance desempenha suas atribuições de maneira totalmente autônoma em relação às demais áreas da Sociedade e terá a capacidade de exercer sua autoridade e poderes sobre qualquer Colaborador.

O Diretor de Compliance, Risco e PLD não desempenhará funções diretamente relacionadas à gestão de recursos, de forma a preservar sua independência e evitar potenciais conflitos de interesse.

- Dever de Reportar

O Colaborador que tomar ciência ou suspeitar de qualquer ato em desacordo com as disposições deste Manual deve, de imediato, informar tal ocorrência ao Diretor de Compliance, Risco e PLD. Nenhum Colaborador enfrentará represálias por denunciar, de maneira honesta, violações ou potenciais violações a este Manual. Ademais, todas as notificações e investigações serão tratadas com confidencialidade, na medida do possível nessas circunstâncias. No entanto, o Colaborador que deixar de cumprir essa obrigação poderá estar sujeito não apenas a medidas disciplinares, mas também à demissão por justa causa, de acordo com o regime jurídico vigente.

- Sanções ("*Enforcement*")

O Diretor de Compliance, Risco e PLD é responsável pela aplicação de eventuais sanções decorrentes do não cumprimento dos princípios deste Manual, assegurando ao Colaborador amplo direito de defesa. Tais sanções podem incluir advertência, suspensão, desligamento ou exclusão por justa causa, se o Colaborador for sócio da Sociedade. Para Colaboradores que sejam empregados, a demissão por justa causa é uma opção, conforme o artigo 482 da CLT, sem prejuízo do direito de a Sociedade buscar indenização pelos prejuízos, perdas, danos e/ou lucros cessantes por meio de medidas legais cabíveis.

A Sociedade não assume a responsabilidade por Colaboradores que violem a lei ou cometam infrações em suas funções. Se a Sociedade for responsabilizada ou sofrer prejuízos devido a ações de seus Colaboradores, reserva-se o direito de regresso contra os responsáveis.

A aplicação das sanções observará os princípios da proporcionalidade e da razoabilidade, sendo sempre precedida de oportunidade de defesa pelo Colaborador envolvido. Na definição da medida aplicável, serão considerados fatores como a gravidade da infração, o grau de culpa, eventual reincidência e os impactos para a Sociedade e seus clientes.

CONFIDENCIALIDADE

- Sigilo e Conduta

As normativas presentes neste Capítulo são destinadas aos Colaboradores que, por meio de suas incumbências na Sociedade, possam ter ou venham a ter acesso a informações confidenciais, reservadas ou privilegiadas, abrangendo aspectos financeiros, técnicos, comerciais, estratégicos, negociais, econômicos, entre outros.

É necessário que todos os Colaboradores leiam minuciosamente e compreendam as disposições contidas neste Manual, sendo também necessário assinar a Declaração de Confidencialidade, conforme modelo apresentado no Anexo II.

Nesse sentido, com base na Declaração de Confidencialidade, é estritamente proibido divulgar qualquer Informação Confidencial, conforme definido a seguir, para fora da Sociedade. Qualquer divulgação, seja no âmbito pessoal ou profissional, que não esteja em conformidade com as normas legais, está expressamente vetada.

São consideradas "Informações Confidenciais", aquelas que não possam ser tornadas públicas, incluindo, mas não se limitando a:

a. Portfólio de Ativos: composição detalhada do portfólio de ativos, incluindo tipos de títulos, valores mobiliários e características específicas de cada fundo gerido pela Sociedade;
b. Relatórios de Risco: avaliações internas de risco, análises de sensibilidade e projeções relacionadas ao desempenho futuro dos fundos;
c. Informações sobre Clientes: dados pessoais e financeiros dos clientes, bem como histórico de transações e investimentos realizados por eles;
d. Acordos Contratuais: termos e condições de contratos, acordos e negociações com parceiros, prestadores de serviços e outras partes envolvidas nas operações;
e. Relatórios de Auditoria Interna: resultados de auditorias internas, incluindo recomendações, conclusões e ações corretivas propostas;
f. Planejamento Estratégico: informações sobre estratégias de negócios, metas corporativas, expansão de mercado e desenvolvimento de novos produtos ou serviços;
g. Informações Regulatórias Sensíveis: comunicações com órgãos reguladores, pareceres legais e informações relacionadas a conformidade com as normas do setor; e
h. Estrutura Organizacional: detalhes sobre a estrutura interna da Sociedade, incluindo cargos, responsabilidades e informações sobre a equipe de gestão e áreas de suporte.

A divulgação a terceiros não colaboradores ou colaboradores não autorizados da Informação Confidencial é proibida em qualquer circunstância.

A colaboração da Sociedade com autoridades fiscalizadoras, a divulgação de Informações Confidenciais a autoridades governamentais por decisões judiciais, arbitrais ou administrativas, requer prévia comunicação ao

Diretor de Compliance, Risco e PLD. Após esgotar medidas jurídicas para evitar a revelação, será definido junto a alta administração sobre o método apropriado.

Essas diretrizes aplicam-se não apenas durante o relacionamento profissional entre a Sociedade e o Colaborador, mas também após seu término. Colaboradores devem manter sigilo sobre Informações Confidenciais, responsabilizando-se por danos em caso de descumprimento, e garantir que os subordinados também o façam e tenham esse mesmo zelo e cuidado com as Informações Confidenciais.

Ao ter acesso a Informações Confidenciais, os Colaboradores devem informar imediatamente o Diretor de Compliance, Risco e PLD, mencionando a fonte. Isso se aplica mesmo quando a informação é conhecida acidentalmente ou por negligência. Os Colaboradores não devem usar ou divulgar a informação, exceto para o Diretor mencionado.

O uso das Informações Confidenciais para obter vantagem indevida, por negociação de títulos e valores mobiliários, é expressamente proibida, sujeitando o Colaborador a penalidades e possível demissão por justa causa.

SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

Por se tratar do momento de constituição e fase pré-operacional, esta Política foi estruturada de forma proporcional à realidade atual da Vino Capital, com previsão de evolução em sofisticação e abrangência conforme o crescimento da operação e o aumento da complexidade dos fundos sob gestão.

Neste estágio, a Vino Capital utiliza endereço virtual apenas para fins de registro societário e recebimento de correspondências, não possuindo atendimento físico nem área compartilhada com outras empresas. Todos os colaboradores atuam em regime remoto, e as atividades da Gestora são integralmente executadas em ambiente digital seguro, com armazenamento em nuvem e acesso restrito.

As medidas previstas neste Manual serão implementadas de forma progressiva, priorizando aquelas essenciais para mitigar riscos imediatos e assegurar a conformidade regulatória mínima desde a fase inicial.

O propósito das medidas de segurança da informação é mitigar ameaças aos interesses da Sociedade, alinhando-se às diretrizes deste Manual e garantindo a proteção das Informações Confidenciais. Para tanto, são adotados controles de acesso rigorosos aos sistemas e arquivos digitais utilizados pela Vino Capital.

Como a Gestora não mantém escritório físico de operação, inexiste circulação de público ou de colaboradores em instalações próprias. Eventuais correspondências recebidas no endereço virtual são tratadas exclusivamente por prestador de serviço contratado, com registro formal de recebimento e encaminhamento imediato aos Diretores.

A disposição dos equipamentos de rede exige que estes sejam armazenados em sala com acesso restrito. As estações de trabalho são fixas, equipadas com computadores seguros, e é obrigatório trancar as sessões abertas quando não estão sob supervisão do Colaborador responsável pelo respectivo computador. A política de segurança cibernética e de proteção de dados leva em conta vários riscos e cenários, considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades da Sociedade.

A responsabilidade direta pela coordenação das iniciativas relacionadas a esta política é atribuída ao Diretor de Compliance, Risco e PLD, que supervisionará a implementação, revisará periodicamente os controles, conduzirá testes e proporcionará treinamento aos Colaboradores, conforme detalhado abaixo.

- Identificação de Riscos *(risk assessment)*

A Sociedade identificou que os riscos indicados abaixo necessitam de maior resguardo, incluindo, mas não se limitando a:

a. Sistemas: inclui dados sobre os sistemas empregados pela Sociedade e as tecnologias desenvolvidas internamente e por terceiros, juntamente com suas possíveis ameaças e vulnerabilidades.

b. Governança da Gestão de Risco: diz respeito à efetividade da gestão de riscos realizada pela Sociedade no que tange às ameaças identificadas.

c. Dados e Informações: abrange as Informações Confidenciais, que englobam dados relativos a investidores, clientes, Colaboradores e à própria Sociedade, além de informações sobre as operações realizadas.

d. Processos e Controles: se enquadram os processos e controles internos que integram a rotina das diversas áreas de negócio da Sociedade.

Não obstante, conforme o Guia de Cibersegurança divulgado pela ANBIMA, destacam-se abaixo os principais ataques cibernéticos que a Sociedade poderá enfrentar:

a. Malware – softwares desenvolvidos para corromper computadores e redes (por exemplo: Vírus, Cavalo de Troia, Spyware e Ransomware);

b. Engenharia Social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

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

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

❖ Ações de Prevenção e Proteção

A Sociedade desenvolveu e estabeleceu um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, que busca impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles internos adequados e robustos.

- Acesso: contas individuais, autenticação multifator (MFA) e perfis mínimos necessários; revisão semestral de acessos.
- Senhas: critérios fortes e renovação periódica; bloqueio após tentativas malsucedidas.
- Ativos: inventário de dispositivos; criptografia de discos; antivírus/EDR; atualizações automáticas.
- Rede/Nuvem: firewalls, segmentação, logs centralizados; provedores de nuvem com certificações reconhecidas.
- *Backups*: rotina diária e teste periódico de restauração.
- *Offboarding*: revogação imediata de acessos e recolhimento de ativos no desligamento.

Essas medidas serão periodicamente revisadas pelo Diretor de Compliance, Risco e PLD, de modo a assegurar sua efetividade e aderência às melhores práticas e regulamentações aplicáveis.

- ❖ Monitoramento e Testes

O Diretor de Compliance, Risco e PLD realizará, ao menos uma vez por ano, o monitoramento por amostragem do uso de sistemas e ferramentas corporativas fornecidas pela Sociedade, incluindo acessos a pastas de rede, sistemas internos e aplicações utilizadas no dia a dia.

Enquanto não houver rede corporativa própria, o monitoramento recairá sobre as ferramentas em nuvem atualmente utilizadas, dentro dos limites técnicos disponíveis.

O objetivo é avaliar a aderência às regras de segurança da informação e restrição de acesso, podendo o Diretor de Compliance, Risco e PLD adotar medidas adicionais de monitoramento sempre que julgar necessário para garantir a conformidade e a eficácia dos controles internos.

- ❖ Plano de Identificação e Resposta a Incidentes: Detalhes e Fundamentação

- o Âmbito e definição: Considera-se incidente de segurança qualquer evento que afete a confidencialidade, integridade ou disponibilidade de informações/sistemas da Sociedade (ex.: acesso não autorizado, perda ou indisponibilidade de dados, malware/ransomware, vazamento de credenciais, fraude ou falha grave de controle).

- o Responsáveis: O Diretor de Compliance, Risco e PLD é o responsável por coordenar o plano e a resposta aos incidentes, podendo designar substituto em caso de impedimento.

- o Detecção e triagem: A identificação de incidentes ocorre por meio de alertas das ferramentas e provedores contratados, bem como relatos de Colaboradores e parceiros. A triagem inicial deve ser realizada em até 24h úteis após o conhecimento do incidente.

- o Classificação: Os incidentes são classificados como baixo, médio ou alto risco, conforme impacto potencial/real em operações, dados pessoais/sensíveis, clientes e requisitos regulatórios.

- o Resposta e contenção: Para incidentes médios ou altos: (i) contenção imediata (ex.: isolamento de contas ou dispositivos), (ii) erradicação (correções técnicas), (iii) recuperação segura (restauração de backups testados) e (iv) verificação de retorno à normalidade.

- o Comunicação e reporte: A Sociedade informará terceiros e autoridades quando exigido pela legislação ou por contrato, inclusive a Autoridade Nacional de Proteção de Dados ("ANPD") e titulares de dados (LGPD), e, se aplicável, CVM/ANBIMA e administradores fiduciários.

- Registro e lições aprendidas: Todos os incidentes, decisões e medidas adotadas são documentados em registro próprio; evidências e relatórios são guardados por 5 anos. Relatório pós-incidente deve ser produzido em até 10 dias úteis após o encerramento.

- Testes: O plano será testado ao menos 1 vez por ano e revisado à luz das lições aprendidas e mudanças regulatórias.

❖ Arquivamento de Informações

A Sociedade manterá arquivados, pelo período legal aplicável, todos os dados, documentos e registros necessários para o pleno atendimento de auditorias, fiscalizações ou investigações conduzidas por autoridades competentes.

O arquivamento será centralizado pela Área de Compliance, em conjunto com as áreas operacionais competentes, garantindo: (i) integridade e disponibilidade das informações; (ii) proteção contra acesso não autorizado; e (iii) observância às normas legais e regulatórias aplicáveis, inclusive no que se refere à prevenção à corrupção e à lavagem de dinheiro.

Considerando a inexistência de instalações físicas, o arquivamento e os backups serão gradualmente estruturados em ambiente de nuvem certificado em padrões de segurança reconhecidos, não havendo previsão de armazenamento permanente em local físico. O acesso a esses repositórios será implementado de forma individualizada, com autenticação multifator e revisões periódicas a serem conduzidas pelo Diretor de Compliance, Risco e PLD, à medida que a operação evolua.

❖ Propriedade Intelectual

Todos os documentos, informações e materiais produzidos pelos Colaboradores no exercício de suas atividades profissionais, incluindo minutas, planilhas, e-mails, relatórios e modelos de avaliação, são de propriedade exclusiva da Sociedade.

O uso desses materiais é restrito às finalidades profissionais e é vedada sua utilização para fins pessoais ou externos, mesmo após o desligamento. Nesse caso, o Colaborador deverá devolver todos os documentos e arquivos da Sociedade em seu poder, em qualquer meio ou formato.

A Sociedade poderá, a seu critério, firmar termos específicos de confidencialidade ou propriedade intelectual, quando aplicável, para reforçar a proteção de ativos estratégicos.

O compromisso com a proteção da propriedade intelectual e da confidencialidade é condição essencial para a relação entre a Sociedade e seus Colaboradores, sendo o descumprimento sujeito às medidas disciplinares e legais cabíveis.

❖ Segregação e Confidencialidade em Endereço Virtual

Embora utilize endereço virtual apenas para fins cadastrais, a Vino Capital mantém contrato que assegura a segregação física de documentos eventualmente recebidos e proíbe o acesso de terceiros a informações sigilosas. Não há compartilhamento de área de trabalho, e o provedor do endereço virtual não participa das atividades da Gestora, atuando exclusivamente como recebedor de correspondências, conforme descrito em contrato.

- ❖ Revisão da Política

Esta Política de Segurança Cibernética e Proteção de Dados deverá ser revisada pelo Diretor de Compliance, Risco e PLD em periodicidade inferior a 24 (vinte e quatro) meses, e sempre que identificada a necessidade de atualização em prazo inferior, decorrente de alterações regulatórias e/ou autorregulatórias, o referido Diretor o fará.

POLÍTICA ANTICORRUPÇÃO

A Sociedade está comprometida com a conduta ética e transparente em todas as suas atividades. A presente Política Anticorrupção estabelece os princípios e diretrizes que norteiam a atuação da empresa na prevenção e combate à corrupção, em consonância com a Lei nº 12.846/13 (Lei Anticorrupção) e o Decreto nº 8.420/15.

- Abrangência

Esta Política aplica-se a todos os Colaboradores da Sociedade, incluindo diretores, sócios, empregados, estagiários e colaboradores, bem como a terceiros que atuem em nome da Sociedade, como consultores, prestadores de serviços, fornecedores e demais parceiros de negócio.

- Definições

Para os fins desta Política, considera-se:

a. Corrupção: qualquer conduta que implique em obtenção de vantagem indevida, direta ou indireta, em razão da função pública exercida pelo agente público;
b. Agente Público: qualquer pessoa que exerça cargo, emprego ou função pública, incluindo os membros de qualquer poder;
c. Propina: vantagem indevida oferecida ou prometida a agente público, para que ele pratique, omita ou retarde ato de ofício;
d. Facilitação de pagamento indevido: vantagem indevida oferecida ou prometida a agente público, para que ele pratique ato de ofício que não seja de seu dever legal;
e. Peculato: apropriação indébita de dinheiro, valor ou qualquer outro bem público;
f. Corrupção Passiva: solicitar ou receber, para si ou para outrem, direta ou indiretamente, vantagem indevida, em razão da função pública exercida;
g. Corrupção Ativa: oferecer ou prometer, direta ou indiretamente, vantagem indevida a agente público, para que ele pratique, omita ou retarde ato de ofício.

- Princípios

A Política Anticorrupção da Sociedade é fundamentada nos seguintes princípios:

a. Transparência: todas as atividades da Sociedade devem ser conduzidas de forma transparente e aberta;
b. Integridade: os Colaboradores da Sociedade devem agir com honestidade e ética em todas as suas relações;
c. Responsabilidade: a Sociedade e seus Colaboradores são responsáveis por seus atos e omissões; e
d. Zero Tolerância: a Sociedade não tolera qualquer tipo de prática corrupta.

- Código de Conduta

De forma a buscar sempre as melhores e mais corretas condutas internas pelos Colaboradores da Sociedade, é expressamente vedado:

a. oferecer, prometer ou dar vantagem indevida a Agente Público;
b. solicitar ou receber vantagem indevida de Agente Público;
c. solicitar ou receber Propina;
d. praticar qualquer ato de corrupção, seja ativa ou passiva; e
e. participar de qualquer esquema de fraude ou corrupção.

❖ Doações a Candidatos e Partidos Políticos

A Sociedade jamais fará doações a candidatos ou partidos políticos, seja diretamente ou por empresas do grupo. As doações individuais dos colaboradores também devem obedecer rigorosamente à legislação em vigor.

❖ Relacionamentos com Agentes Públicos

Em eventuais encontros com Agentes Públicos, a Sociedade se fará representar, sempre que possível, por ao menos dois representantes. Todas as interações deverão ser registradas (agenda, participantes, assuntos tratados) e reportadas ao Diretor de Compliance, Risco e PLD.

❖ Canal de Denúncia

A Sociedade disponibiliza canal de denúncia acessível a todos os Colaboradores e terceiros interessados, garantindo anonimato, confidencialidade e proteção contra retaliação.

Canal de Compliance e Ouvidoria está disponível na página: https://www.vinocapital.com.br/

❖ Treinamentos

A Sociedade promoverá treinamentos anuais e obrigatórios sobre anticorrupção para todos os Colaboradores, bem como treinamentos extraordinários sempre que houver alterações regulatórias relevantes ou incidentes que justifiquem reforço. Os treinamentos abordarão, no mínimo: (i) a Lei Anticorrupção; (ii) o Código de Conduta da Sociedade; (iii) os canais de denúncia; e (iv) as medidas disciplinares aplicáveis em caso de violação desta Política.

❖ Investigações e Sanções

Todas as denúncias de práticas corruptas serão apuradas pela Sociedade, por meio do Diretor de Compliance, Risco e PLD. Confirmada a ocorrência, serão aplicadas as medidas disciplinares cabíveis (advertência, suspensão, rescisão contratual ou demissão por justa causa), sem prejuízo das responsabilidades civis,

administrativas e criminais. A Sociedade comunicará às autoridades competentes (tais como Ministério Público, CVM, CGU ou outros órgãos aplicáveis) os casos em que haja obrigação legal ou relevância material.

- ❖ Revisão e Atualização

A presente Política será revisada anualmente ou sempre que houver alterações relevantes na legislação ou nas práticas internas, de modo a assegurar sua efetividade e aderência às melhores práticas de mercado.

POLÍTICAS DE TREINAMENTO

- Abrangência e Importância

A Sociedade reconhece a importância de capacitar continuamente seus Colaboradores quanto aos princípios éticos, às normas legais e regulatórias e às políticas internas que norteiam suas atividades. Para tanto, mantém programa de treinamento obrigatório que compreende:

a. Treinamento inicial: aplicável a todos os novos Colaboradores no momento de sua admissão;
b. Reciclagem anual: para atualização contínua;
c. Treinamentos extraordinários: sempre que houver alterações regulatórias relevantes ou necessidades identificadas pelo Diretor de Compliance, Risco e PLD.

- Conteúdo Essencial

Os treinamentos abordarão, no mínimo:

a. Princípios Éticos e de Conduta: código de conduta, valores e responsabilidades dos Colaboradores;
b. Normas de Compliance: regras e procedimentos para garantir a conformidade com leis e regulamentações;
c. Políticas de Segregação: medidas para prevenir conflitos de interesse, conforme aplicável;
d. Confidencialidade, Segurança da Informação e Segurança Cibernética: proteção de dados e Informações Confidenciais da Sociedade;
e. Código de Ética e Política de Negociação: diretrizes para o comportamento dos Colaboradores;
f. Penalidades por descumprimento das regras: medidas disciplinares cabíveis; e
g. Leis e normas aplicáveis: legislação relevante para as atividades da Sociedade.

- Responsabilidades e Implementação

Compete ao Diretor de Compliance, Risco e PLD:

a. planejar e implementar o programa de treinamentos, definindo conteúdo, periodicidade e metodologia;
b. garantir a participação obrigatória dos Colaboradores, mantendo registros formais de presença e aproveitamento; e
c. contratar, quando necessário, profissionais especializados para ministrar treinamentos específicos.

- Dever dos Colaboradores

Todos os Colaboradores devem participar ativamente dos treinamentos, aplicar os conhecimentos no exercício de suas funções e adotar conduta compatível com os valores e normas da Sociedade. O não cumprimento das obrigações de participação poderá ser considerado falta disciplinar.

POLÍTICA DE CERTIFICAÇÃO

- Visão Geral

A Sociedade, na qualidade de gestora de recursos de terceiros, observa integralmente o disposto no Código de Certificação da ANBIMA. Nesse sentido, todos os Colaboradores que detenham poder de decisão de investimentos e desinvestimentos nos fundos sob gestão devem possuir a Certificação ANBIMA aplicável, atualmente a CGE – Certificação de Gestores ANBIMA, válida e ativa, ou outra certificação que venha a ser exigida pela regulação ou autorregulação para as atividades exercidas.

- Identificação de Profissionais Certificados

Antes da contratação, o Diretor de Compliance, Risco e PLD avaliará: (i) a necessidade de certificação em função do cargo e das atribuições do potencial colaborador; e (ii) a comprovação da certificação aplicável (ou isenção), que deverá ser entregue e arquivada em meio físico ou eletrônico, como condição prévia à admissão.

- Rotinas de Verificação

Anualmente, o Diretor de Compliance, Risco e PLD verificará a validade e vigência das certificações dos Colaboradores, bem como eventuais alterações de funções que demandem atualização da certificação.

Quando necessário, o Colaborador será notificado para regularização ou renovação antes do vencimento, sendo certo que:

a. Colaboradores sem certificação válida não podem exercer atividades de gestão com poder de decisão;
b. irregularidades na certificação ensejarão afastamento imediato e apuração de responsabilidades.

- Treinamento e Afastamento

Assuntos de certificação serão abordados no treinamento anual de Compliance. Adicionalmente, no ingresso de cada Colaborador, este terá a oportunidade de esclarecer dúvidas com o Diretor de Compliance, Risco e PLD sobre a certificação exigida.

Profissionais não certificados ou com certificação vencida serão afastados imediatamente das atividades elegíveis até a regularização. Profissionais desligados da Sociedade deverão assinar termo específico de afastamento, conforme modelo constante do Anexo IV.