TRÍTONO
CAPITAL

MANUAL DE COMPLIANCE, REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

TRÍTONO CAPITAL GESTÃO DE RECURSOS LTDA.

CNPJ: 62.955.469/0001-31
Endereço: Rua Potiguar Medeiros, S/N, Pinheiros, São Paulo/SP, CEP 05422-100
Versão: 1.1
Data de Aprovação: Janeiro de 2026
Responsável: Diretoria

CONTROLE DE VERSÕES:

Versão	Data	Responsável	Aprovação
1.1	Janeiro/2026	Diretoria	Diretoria

SUMÁRIO

1. INTRODUÇÃO

A Trítono Capital Gestão de Recursos Ltda. ("Trítono Capital" ou "Gestora") é uma gestora de recursos independente constituída com foco exclusivo na gestão de Fundos de Investimento em Participações (FIPs), destinados a investidores qualificados e profissionais.

Este Manual de Compliance, Regras, Procedimentos e Controles Internos estabelece as diretrizes, procedimentos e controles necessários para assegurar o cumprimento das obrigações regulamentares e o adequado funcionamento das atividades da Gestora, em conformidade com a Resolução CVM nº 21, de 25 de fevereiro de 2021, e suas alterações posteriores, bem como com o Código ANBIMA de Administração e Gestão de Recursos de Terceiros e demais normas aplicáveis.

O presente Manual tem por objetivo estabelecer a estrutura de controles internos da Gestora, definir responsabilidades e atribuições dos colaboradores, implementar procedimentos de compliance e gestão de riscos, assegurar o cumprimento das obrigações regulamentares, proteger os interesses dos investidores e da Gestora, e promover a transparência e a integridade das operações.

A Gestora possui credenciamento perante a CVM e aderência aos Códigos ANBIMA de Autorregulação, desenvolvendo suas atividades em conformidade com a regulamentação aplicável ao mercado de capitais brasileiro.

Todos os colaboradores, prestadores de serviços e terceiros que atuem em nome da Gestora devem conhecer e cumprir integralmente as disposições deste Manual, sendo obrigatória a assinatura de termo de ciência e aderência.

2. DEFINIÇÕES GERAIS

Para os fins deste Manual, aplicam-se as seguintes definições:

Administração de Carteiras de Valores Mobiliários: Atividade que consiste no exercício profissional de atividades relacionadas, direta ou indiretamente, ao funcionamento, à manutenção e à gestão de uma carteira de valores mobiliários, incluindo a aplicação de recursos financeiros no mercado de valores mobiliários por conta do investidor.

ANBIMA: Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.

Ativos Financeiros: Bens e direitos de qualquer natureza, valores mobiliários e ativos financeiros definidos pela Comissão de Valores Mobiliários e/ou pelo Banco Central do Brasil.

Colaboradores: Todas as pessoas físicas que prestam serviços à Trítono Capital, incluindo sócios, diretores, administradores, funcionários, estagiários e prestadores de serviços contratados.

Comitê de Compliance, Risco e PLD: Órgão colegiado permanente da Gestora responsável pela supervisão das atividades de compliance, gestão de riscos e prevenção à lavagem de dinheiro, composto por membros permanentes e eventuais conforme definido nas políticas vigentes da Gestora.

Compliance: Conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

Conflito de Interesses: Situação em que os interesses pessoais, profissionais ou comerciais de um colaborador possam interferir ou parecer interferir com os interesses da Gestora ou de seus investidores.

Controles Internos: Conjunto de regras, procedimentos, diretrizes e estruturas estabelecidas para assegurar que os objetivos da instituição sejam atingidos, que as informações financeiras sejam confiáveis e que as leis e regulamentos sejam cumpridos.

CVM: Comissão de Valores Mobiliários.

FIP: Fundo de Investimento em Participações.
Gestora: Trítono Capital Gestão de Recursos Ltda.

Informação Privilegiada: Informação relevante sobre valores mobiliários ou seus emissores que não tenha sido divulgada ao mercado e que seja capaz de influenciar de modo ponderável a cotação dos valores mobiliários ou a decisão dos investidores.

Investidor Qualificado: Investidor que se enquadra nas definições do artigo 9º-A da Instrução CVM nº 539, de 13 de novembro de 2013.

Investidor Profissional: Investidor que se enquadra nas definições do artigo 9º da Instrução CVM nº 539, de 13 de novembro de 2013.

PLD/FTP: Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

Participações Societárias: Investimentos em quotas ou ações de empresas, representando participação no capital social de sociedades empresárias.

Private Equity: Modalidade de investimento em participações societárias de empresas com potencial de crescimento, envolvendo gestão ativa e estratégias de criação de valor.

3. ABRANGÊNCIA

Este Manual aplica-se a todos os colaboradores da Gestora, incluindo diretores, funcionários, estagiários, consultores e prestadores de serviços que tenham acesso a informações da Gestora ou que atuem em seu nome.

As disposições deste Manual estendem-se a todas as atividades desenvolvidas pela Gestora, especialmente a gestão de Fundos de Investimento em Participações, análise de oportunidades de investimento, *due diligence* de empresas-alvo, monitoramento de investimentos, exercício de direitos societários, relacionamento com investidores, e demais atividades correlatas.

A Gestora atua exclusivamente na gestão de FIPs destinados a investidores qualificados e profissionais, não desenvolvendo atividades de distribuição de produtos de investimento ou outras modalidades de gestão de recursos.

4. IMPLEMENTAÇÃO E REVISÃO

A implementação deste Manual se dará de forma imediata após sua aprovação pela Diretoria da Gestora. Todos os colaboradores devem tomar conhecimento de suas disposições e assinar termo de ciência e aderência.

Este Manual será revisado anualmente ou sempre que houver alterações na regulamentação aplicável, mudanças na estrutura organizacional da Gestora, ou identificação de necessidades de aprimoramento nos controles internos.

As revisões serão coordenadas pelo Diretor de Compliance e aprovadas pela Diretoria, sendo comunicadas tempestivamente a todos os colaboradores e prestadores de serviços relevantes.

5. RESPONSABILIDADE

Compete ao Diretor de Compliance a gestão e aplicação deste Manual, incluindo a supervisão do cumprimento de suas disposições, o treinamento de colaboradores, a investigação de violações, a elaboração de relatórios de compliance, e a coordenação do Comitê de Compliance, Risco e PLD.

O Comitê de Compliance, Risco e PLD é responsável pela supervisão das atividades de compliance, gestão de riscos e PLD/FTP, análise de situações críticas, definição de diretrizes estratégicas, e aprovação de políticas e procedimentos relacionados às suas áreas de competência.

A Diretoria é responsável pela aprovação e revisão deste Manual, bem como pela definição da estratégia de compliance da Gestora e pela alocação de recursos adequados para sua implementação.

Todos os colaboradores são responsáveis por conhecer e cumprir as disposições deste Manual, reportar violações ou suspeitas de violações, e cooperar com investigações de compliance.

6. ENDEREÇO ELETRÔNICO

Para comunicações relacionadas a compliance, dúvidas sobre este Manual, ou reportes de violações, deve ser utilizado o seguinte endereço eletrônico:

E-mail: compliance@tritonocapital.com.br

As comunicações serão tratadas com confidencialidade e investigadas adequadamente conforme a natureza da questão reportada.

7. RISCOS DE COMPLIANCE

A Gestora identifica e monitora os seguintes riscos de compliance relacionados às suas atividades:

7.1. Riscos Regulamentares

Descumprimento da Regulamentação CVM: Risco de violação das disposições da Resolução CVM nº 21/2021 e demais normas aplicáveis à gestão de recursos, incluindo requisitos de estrutura, controles internos, e prestação de informações.

Não Conformidade com Códigos ANBIMA: Risco de descumprimento do Código ANBIMA de Administração e Gestão de Recursos de Terceiros e demais códigos de autorregulação aplicáveis.

Violação de Normas de Mercado: Risco de descumprimento de normas relacionadas ao uso de informação privilegiada, manipulação de mercado, e outras práticas vedadas.

7.2. Riscos Operacionais

Conflitos de Interesse: Risco de situações em que os interesses pessoais dos colaboradores conflitem com os interesses da Gestora ou dos investidores dos FIPs.

Falhas em Controles Internos: Risco de inadequação ou falha na implementação de controles internos, resultando em perdas ou violações regulamentares.

Segregação Inadequada de Funções: Risco de concentração inadequada de responsabilidades ou falta de segregação entre atividades de gestão e controle.

7.3. Riscos de Informação

Vazamento de Informações Confidenciais: Risco de divulgação inadequada de informações sobre investidores, estratégias de investimento, ou empresas investidas.

Uso Inadequado de Informação Privilegiada: Risco de utilização de informações privilegiadas para benefício próprio ou de terceiros.

Falhas na Proteção de Dados: Risco de violação da Lei Geral de Proteção de Dados (LGPD) no tratamento de dados pessoais de investidores e colaboradores.

7.4. Riscos de Terceiros

Prestadores de Serviços Inadequados: Risco de contratação de prestadores de serviços que não atendam aos padrões de qualidade e compliance exigidos.

Falhas de Terceirizados: Risco de falhas ou violações por parte de prestadores de serviços que possam impactar a Gestora.

8. ESTRUTURA DE CONTROLES INTERNOS

8.1. Ambiente de Controle: A Gestora mantém ambiente de controle que promove a integridade, a ética e a competência, estabelecendo a base para todos os outros componentes dos controles internos.

Cultura Organizacional: A Gestora promove cultura organizacional baseada na ética, transparência e cumprimento de normas, com liderança comprometida com os mais altos padrões de conduta.

Estrutura Organizacional: A Gestora mantém estrutura organizacional clara, com definição adequada de responsabilidades, autoridades e linhas de reporte.

Políticas e Procedimentos: A Gestora estabelece políticas e procedimentos abrangentes que orientam as atividades dos colaboradores e asseguram o cumprimento de obrigações.

8.2. Avaliação de Riscos: A Gestora implementa processo sistemático de identificação, avaliação e tratamento de riscos que possam impactar o alcance de seus objetivos.

Identificação de Riscos: Processo contínuo de identificação de riscos internos e externos que possam afetar as atividades da Gestora.

Avaliação de Riscos: Análise da probabilidade e impacto dos riscos identificados, considerando a efetividade dos controles existentes.

Tratamento de Riscos: Implementação de controles e medidas para mitigar, transferir, aceitar ou evitar os riscos identificados.

8.3. Atividades de Controle: A Gestora estabelece atividades de controle em todos os níveis organizacionais e para todos os processos críticos.

Controles Preventivos: Controles projetados para prevenir a ocorrência de eventos indesejados, incluindo aprovações, autorizações e segregação de funções.

Controles Detectivos: Controles projetados para identificar eventos indesejados após sua ocorrência, incluindo reconciliações, revisões e monitoramento.

Controles Corretivos: Controles projetados para corrigir eventos indesejados identificados, incluindo ações corretivas e planos de melhoria.

8.4. Informação e Comunicação: A Gestora assegura que informações relevantes sejam identificadas, capturadas e comunicadas de forma tempestiva e adequada.

Sistemas de Informação: Sistemas adequados para captura, processamento e reporte de informações necessárias para as atividades da Gestora.

Comunicação Interna: Canais efetivos de comunicação interna para assegurar que todos os colaboradores recebam informações necessárias.

Comunicação Externa: Processos adequados para comunicação com investidores, reguladores e outros stakeholders externos.

8.5. Monitoramento: A Gestora implementa atividades de monitoramento para avaliar a efetividade dos controles internos ao longo do tempo.

Monitoramento Contínuo: Atividades de monitoramento incorporadas aos processos regulares da Gestora.

Avaliações Independentes: Avaliações periódicas da efetividade dos controles internos por parte de auditores internos ou externos.

Deficiências e Ações Corretivas: Processo para identificação, comunicação e correção de deficiências nos controles internos.

9. CONTROLES INTERNOS E COMPLIANCE

9.1. Função de Compliance: A função de compliance da Gestora é exercida pelo Diretor de Compliance, que atua de forma independente e reporta-se diretamente à Diretoria.

Independência: O Diretor de Compliance mantém independência funcional em relação às atividades operacionais de gestão de investimentos.

Recursos Adequados: A Gestora assegura que a função de compliance disponha de recursos humanos, tecnológicos e financeiros adequados.

Acesso a Informações: O Diretor de Compliance tem acesso irrestrito a todas as informações necessárias para o exercício de suas funções.

9.2. Responsabilidades de Compliance

Desenvolvimento de Políticas: Elaboração e atualização de políticas e procedimentos de compliance.

Monitoramento: Monitoramento contínuo do cumprimento de normas regulamentares e políticas internas.

Treinamento: Desenvolvimento e implementação de programas de treinamento em compliance.

Investigação: Investigação de violações ou suspeitas de violações de normas e políticas.

Reporte: Elaboração de relatórios periódicos sobre atividades de compliance para a Diretoria.

Coordenação do Comitê: Coordenação das atividades do Comitê de Compliance, Risco e PLD, incluindo convocação de reuniões, elaboração de pautas, e acompanhamento da implementação de decisões.

Apresentação ao Comitê: Apresentação regular de relatórios e situações relevantes ao Comitê para análise e deliberação.

9.3. Programa de Compliance: A Gestora mantém programa abrangente de compliance que inclui:

Código de Ética: Estabelecimento de padrões éticos e de conduta para todos os colaboradores.

Políticas Específicas: Desenvolvimento de políticas específicas para áreas de risco, incluindo conflitos de interesse, informação privilegiada, e investimentos pessoais.

Controles de Acesso: Implementação de controles de acesso a informações confidenciais e sistemas críticos.

Monitoramento de Transações: Monitoramento de transações e atividades para identificação de irregularidades.

Canal de Denúncias: Estabelecimento de canal confidencial para reporte de violações ou suspeitas.

10. SEGREGAÇÃO ESTRUTURAL E DE FUNÇÕES

10.1. Princípios de Segregação: A Gestora implementa adequada segregação de atribuições e funções para prevenir conflitos de interesse e assegurar a efetividade de controles adequados, considerando sua estrutura enxuta.

Segregação entre Gestão e Controle: Separação clara entre atividades de gestão de investimentos e atividades de controle e compliance.

Segregação de Responsabilidades: Distribuição adequada de responsabilidades para evitar concentração excessiva de poder.

Supervisão Independente: Implementação de mecanismos de supervisão independente para atividades críticas.

Segregação Funcional: Adoção de regras e procedimentos para evitar conflito de interesses nas atividades desenvolvidas pelos colaboradores da Gestora em atividades não relacionadas ao seu *core business*, sujeita à Política de Segregação de Atividades e Confidencialidade.

10.2. Estrutura Organizacional

Diretoria: Composta pelo Diretor Presidente e Diretor de Compliance, com responsabilidades claramente definidas.

Diretor Presidente: Responsável pela gestão de investimentos, relacionamento com investidores, e decisões estratégicas.

Diretor de Compliance: Responsável por compliance, controles internos, gestão de riscos, e relacionamento regulatório.

Comitê de Gestão de Recursos: órgão responsável por discutir cenários macroeconômicos e setoriais, avaliar oportunidades de investimento, analisar riscos e fornecer subsídios para as decisões de alocação de recursos dos fundos geridos pela Gestora.

Comitê de Compliance: Órgão colegiado permanente responsável pela supervisão das atividades de compliance, gestão de riscos e prevenção à lavagem de dinheiro

10.3. Controles de Segregação

Controles de Acesso: Implementação de controles de acesso baseados em funções e responsabilidades.

Aprovações Cruzadas: Estabelecimento de processos de aprovação que envolvam múltiplas pessoas.

Revisões Independentes: Implementação de revisões independentes para atividades críticas.

Documentação: Manutenção de documentação adequada de responsabilidades e autorizações.

11. GOVERNANÇA

11.1. Estrutura de Governança: A Gestora adota estrutura de governança adequada ao seu porte e complexidade, assegurando supervisão efetiva das atividades e tomada de decisões transparente.

Assembleia de Sócios: Órgão máximo de decisão da Gestora, responsável por decisões estratégicas e aprovação de políticas fundamentais.

Diretoria: Órgão executivo responsável pela gestão das atividades da Gestora e implementação das decisões da Assembleia de Sócios.

11.2. Responsabilidades da Diretoria

Estratégia: Definição da estratégia de negócios e de investimentos da Gestora.

Políticas: Aprovação de políticas e procedimentos internos.

Supervisão: Supervisão das atividades da Gestora e monitoramento de performance.

Compliance: Assegurar o cumprimento de obrigações regulamentares e contratuais.

Gestão de Riscos: Supervisão da gestão de riscos da Gestora.

11.3. Tomada de Decisões

Decisões de Investimento: Processo estruturado para análise e aprovação de investimentos dos FIPs.

Decisões Operacionais: Processos adequados para tomada de decisões operacionais do dia a dia.

Decisões Estratégicas: Processo formal para decisões estratégicas que afetem o direcionamento da Gestora.

11.4. Transparência e Prestação de Contas

Relatórios Gerenciais: Elaboração de relatórios gerenciais regulares para acompanhamento de performance.

Comunicação com Investidores: Manutenção de comunicação regular e transparente com investidores dos FIPs.

Prestação de Contas: Prestação de contas adequada sobre atividades e resultados da Gestora.

11.5. Comitê de Compliance, Risco e PLD

Composição: O Comitê será composto pelos seguintes membros permanentes:

- Diretor de Compliance, Risco e PLD (Coordenador)
- Diretor Presidente
- Membros da Equipe de Compliance, Risco e PLD selecionados pelo Diretor de Compliance

Funcionamento: O Comitê se reunirá sempre que necessário, com quórum mínimo de 2 (dois) membros permanentes, sendo obrigatória a presença do Coordenador. As deliberações serão tomadas por maioria dos membros permanentes presentes, com registro em ata. O Diretor de Gestão não terá poder de voto em matérias estritamente de compliance.

Atribuições: São atribuições do Comitê:

(I) Supervisionar a implementação e o cumprimento das políticas e procedimentos de compliance, risco e PLD/FTP;
(II) Analisar e deliberar sobre situações de conflito de interesse;
(III) Aprovar e revisar periodicamente as políticas e manuais da Gestora;
(IV) Analisar os relatórios de compliance, risco e PLD/FTP;
(V) Deliberar sobre a aplicação de sanções em casos de violações graves;
(VI) Avaliar e aprovar a contratação de prestadores de serviços críticos;
(VII) Acompanhar a evolução do ambiente regulatório e propor ajustes nas políticas internas;
(VIII) Supervisionar o programa de treinamentos em compliance, risco e PLD/FTP.

Independência: O Comitê atua de forma independente em relação às áreas de negócio, reportando-se diretamente à Diretoria Executiva. O Coordenador do Comitê possui autonomia para convocar reuniões extraordinárias.

12. POLÍTICA DE CONFIDENCIALIDADE

12.1. Princípios de Confidencialidade: A Gestora reconhece a importância da proteção de informações confidenciais e implementa controles adequados para assegurar sua confidencialidade, integridade e disponibilidade. Além dos parâmetros aqui definidos, os as regras e procedimentos destinados a assegurar o sigilo de informações está contido na Política de Segurança Cibernética e Proteção de Dados.

Classificação de Informações: Todas as informações são classificadas conforme seu nível de confidencialidade e criticidade.

Acesso Baseado em Necessidade: Acesso a informações confidenciais é concedido apenas com base na necessidade profissional.

Proteção Adequada: Implementação de controles físicos, lógicos e administrativos para proteção de informações.

12.2. Tipos de Informações Confidenciais

Informações de Investidores: Dados pessoais, financeiros e de investimento dos cotistas dos FIPs.

Estratégias de Investimento: Informações sobre estratégias, critérios e processos de investimento da Gestora.

Informações de Empresas Investidas: Dados financeiros, estratégicos e operacionais das empresas em que os FIPs investem.

Informações Privilegiadas: Informações materiais não públicas sobre empresas investidas ou potenciais investimentos.

12.3. Controles de Confidencialidade

Acordos de Confidencialidade: Todos os colaboradores e terceiros assinam acordos de confidencialidade.

Controles de Acesso: Implementação de controles de acesso físico e lógico a informações confidenciais.

Treinamento: Treinamento regular sobre proteção de informações confidenciais.

Monitoramento: Monitoramento de acesso e uso de informações confidenciais.

13. PREVENÇÃO À LAVAGEM DE DINHEIRO

13.1. Programa de PLD/FTP: A Gestora mantém programa robusto de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, em conformidade com a legislação aplicável.

Políticas e Procedimentos: Estabelecimento de políticas e procedimentos específicos para PLD/FTP.

Conhecimento de Investidores: Implementação de procedimentos rigorosos de conhecimento de investidores (*KYClient*).

Monitoramento de Operações: Monitoramento sistemático de operações para identificação de atividades suspeitas.

Comunicação às Autoridades: Procedimentos para comunicação de operações suspeitas às autoridades competentes.

Supervisão pelo Comitê: O programa de PLD/FTP é supervisionado pelo Comitê de Compliance, Risco e PLD, que avalia sua efetividade e determina aprimoramentos quando necessário.

13.2. Conhecimento de Investidores (KYClient)

Identificação: Verificação da identidade dos investidores através de documentos oficiais.

Qualificação: Confirmação da qualificação dos investidores conforme regulamentação aplicável.

Origem de Recursos: Verificação da origem lícita dos recursos a serem investidos.

Perfil de Risco: Avaliação do perfil de risco de PLD/FTP de cada investidor.

13.3. Monitoramento de Operações

Operações Atípicas: Identificação e análise de operações que fujam do padrão normal dos investidores.

Operações Suspeitas: Identificação de operações que possam caracterizar lavagem de dinheiro ou financiamento ao terrorismo.

Registros e Controles: Manutenção de registros adequados de todas as operações monitoradas.

Comunicação: Comunicação tempestiva de operações suspeitas ao COAF.

14. CONHECIMENTO DE INVESTIDORES E CONTRAPARTE

14.1. Procedimentos de Conhecimento: A Gestora implementa procedimentos abrangentes de conhecimento de investidores e terceiros, adequados ao perfil de investidores qualificados e profissionais dos FIPs.

***Due Diligence* de Investidores:** Processo estruturado de análise e verificação de informações dos investidores.

Documentação Obrigatória: Coleta e verificação de documentação necessária para conhecimento adequado.

Atualização Periódica: Atualização regular das informações de investidores e terceiros.

Arquivo de Documentos: Manutenção de arquivo organizado de toda a documentação coletada.

14.2. Critérios de Aceitação

Investidores Qualificados: Verificação do enquadramento como investidor qualificado conforme regulamentação.

Investidores Profissionais: Verificação do enquadramento como investidor profissional conforme regulamentação.

Origem de Recursos: Confirmação da origem lícita dos recursos a serem investidos.

Adequação ao Perfil: Verificação da adequação do investidor ao perfil e estratégia dos FIPs.

14.3. Monitoramento Contínuo

Acompanhamento de Investidores: Monitoramento contínuo do perfil e atividades dos investidores.

Identificação de Mudanças: Identificação de mudanças significativas no perfil ou situação dos investidores.

Ações Corretivas: Implementação de ações corretivas quando necessário.

Relatórios: Elaboração de relatórios periódicos sobre o perfil da base de investidores.

14.4 Conhecimento e Controle de Contrapartes (*KYCounterparty*)

Princípio Geral: A Gestora não se eximirá de realizar o controle de contrapartes para qualquer que seja o ativo e/ou o seu ambiente de negociação. Este controle aplica-se a todas as operações realizadas pelos fundos sob gestão, independentemente do tipo de ativo, mercado ou ambiente de negociação.

Definição de Contraparte: Para fins desta política, considera-se "contraparte" qualquer pessoa física ou jurídica que:

- Seja parte em operações de compra, venda ou transferência de ativos dos fundos geridos;
- Atue como intermediária em operações dos fundos (corretoras, distribuidoras, consultores);
- Seja fornecedora de serviços essenciais relacionados às operações dos fundos;
- Participe de operações societárias envolvendo as empresas investidas (sócios, acionistas, investidores estratégicos);
- Seja parte em acordos de acionistas, contratos de investimento ou desinvestimento;
- Atue como compradora potencial em processos de saída (exit) dos investimentos.

Procedimentos de *Due Diligence* de Contrapartes: A Gestora implementará os seguintes procedimentos de conhecimento de contrapartes (*Know Your Counterparty - KYC*):

1. <u>Identificação e Qualificação</u>:
- Coleta de documentos de identificação (RG, CPF, CNPJ, contrato social);
- Verificação de poderes de representação e procurações;
- Identificação de beneficiários finais (pessoas físicas que detêm controle efetivo);
- Verificação de vínculos com Pessoas Politicamente Expostas (PPE).

2. <u>Análise de Reputação e Histórico:</u>
- Consulta a bases de dados públicas e privadas;
- Verificação de processos judiciais, administrativos e regulatórios;
- Análise de notícias negativas (negative news screening);
- Consulta a listas restritivas nacionais e internacionais (sanções, PEPs, terrorismo).

3. <u>Avaliação de Risco:</u>
- Classificação de risco da contraparte (baixo, médio, alto) com base em critérios objetivos;
- Consideração de fatores como jurisdição, setor de atuação, estrutura societária complexa;

- Identificação de red flags (sinais de alerta) que possam indicar risco de lavagem de dinheiro.

4. Origem dos Recursos:
- Quando aplicável, verificação da origem dos recursos utilizados pela contraparte na operação;
- Análise de compatibilidade entre o patrimônio declarado e a operação proposta;
- Solicitação de declaração de origem lícita dos recursos.

5. Monitoramento Contínuo:
- Atualização periódica das informações cadastrais das contrapartes recorrentes;
- Monitoramento de mudanças significativas na estrutura ou controle da contraparte;
- Reavaliação de risco em caso de eventos relevantes (processos, sanções, mudança de controle).

Aplicação em Operações de FIPs: Considerando a natureza das operações em Fundos de Investimento em Participações, a Gestora aplicará os controles de contrapartes especialmente nas seguintes situações:
- Aquisição de Participações: *Due diligence* dos vendedores (sócios atuais, fundadores, investidores anteriores);
- Operações Societárias: Análise de novos sócios que ingressem nas empresas investidas;
- Desinvestimentos (Exit): *Due diligence* de compradores potenciais (investidores estratégicos, fundos concorrentes, compradores corporativos);
- Operações de Mercado Secundário: Quando aplicável, controle de contrapartes em negociações de cotas dos fundos;
- Prestadores de Serviços: *Due diligence* de assessores financeiros, jurídicos e outros intermediários envolvidos nas operações.

Responsabilidades: O Diretor de Compliance, Risco e PLD é responsável por:
- Coordenar o processo de *due diligence* de contrapartes;
- Aprovar ou vetar operações com base na análise de risco da contraparte;
- Manter registros atualizados das análises realizadas;
- Reportar ao Comitê de Compliance, Risco e PLD situações de alto risco ou red flags identificados;
- Comunicar as autoridades, conforme aplicável, sobre operações suspeitas envolvendo contrapartes.

Documentação e Registros: Todas as análises de contrapartes serão documentadas e arquivadas, incluindo:
- Formulário de cadastro da contraparte;
- Documentos de identificação coletados;
- Relatório de *due diligence* com análise de risco;

- Aprovação ou rejeição da operação com a contraparte;
- Evidências de consultas realizadas (bases de dados, listas restritivas).

A documentação será mantida por prazo mínimo de 5 (cinco) anos após o encerramento do relacionamento com a contraparte, em conformidade com a legislação de PLD/FT.

Integração com Prestadores de Serviços: A Gestora poderá utilizar serviços de terceiros especializados (bureaus de crédito, plataformas de compliance, consultorias) para auxiliar no processo de *due diligence* de contrapartes, sem prejuízo da responsabilidade final da Gestora pela análise e decisão. Quando as operações forem intermediadas por instituições financeiras autorizadas (corretoras, bancos de investimento), a Gestora considerará os controles de PLD/FT já realizados por essas instituições, mas não se eximirá de realizar sua própria análise de risco da contraparte final da operação.

Recusa de Operações: A Gestora se reserva o direito de recusar operações com contrapartes que:

- Não forneçam informações suficientes para o processo de due *diligence*;
- Apresentem alto risco de lavagem de dinheiro ou financiamento do terrorismo;
- Constem em listas restritivas ou apresentem impedimentos regulatórios;
- Não atendam aos padrões de integridade e reputação estabelecidos pela Gestora.

A recusa será documentada e comunicada ao Comitê de Compliance, Risco e PLD.

15. POLÍTICA DE RATEIO DE OPORTUNIDADES

15.1. Princípios de Rateio: A Gestora adota critérios objetivos e transparentes para rateio de oportunidades de investimento entre os FIPs sob sua gestão, assegurando tratamento equitativo.

Equidade: Tratamento equitativo de todos os FIPs na distribuição de oportunidades.

Transparência: Critérios claros e transparentes para rateio de oportunidades.

Documentação: Documentação adequada de todas as decisões de rateio.

Supervisão: Supervisão adequada do processo de rateio pelo Diretor de Compliance e pelo Comitê de Compliance, Risco e PLD, que pode determinar ajustes nos critérios quando necessário.

15.2. Critérios de Rateio

Estratégia de Investimento: Adequação da oportunidade à estratégia específica de cada FIP.

Ticket Mínimo e Máximo: Consideração dos limites de investimento de cada FIP.

Disponibilidade de Recursos: Disponibilidade de recursos para investimento em cada FIP.

Diversificação: Consideração dos objetivos de diversificação de cada FIP.

Timing: Consideração do timing adequado para cada FIP.

15.3. Processo de Rateio

Identificação de Oportunidades: Processo estruturado para identificação e análise de oportunidades.

Avaliação de Adequação: Avaliação da adequação de cada oportunidade aos FIPs.

Decisão de Rateio: Processo formal para decisão sobre rateio de oportunidades.

Documentação: Documentação detalhada das razões para cada decisão de rateio.

Comunicação: Comunicação adequada das decisões aos investidores quando relevante.

15.4. *Soft Dollar*

Regra Geral: A Gestora, como norma geral, proíbe a realização de acordos de Soft Dollar.

Exceções: O recebimento de Soft Dollar é aceitável em exceções, desde que cumulativamente: (a) não afete a capacidade de decisão e a neutralidade da Gestora; (b) não seja imposta nenhuma obrigação de reciprocidade; (c) os benefícios sejam direta ou indiretamente revertidos aos fundos geridos; e (d) no caso de corretoras, os valores sejam justificados pelo montante das comissões pagas.

Processo de Aprovação: Caberá ao Diretor de Compliance, Risco e PLD a responsabilidade por autorizar previamente o recebimento de Soft Dollar, mediante análise documentada.

15.5. *Best Execution*

Compromisso: A Gestora se compromete a assegurar a melhor execução (*best execution*) de ordens para os fundos sob sua gestão, considerando as características específicas dos FIPs.

Princípios Fundamentais: Na avaliação e seleção de prestadores de serviços, a Gestora segue os seguintes princípios: (i) rigorosa observância do dever fiduciário; (ii) capacidade reconhecida de execução e liquidação; (iii) custo-benefício; e (iv) minimização de situações de conflito de interesses.

Aplicação em FIPs: A melhor execução envolve a seleção de assessores financeiros e jurídicos com expertise, negociação de termos adequados e avaliação criteriosa de custos de transação.

16. POLÍTICA DE CERTIFICAÇÃO

16.1. Requisitos de Certificação: A Gestora assegura que todos os profissionais em atividades elegíveis possuam certificações adequadas conforme exigências da ANBIMA.

Identificação de Atividades Elegíveis: Mapeamento de todas as atividades que requerem certificação.

Certificações Necessárias: Identificação das certificações necessárias para cada atividade.

Cronograma de Adequação: Estabelecimento de cronograma para adequação de profissionais.

Monitoramento: Monitoramento contínuo do status de certificações.

16.2. Gestão de Certificações

Controle de Validade: Controle rigoroso das datas de validade das certificações.

Educação Continuada: Acompanhamento do cumprimento de requisitos de educação continuada.

Renovações: Processo para assegurar renovação tempestiva de certificações.

Registros: Manutenção de registros atualizados de todas as certificações.

16.3. Treinamento e Desenvolvimento

Programas de Treinamento: Desenvolvimento de programas de treinamento para preparação para certificações.

Apoio Financeiro: Política de apoio financeiro para obtenção e manutenção de certificações.

Desenvolvimento Profissional: Incentivo ao desenvolvimento profissional contínuo dos colaboradores.

17. PLANO DE CONTINUIDADE DE NEGÓCIOS

Coordenador de Contingência: O Diretor de Compliance, Risco e PLD atuará como Coordenador de Contingência, sendo responsável por avaliar a gravidade da situação, decidir pela ativação do Plano, coordenar as ações de resposta e comunicar todos os envolvidos.

Situações de Ativação: O Plano poderá ser ativado em situações como: (i) Desastres Naturais; (ii) Pandemias ou Crises de Saúde Pública; (iii) Falhas Tecnológicas Graves; (iv) Ausência de Pessoal Crítico; (v) Interrupção de Serviços Essenciais de terceiros.

Prazo de Normalização: Será de responsabilidade do Coordenador de Contingência assegurar que as operações críticas da Gestora (acesso a sistemas, comunicação com prestadores, cumprimento de obrigações regulatórias) voltem à normalidade no mesmo dia útil em que ocorrer a ativação do Plano. Para situações de maior complexidade, o Coordenador deverá estabelecer um plano de recuperação com prazos realistas e comunicar a Diretoria.

Testes e Revisão: O Plano de Continuidade será testado anualmente para verificar sua eficácia, e os resultados serão documentados e utilizados para aprimoramento contínuo.

18. GESTÃO DE RISCOS

18.1. Framework de Gestão de Riscos: A Gestora implementa framework abrangente de gestão de riscos adequado às suas atividades de gestão de FIPs.

Identificação de Riscos: Processo sistemático para identificação de todos os tipos de riscos.

Avaliação de Riscos: Metodologia para avaliação da probabilidade e impacto dos riscos.

Tratamento de Riscos: Estratégias para mitigação, transferência, aceitação ou eliminação de riscos.

Monitoramento: Monitoramento contínuo dos riscos e efetividade dos controles.

18.2. Tipos de Riscos Gerenciados

Riscos de Mercado: Riscos relacionados a variações nos preços de ativos e condições de mercado.

Riscos de Crédito: Riscos relacionados à capacidade de pagamento de devedores e contrapartes.

Riscos de Liquidez: Riscos relacionados à capacidade de liquidar posições quando necessário.

Riscos Operacionais: Riscos relacionados a falhas em processos, pessoas, sistemas ou eventos externos.

Riscos de Compliance: Riscos relacionados ao descumprimento de normas regulamentares ou políticas internas.

18.3. Controles de Riscos

Limites de Exposição: Estabelecimento de limites adequados para diferentes tipos de exposição.

Diversificação: Políticas de diversificação para redução de concentração de riscos.

Monitoramento: Sistemas de monitoramento contínuo de exposições e riscos.

Relatórios: Elaboração de relatórios regulares sobre riscos para a Diretoria.

Supervisão pelo Comitê: Os controles de riscos são supervisionados pelo Comitê de Compliance, Risco e PLD, que avalia sua adequação e efetividade, podendo determinar ajustes quando necessário.

19. SEGURANÇA DA INFORMAÇÃO E TESTES PERIÓDICOS

19.1. Princípios de Segurança da Informação: A Gestora mantém política de segurança cibernética e proteção de dados com intuito de preserva o sigilo de dados confidenciais de investidores, empresas investidas e informações estratégicas, com foco especial em informações mantidas em meio eletrônico. A política baseia-se nos princípios de confidencialidade, integridade, disponibilidade, conformidade regulatória e melhoria contínua.

19.2. Programa de Testes Periódicos de Segurança: A Gestora implementa programa de testes periódicos de segurança para sistemas de informações confidenciais,

abrangendo todos os dispositivos e sistemas utilizados por sócios, administradores, colaboradores e funcionários.

19.2.1. Periodicidade dos Testes

Testes Anuais:

- Auditoria completa de segurança da informação
- Revisão de política de segurança e procedimentos
- Avaliação de conformidade com LGPD e regulamentação CVM
- Análise de efetividade dos controles implementados

Testes Semestrais:

- Testes de vulnerabilidade de sistemas e aplicações
- Varredura de vulnerabilidades em sistemas de armazenamento em nuvem
- Análise de configurações de segurança
- Revisão de permissões de acesso a sistemas e arquivos
- Avaliação de políticas de senha e autenticação

Testes Trimestrais:

- Testes de backup e recuperação de dados
- Validação de integridade de backups armazenados
- Verificação de tempo de recuperação (RTO) e ponto de recuperação (RPO)
- Testes de restauração de arquivos críticos
- Verificação de controles de acesso a sistemas e plataformas
- Revisão de logs de acesso e atividades suspeitas
- Atualização de listas de usuários autorizados
- Verificação de atualizações de segurança instaladas
- Monitoramento de tentativas de acesso não autorizado
- Monitoramento Contínuo:
- Monitoramento de antivírus e antimalware em tempo real
- Alertas de segurança automáticos
- Verificação automática de atualizações de segurança
- Monitoramento de firewall e sistemas de proteção

19.2.2. Escopo dos Testes

Os testes de segurança abrangem:

Sistemas de Armazenamento em Nuvem:

- Google Drive, Google Workspace, Microsoft OneDrive, SharePoint
- Dropbox e outras plataformas de armazenamento
- Sistemas de backup em nuvem
- Plataformas de compartilhamento de arquivos

Sistemas de Comunicação:
- E-mail corporativo
- Sistemas de mensagens instantâneas corporativas
- Plataformas de videoconferência
- Telefonia corporativa

Plataformas de Gestão e Controle:
- Planilhas e modelos proprietários em Excel
- Sistemas de controle de investimentos
- Plataformas de análise financeira
- Sistemas de gestão de documentos
- Ferramentas de modelagem e valuation

Sistemas de Prestadores de Serviços:
- Plataformas do administrador fiduciário
- Sistemas do custodiante
- Portais de escrituração
- Sistemas de contabilidade terceirizada
- Outras plataformas de prestadores críticos
- Dispositivos de Sócios, Administradores, Colaboradores e Funcionários:
- Notebooks corporativos
- Computadores desktop
- Smartphones corporativos ou pessoais utilizados para atividades da Gestora
- Tablets utilizados para acesso a sistemas corporativos
- Dispositivos de armazenamento externo

Infraestrutura de Rede:
- Rede Wi-Fi corporativa
- Roteadores e equipamentos de rede
- Firewalls e sistemas de proteção
- VPN (Virtual Private Network) quando utilizada

19.2.3. Tipos de Testes Realizados

Testes de Vulnerabilidade: Identificação de falhas de segurança em sistemas e aplicações, varredura automatizada de vulnerabilidades conhecidas, análise de configurações inadequadas, identificação de software desatualizado, e relatório de vulnerabilidades por criticidade.

Testes de Controle de Acesso: Verificação de permissões de usuários em sistemas e arquivos, identificação de acessos desnecessários ou excessivos, revisão de usuários inativos, validação de segregação de funções, e testes de autenticação multifator.

Testes de Backup e Recuperação: Validação de integridade de backups realizados, testes de restauração de arquivos individuais e completa de sistemas, verificação de tempo de recuperação e ponto de recuperação, e testes de recuperação em ambiente alternativo.

Testes de Resposta a Incidentes: Simulação de cenários de violação de segurança, testes de procedimentos de contenção e mitigação, validação de comunicação em situações de crise, e avaliação de tempo de resposta a incidentes.

Testes de Conscientização: Avaliação de comportamento de usuários e identificação de necessidades de treinamento adicional.

Testes de Criptografia: Verificação de criptografia de discos rígidos, validação de criptografia de comunicações, testes de criptografia de backups, e verificação de proteção de arquivos sensíveis.

19.2.4. Responsabilidades

Diretor de Compliance, Risco e PLD: Coordenar o programa de testes periódicos de segurança, aprovar o cronograma anual de testes, revisar relatórios de testes realizados, acompanhar implementação de ações corretivas, reportar ao Comitê de Compliance sobre resultados dos testes, e comunicar à Diretoria vulnerabilidades críticas identificadas.

Prestadores de Serviços de TI: Executar os testes técnicos de segurança conforme cronograma, elaborar relatórios detalhados de vulnerabilidades identificadas, recomendar ações corretivas e melhorias, implementar correções aprovadas pela Gestora, e manter documentação técnica atualizada.

Diretoria: Aprovar recursos necessários para o programa de testes, revisar relatórios de testes de segurança, tomar decisões sobre investimentos em segurança, e supervisionar implementação de ações corretivas críticas.

Todos os Colaboradores: Participar de testes de conscientização, reportar imediatamente incidentes de segurança identificados, cooperar com testes e auditorias de segurança, manter dispositivos corporativos atualizados e protegidos, e cumprir políticas de segurança estabelecidas.

19.2.5. Documentação e Registros: Todos os testes de segurança são documentados e os registros mantidos por prazo mínimo de 5 anos, incluindo cronograma de testes com planejamento anual e registro de testes realizados, relatórios técnicos detalhados de cada teste com vulnerabilidades identificadas e classificação de criticidade, planos de ação corretiva com priorização e prazos, evidências de implementação de correções, e relatórios gerenciais trimestrais para a Diretoria com indicadores de segurança.

19.3. Controles de Acesso e Segurança de Dispositivos

19.3.1. Dispositivos Corporativos: Todos os dispositivos corporativos utilizados por sócios, administradores, colaboradores e funcionários devem atender aos seguintes requisitos mínimos de segurança:

Criptografia de Disco: Criptografia completa de disco rígido obrigatória em todos os dispositivos que armazenam informações da Gestora, com verificação semestral de status de criptografia.

Proteção contra Malware: Antivírus corporativo instalado e atualizado automaticamente, varredura em tempo real ativa, varredura completa semanal agendada, e proteção contra ransomware.

Firewall e Atualizações: Firewall do sistema operacional ativo, atualizações automáticas de sistema operacional ativadas, instalação de patches de segurança críticos em até 7 dias, e verificação mensal de software desatualizado.

Autenticação: Senhas fortes obrigatórias (mínimo 12 caracteres com letras maiúsculas, minúsculas, números e símbolos), autenticação de dois fatores obrigatória para sistemas críticos, bloqueio automático de tela após 10 minutos de inatividade, e proibição de compartilhamento de credenciais.

Controle de Acesso Físico: Proteção física de dispositivos, procedimento de bloqueio remoto em caso de perda ou roubo, possibilidade de limpeza remota de dados corporativos, e registro de dispositivos corporativos com número de série e responsável.

19.3.2. Política BYOD (*Bring Your Own Device*): Quando colaboradores utilizarem dispositivos pessoais para atividades da Gestora, devem atender aos mesmos requisitos de segurança dos dispositivos corporativos, incluindo separação de dados pessoais e corporativos, criptografia de dados corporativos, autenticação forte para acesso a sistemas da Gestora, e aceitação de possibilidade de limpeza remota apenas de dados corporativos.

Restrições aplicáveis incluem proibição de armazenamento de informações confidenciais em dispositivos pessoais não protegidos, obrigatoriedade de uso de aplicativos corporativos para comunicação sensível, e proibição de uso de redes Wi-Fi públicas sem VPN para acesso a sistemas corporativos.

19.3.3. Acesso Remoto: Acesso remoto a sistemas da Gestora deve seguir controles específicos, incluindo uso obrigatório de VPN quando aplicável, autenticação multifator para conexão VPN e acesso a sistemas em nuvem, monitoramento de conexões e acessos remotos, e logs de acesso remoto mantidos por 12 meses.

Para trabalho remoto, aplicam-se orientações específicas incluindo proibição de uso de computadores compartilhados ou públicos, uso de conexões seguras, e proteção física de documentos impressos em ambiente doméstico.

19.4. Gestão de Incidentes de Segurança

19.4.1. Definição de Incidente de Segurança: Considera-se incidente de segurança qualquer evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade de informações da Gestora, incluindo acesso não autorizado a informações confidenciais, vazamento de dados, perda ou roubo de dispositivos, alteração não autorizada de dados, indisponibilidade de sistemas críticos, infecção por vírus ou malware, e tentativas de phishing bem-sucedidas.

19.4.2. Processo de Resposta a Incidentes: O processo de resposta a incidentes compreende:

Identificação e Classificação: Detecção do incidente, classificação de criticidade (crítica, alta, média, baixa), acionamento imediato do Diretor de Compliance para incidentes críticos ou altos, e documentação inicial do incidente.

Contenção e Mitigação Imediata: Isolamento de sistemas afetados, bloqueio de acessos comprometidos, mudança de senhas quando aplicável, desconexão de dispositivos infectados da rede, e ativação de backups para restauração quando necessário.

Investigação e Análise: Análise de causa raiz do incidente, identificação de extensão do comprometimento, coleta de evidências técnicas, avaliação de impacto, e determinação de responsabilidades.

Comunicação: Comunicação imediata à Diretoria para incidentes críticos, avaliação de necessidade de comunicação a investidores afetados, comunicação à ANPD quando aplicável conforme LGPD, comunicação a autoridades reguladoras quando exigido, e comunicação a prestadores de serviços afetados.

Implementação de Medidas Corretivas: Correção de vulnerabilidades que permitiram o incidente, implementação de controles adicionais para prevenção, atualização de políticas e procedimentos, treinamento adicional de colaboradores quando aplicável, e melhoria de sistemas de detecção e resposta.

Documentação e Lições Aprendidas: Relatório completo do incidente com cronologia detalhada, análise de efetividade da resposta, identificação de melhorias necessárias, atualização de procedimentos de resposta a incidentes, e compartilhamento de lições aprendidas com a equipe.

19.4.3. Prazos de Resposta

Incidentes Críticos (vazamento de dados, ransomware, acesso não autorizado a sistemas críticos): Contenção imediata (até 1 hora), comunicação à Diretoria imediata (até 2 horas), investigação inicial (até 24 horas), e plano de ação (até 48 horas).

Incidentes Altos (tentativa de phishing bem-sucedida, perda de dispositivo): Contenção (até 4 horas), comunicação à Diretoria (até 24 horas), investigação (até 3 dias úteis), e plano de ação (até 5 dias úteis).

Incidentes Médios e Baixos: Tratamento conforme cronograma regular de segurança, com documentação e análise em até 10 dias úteis.

19.5. Treinamento e Conscientização

19.5.1. Programa de Treinamento: Todos os colaboradores recebem treinamento periódico sobre segurança da informação:

Treinamento Inicial (na admissão): Políticas de segurança da informação da Gestora, boas práticas de segurança, identificação de tentativas de phishing e engenharia social, procedimentos de resposta a incidentes, e responsabilidades individuais.

Treinamento Anual (todos os colaboradores): Atualização sobre novas ameaças e tipologias de ataques, revisão de políticas e procedimentos, casos práticos e lições aprendidas, simulação de cenários de incidentes, e avaliação de conhecimento.

Treinamento Específico (para funções críticas): Diretor de Compliance recebe treinamento em gestão de incidentes e conformidade LGPD. Equipe de TI recebe treinamento em resposta técnica a incidentes e testes de segurança. Todos recebem treinamento sobre proteção de informações confidenciais de investidores.

19.5.2. Campanhas de Conscientização: A Gestora realiza campanhas periódicas de conscientização incluindo e-mails mensais com dicas de segurança, alertas sobre novas ameaças identificadas, lembretes sobre boas práticas, divulgação de resultados de testes de conscientização, simulação trimestral de e-mails de phishing, avaliação de taxa de cliques em links suspeitos, e feedback individual para colaboradores que falharam nos testes.

19.6. Conformidade com LGPD: A Gestora mantém conformidade com a Lei Geral de Proteção de Dados em todas as atividades de tratamento de dados pessoais, aplicando os princípios de finalidade, adequação, necessidade, transparência e segurança. A Gestora respeita os direitos dos titulares de dados incluindo confirmação de existência de

tratamento, acesso aos dados pessoais, correção de dados, anonimização ou eliminação de dados, portabilidade de dados, e informação sobre compartilhamento de dados.

As medidas de segurança para proteção de dados pessoais incluem criptografia de dados sensíveis, controles de acesso baseados em necessidade, anonimização quando possível, registro de operações de tratamento, e avaliação de impacto à proteção de dados quando aplicável.

19.7. Referência à Política Específica: Além das regras previstas neste Manual, os procedimentos técnicos e operacionais detalhados de segurança cibernética e proteção de dados estão estabelecidos na Política de Segurança Cibernética e Proteção de Dados , que complementa e detalha as diretrizes desta seção. Tal Política aborda de forma aprofundada arquitetura de segurança de sistemas e redes, procedimentos técnicos de testes de segurança, gestão de vulnerabilidades e patches, segurança de aplicações e desenvolvimento, continuidade de negócios e recuperação de desastres, conformidade com regulamentações de proteção de dados, e outros aspectos técnicos de segurança cibernética.

19.8. Revisão e Atualização: A política de segurança da informação é revisada anualmente ou sempre que houver mudanças significativas em sistemas ou infraestrutura, identificação de novas ameaças ou vulnerabilidades, incidentes de segurança relevantes, mudanças na regulamentação aplicável, ou recomendações de auditorias ou testes de segurança. A revisão é coordenada pelo Diretor de Compliance, com apoio de prestadores de serviços de TI, e aprovada pela Diretoria.

20. DISPOSIÇÕES GERAIS

20.1. Vigência: Este Manual entra em vigor na data de sua aprovação pela Diretoria e permanece válido até sua revogação ou substituição por versão atualizada.

20.2. Atualizações: Este Manual será atualizado sempre que necessário para refletir mudanças na regulamentação, na estrutura da Gestora, ou nas melhores práticas de mercado.

20.3. Treinamento: Todos os colaboradores devem receber treinamento adequado sobre as disposições deste Manual e suas atualizações.

O processo de treinamento inicial dos colaboradores da Trítono Capital ocorre no momento de sua admissão e tem como objetivo assegurar o conhecimento adequado das políticas internas, da regulamentação aplicável e das responsabilidades associadas às funções desempenhadas.

O treinamento inicial abrange, no mínimo:

(i) apresentação da estrutura organizacional da gestora;

(ii) leitura e explicação das políticas internas vigentes, incluindo, entre outras, as políticas de controles internos, gestão de riscos, compliance e prevenção à lavagem de dinheiro;
(iii) orientações sobre conduta ética, confidencialidade das informações e prevenção de conflitos de interesse.

Adicionalmente, a Trítono Capital mantém programa de reciclagem periódica, realizado, no mínimo, anualmente, ou sempre que houver alterações relevantes na regulamentação ou nas políticas internas. O programa de reciclagem consiste em sessões internas de atualização, comunicados formais e revisões dirigidas das políticas aplicáveis, sendo conduzido pelo Diretor de Compliance ou por profissional por ele designado.

O controle do treinamento inicial e reciclagem é feito por meio de um sistema proprietário que inclui um checklist das obrigações de leitura e adesão às políticas vigentes no início das atividades de cada colaborador, assim como as reciclagens periódicas.

A participação dos colaboradores nos treinamentos iniciais e nas reciclagens periódicas é registrada e arquivada em meio eletrônico, com indicação da data, conteúdo abordado e participantes.

20.4. Sanções: O descumprimento das disposições deste Manual pode resultar em medidas disciplinares, incluindo advertência, suspensão ou desligamento, conforme a gravidade da violação.

20.5. Casos Omissos: Casos omissos ou situações não previstas neste Manual devem ser submetidos ao Diretor de Compliance para análise inicial. Casos de maior complexidade ou relevância devem ser levados ao Comitê de Compliance, Risco e PLD para deliberação.

20.6. Integração com Outras Políticas: Este Manual deve ser lido em conjunto com outras políticas internas da Gestora, incluindo o Código de Ética, políticas específicas de gestão de riscos, e demais documentos regulatórios.

Aprovado pela Diretoria da Trítono Capital Gestão de Recursos Ltda.
São Paulo, Janeiro de 2026

Daniel Teruo Famano
Diretor Presidente

Guilherme Maitto Caputo
Diretor de Compliance