TRÍTONO
CAPITAL

POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E CONFIDENCIALIDADE

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: 1.0
Data de Aprovação: Fevereiro de 2026
Responsável: Diretoria

CONTROLE DE VERSÕES:

Versão	Data	Responsável	Aprovação
1.1	Fevereiro/2026	Diretoria	Diretoria

SUMÁRIO

1. INTRODUÇÃO
2. ABRANGÊNCIA
3. IMPLEMENTAÇÃO E REVISÃO
4. RESPONSABILIDADES
5. ENDEREÇO ELETRÔNICO
6. SEGREGAÇÃO DE COMPLIANCE
7. CHINESE WALL E SEGREGAÇÃO DE FUNÇÕES
8. CONFLITOS DE INTERESSES
9. POLÍTICA DE CONFIDENCIALIDADE
10. DISPOSIÇÕES GERAIS

1. INTRODUÇÃO

A Política de Segregação de Atividades e Confidencialidade da Trítono Capital Gestão de Recursos Ltda. ("Trítono Capital" ou "Gestora") visa estabelecer as orientações necessárias para garantir as devidas segregações de atividades e a confidencialidade necessária ao atendimento das funções da Gestora, em conformidade com o artigo 28, incisos I e II, da Resolução CVM nº 21/2021.

Por intermédio deste instrumento, visa-se o atendimento integral e ininterrupto às normas, políticas e regulamentações vigentes, promovendo a transparência na condução dos negócios, a salvaguarda da confidencialidade das informações outorgadas pelos investidores, a eliminação de conflitos de agência entre os diversos atores da entidade, evitando ganhos pessoais indevidos por meio da criação de condições artificiais de mercado ou da manipulação e uso de informação privilegiada.

Esta política foi desenvolvida para o cumprimento das obrigações estabelecidas pelas Instruções da Comissão de Valores Mobiliários, especialmente a Resolução CVM nº 21/2021, pela legislação aplicável e demais práticas nacionais e internacionais aplicadas à política de compliance, considerando as especificidades da gestão de Fundos de Investimento em Participações.

A Gestora reconhece que a adequada segregação de atividades e a manutenção da confidencialidade são elementos fundamentais para a proteção dos investidores e a integridade do mercado de capitais, especialmente no contexto de investimentos em participações societárias onde o acesso a informações privilegiadas é frequente.

2. ABRANGÊNCIA

Esta política é aplicável a todos os administradores, colaboradores, estagiários, terceirizados e prestadores de serviços envolvidos com negócios e atividades da Gestora, bem como aos sócios controladores da Gestora.

A política abrange todas as atividades desenvolvidas pela Gestora, incluindo:

- 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
- Atividades de compliance e controles internos
- Gestão de riscos
- Outras atividades correlatas

A aplicação desta política estende-se também às informações e atividades relacionadas a empresas investidas, potenciais investimentos, estratégias de investimento, informações de investidores e demais dados confidenciais sob responsabilidade da Gestora.

3. IMPLEMENTAÇÃO E REVISÃO

3.1. Implementação: A implementação desta política se dará de forma imediata após a aprovação da Diretoria e será comunicada a todos os colaboradores e prestadores de serviços relevantes.

3.2. Revisão: Esta política será revisada anualmente ou sempre que houver mudanças significativas nos negócios ou na regulação. O planejamento de compliance e controles internos é efetuado anualmente, com o objetivo de revisar e atualizar todos os procedimentos, códigos, manuais e políticas da Gestora.

3.3. Relatório Anual: A revisão desta política coincidirá com a entrega do Relatório Anual de Controles Internos e Cumprimento da Resolução CVM nº 21/2021, no prazo legal estabelecido.

3.4. Revisões Extraordinárias: Revisões extraordinárias desta política poderão ocorrer em caso de situações imprevistas e/ou mudanças significativas e repentinas, também com vistas a apurar a permanência da conformidade.

Deficiências de controles internos detectadas devem ser relatadas para as áreas responsáveis por tais controles e reportadas à Diretoria.

4. RESPONSABILIDADES

4.1. Diretor de Compliance: Compete ao Diretor de Compliance a gestão e a aplicação desta política, incluindo:

- Supervisão do cumprimento das diretrizes estabelecidas
- Monitoramento da efetividade dos controles de segregação
- Investigação de potenciais violações
- Treinamento de colaboradores
- Comunicação com órgãos reguladores
- Elaboração de relatórios de compliance

4.2. Diretoria: A Diretoria é responsável por:

- Aprovar e revisar esta política
- Assegurar recursos adequados para implementação
- Tomar decisões sobre conflitos de interesse
- Supervisionar a efetividade dos controles
- Comunicar-se com stakeholders sobre questões de compliance

4.3. Colaboradores: Todos os colaboradores devem:

- Conhecer e cumprir as diretrizes desta política
- Reportar potenciais conflitos de interesse
- Manter confidencialidade de informações
- Participar de treinamentos obrigatórios
- Cooperar com investigações de compliance

4.4. Esclarecimentos: Este documento não detalha necessariamente todas as situações passíveis de ocorrência no dia a dia dos negócios. Quaisquer dúvidas deverão ser remetidas ao Diretor de Compliance.

5. ENDEREÇO ELETRÔNICO

Em conformidade com o artigo 16, inciso II, da Resolução CVM nº 21/2021, este documento estará disponível no site da Gestora (www.tritonocapital.com.br) quando em funcionamento.

Para comunicações relacionadas a esta política, dúvidas 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.

6. SEGREGAÇÃO DE COMPLIANCE

6.1. Independência do Compliance: O Diretor de Compliance atua em funções de supervisão, controle e conformidade, em área funcionalmente segregada daquelas utilizadas para a operacionalização dos negócios da Gestora. É considerado profissional "behind all barriers", na forma das melhores práticas vigentes, sob quem recai o dever legal de zelar pela perfeita segregação de atividades da entidade.

6.2. Autonomia Funcional: A Gestora atua com a premissa de que a função de compliance deve ser completamente independente, de modo que não haja interferência no trabalho desenvolvido. A segregação funcional do Diretor de Compliance e demais órgãos da entidade é garantida pela Gestora, fornecendo meios para que possa agir de modo independente, fiscalizar qualquer tipo de conduta imprópria e com poderes para vedar a realização de determinados negócios.

6.3. Estrutura de Reporte: O Diretor de Compliance reporta-se diretamente à Diretoria, mantendo independência em relação às atividades operacionais de gestão de investimentos. Esta estrutura assegura que questões de compliance sejam tratadas com a devida prioridade e independência.

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

- Documentos de investimentos
- Comunicações internas e externas
- Registros de transações
- Informações de due diligence
- Dados de monitoramento de investimentos
- Outras informações relevantes para compliance

7. CHINESE WALL E SEGREGAÇÃO DE FUNÇÕES

7.1. Conceito de Chinese Wall: A Gestora implementa barreiras informacionais ("Chinese Wall") para prevenir o fluxo inadequado de informações confidenciais entre diferentes áreas e atividades, especialmente considerando o acesso a informações privilegiadas inerente à gestão de FIPs.

7.2. Segregação Física e Lógica: Embora a Gestora mantenha estrutura enxuta, implementa controles adequados de segregação:

Segregação Física: - Controles de acesso a documentos físicos - Armazenamento seguro de informações confidenciais - Restrições de acesso a áreas sensíveis - Controles de visitantes e terceiros

Segregação Lógica: - Controles de acesso a sistemas de informação - Perfis de usuário diferenciados - Logs de acesso e auditoria - Criptografia de dados sensíveis

7.3. Segregação de Funções: A Gestora implementa adequada segregação de funções considerando sua estrutura:

Gestão vs. Compliance: - Separação entre atividades de investimento e controle - Independência na avaliação de compliance - Processos de aprovação diferenciados - Reportes independentes

Front Office vs. Back Office: - Terceirização de atividades de back office - Controles sobre prestadores de serviços - Reconciliações independentes - Monitoramento de atividades terceirizadas

7.4. Controles de Informação: Lista de Insiders: - Manutenção de lista de pessoas com acesso a informações privilegiadas - Controles específicos para cada investimento - Monitoramento de transações pessoais - Restrições de negociação quando aplicável

Compartimentalização: - Acesso a informações baseado em "need to know" - Projetos com codinomes quando apropriado - Controles específicos para cada deal - Documentação de acessos e autorizações

7.5. Utilização de Ambientes Físicos e Espaços Compartilhados

A Gestora assegura que todas as suas atividades sejam realizadas em ambientes que garantam a segurança e a confidencialidade das informações, sejam eles escritórios dedicados ou espaços em ambientes compartilhados, como coworkings.

Independentemente do local físico de trabalho, aplicam-se as seguintes regras:

Ambientes Restritos: As atividades da Gestora devem ser realizadas exclusivamente em ambientes físicos restritos aos seus colaboradores, sem acesso de terceiros não autorizados. Isso inclui escritórios privativos, salas de reunião dedicadas ou outras áreas de acesso controlado.

Proibição de Espaços Comuns: É vedada a realização de atividades sensíveis, discussões sobre investimentos, reuniões confidenciais ou o manuseio de documentos sigilosos em espaços comuns de ambientes compartilhados, tais como áreas de café, lounges ou recepções abertas.

Controle de Acesso: Quando em ambientes compartilhados, a Gestora utilizará exclusivamente salas ou escritórios que permitam o controle de acesso, preferencialmente

por meio de reserva prévia que garanta o uso exclusivo do espaço durante o período de utilização.

Segurança da Informação: Os colaboradores devem garantir a segurança de seus equipamentos (laptops, celulares) e documentos, aplicando bloqueio de tela sempre que se ausentarem e utilizando fones de ouvido para chamadas confidenciais. A impressão de documentos sensíveis em impressoras compartilhadas deve ser evitada.

Esta política se aplica a qualquer modalidade de trabalho, seja em sede própria, filial, escritório compartilhado (coworking) ou trabalho remoto, visando sempre a proteção das informações da Gestora e de seus clientes.

8. CONFLITOS DE INTERESSES

8.1. Identificação de Conflitos: A Gestora mantém processo sistemático de identificação de conflitos de interesse, incluindo:

Conflitos Pessoais: - Investimentos pessoais dos colaboradores - Relacionamentos familiares ou pessoais - Atividades profissionais externas - Interesses financeiros diretos ou indiretos

Conflitos Institucionais: - Relacionamentos com empresas investidas - Prestadores de serviços comuns - Investidores com interesses conflitantes - Oportunidades de investimento concorrentes

8.2. Atividades de Colaboradores Alheias à Gestora: A Gestora estabelece regras e procedimentos para assegurar que atividades profissionais, acadêmicas ou pessoais de seus colaboradores, não relacionadas à Gestora, sejam conduzidas de forma a não gerar conflitos de interesse, não comprometer suas responsabilidades fiduciárias e não prejudicar a dedicação necessária às suas funções.

8.2.1. Princípios Gerais de Atividades Externas:

Dedicação Prioritária: Todos os colaboradores devem ter dedicação prioritária às atividades da Gestora. Atividades externas são permitidas, desde que não comprometam a atenção, a disponibilidade e a qualidade do trabalho exigidas para o pleno funcionamento da Gestora.

Natureza das Atividades Permitidas: São permitidas atividades externas de natureza conexa, complementar e não conflitante com as atividades da Gestora, incluindo atividades acadêmicas, pro-bono, participação em conselhos ou comitês de entidades não concorrentes e atividades em entidades de classe.

Limite de Dedicação: A dedicação de tempo a atividades externas não deve, em conjunto, exceder 10% da carga horária profissional total do colaborador, salvo aprovação expressa e justificada da Diretoria, após análise do Comitê de Compliance.

8.2.2. Segregação de Atividades Externas: Para prevenir conflitos e o uso indevido de recursos, a Gestora impõe as seguintes regras de segregação:

Segregação Física e de Ambiente: Nenhuma atividade externa deve ser desempenhada nos ambientes físicos (escritórios, salas de reunião) ou virtuais (sistemas, redes, e-mails corporativos) da Gestora.

Segregação Funcional e de Recursos: É vedada a utilização de quaisquer recursos materiais (computadores, telefones, impressoras) ou informacionais (softwares, bases de dados, informações confidenciais) da Gestora para a realização de atividades externas.

Segregação Sistêmica e de Relacionamento: Nenhuma entidade na qual um colaborador exerça atividade externa poderá prestar serviços, fornecer produtos ou figurar como contraparte da Gestora ou dos fundos sob sua gestão, salvo em condições de mercado estritas, com total transparência e após aprovação prévia do Comitê de Compliance.

8.2.3. Procedimento de Avaliação e Aprovação Prévia: Qualquer atividade externa remunerada ou que possa gerar potencial conflito de interesse deve ser submetida à análise e aprovação prévia do Comitê de Compliance, Risco e PLD. O colaborador deve fornecer informações detalhadas sobre a natureza da atividade, a entidade envolvida, o tempo de dedicação estimado e os potenciais riscos de conflito. O Comitê avaliará a solicitação com base nos princípios desta política e emitirá parecer formal, que será arquivado.

8.2.4. Gestão de Potenciais Conflitos: A Gestora adota uma abordagem preventiva, não autorizando a atuação de colaboradores em atividades permitidas que estejam em conflito com os interesses da Gestora e dos fundos sob sua gestão. O processo de gestão de conflitos de interesse relacionados a atividades externas é conduzido pelo Comitê de Compliance, Risco e PLD.

Quando uma atividade externa é submetida à análise e identificada como potencialmente conflitante, ou enquanto estiver sob avaliação, o Comitê de Compliance implementará medidas internas para impedir o acesso do colaborador a informações sensíveis ou para subtrair os efeitos deletérios de tais potenciais conflitos. Essas medidas podem incluir o estabelecimento de barreiras de informação adicionais, a restrição à participação do colaborador em determinadas decisões de investimento ou a obrigatoriedade de desinvestimento de posições pessoais.

Após a análise, o Comitê de Compliance emitirá uma decisão formal. Caso se conclua que não há interesses na atividade permitida que sejam contrapostos aos da Gestora e dos

fundos sob sua gestão, nenhuma limitação será atribuída ao colaborador. Contudo, se for constatado que há interesses contrapostos, o colaborador não poderá exercer a atividade em questão. A decisão do Comitê será sempre documentada e comunicada formalmente ao colaborador.

8.3. Declaração de Conflito de Interesses

Processo de Declaração: - Declaração inicial na admissão - Atualizações anuais obrigatórias - Comunicação imediata de mudanças - Formulários padronizados

Avaliação e Tratamento: - Análise de cada situação declarada - Implementação de controles específicos - Monitoramento contínuo - Revisão periódica de medidas adotadas

8.4. Gestão de Conflitos

Medidas Preventivas: - Políticas claras de prevenção - Treinamento regular de colaboradores - Controles automatizados quando possível - Cultura de transparência e ética

Medidas Corretivas: - Investigação de violações - Implementação de ações corretivas - Sanções disciplinares quando apropriado - Melhoria de controles e processos

9. POLÍTICA DE CONFIDENCIALIDADE

9.1. Objetivo e Aplicação. Esta seção estabelece diretrizes para proteção de informações confidenciais da Gestora, seus investidores e empresas investidas, aplicando-se a todos os colaboradores, prestadores de serviços e terceiros com acesso a informações da Gestora.

9.2. Definições

Informação Confidencial: - Estratégias de investimento - Informações sobre investidores - Dados financeiros de empresas investidas - Informações de due diligence - Documentos contratuais - Outras informações não públicas

Informação Privilegiada: - Informações materiais não divulgadas sobre empresas investidas - Dados sobre operações em andamento - Informações sobre estratégias de saída - Outros fatos relevantes não públicos

9.3. Diretrizes de Confidencialidade

Princípios Gerais: - Todas as informações da Gestora são consideradas confidenciais por padrão - Acesso baseado em necessidade profissional - Proibição de uso para benefício pessoal - Manutenção de confidencialidade após término do vínculo

Controles de Acesso: - Classificação de informações por nível de confidencialidade - Controles de acesso físico e lógico - Monitoramento de acessos - Trilhas de auditoria

9.4. Controles e Barreiras

Controles Físicos: - Acesso restrito a instalações - Armazenamento seguro de documentos - Controles de impressão e cópia - Descarte seguro de informações

Controles Lógicos: - Senhas robustas e autenticação multifator - Criptografia de dados sensíveis - Controles de acesso a sistemas - Backup seguro de informações

Controles Administrativos: - Políticas e procedimentos claros - Treinamento regular de colaboradores - Acordos de confidencialidade - Monitoramento de compliance

9.5. Segurança Cibernética

Proteção de Sistemas: - Firewall e sistemas de detecção de intrusão - Antivírus e anti-malware atualizados - Atualizações regulares de segurança - Monitoramento de ameaças

Proteção de Dados: - Backup regular e seguro - Criptografia de dados em trânsito e em repouso - Controles de acesso granulares - Políticas de retenção de dados

Resposta a Incidentes: - Plano de resposta a incidentes de segurança - Equipe de resposta designada - Procedimentos de contenção e recuperação - Comunicação com autoridades quando necessário

9.6. Testes de Segurança

Testes Regulares: - Testes e Avaliações Periódicas de vulnerabilidade e Revisão de controles de acesso, conforme detalhamento feito no Manual de Compliance.

Melhoria Contínua: - Implementação de correções identificadas - Atualização de políticas e procedimentos - Treinamento baseado em resultados - Monitoramento de efetividade

9.7. Comunicação Externa

Princípios: - Comunicação apenas de informações autorizadas - Aprovação prévia para divulgações - Consistência nas mensagens - Proteção de informações confidenciais

Canais Autorizados: - Porta-vozes designados - Canais oficiais de comunicação - Procedimentos para imprensa - Comunicação com reguladores

9.8. Violações e Sanções

Investigação: - Processo formal de investigação - Preservação de evidências - Entrevistas com envolvidos - Documentação adequada

Sanções: - Medidas disciplinares proporcionais - Ações corretivas - Comunicação a autoridades quando necessário - Melhoria de controles

10. DISPOSIÇÕES GERAIS

10.1. Vigência. Esta política entra em vigor na data de sua aprovação pela Diretoria e permanece válida até sua revogação ou substituição por versão atualizada.

10.2. Treinamento. Todos os colaboradores devem receber treinamento sobre esta política, incluindo:

- Conceitos de segregação de atividades
- Identificação de conflitos de interesse
- Proteção de informações confidenciais
- Procedimentos de reporte
- Consequências de violações

10.3. Monitoramento. O cumprimento desta política é monitorado através de:

- Revisões periódicas de controles
- Testes de efetividade
- Auditoria interna e externa
- Indicadores de performance
- Relatórios de compliance

10.4. Integração com Outras Políticas. Esta política deve ser lida em conjunto com:

- Código de Ética e Conduta
- Manual de Compliance
- Política de Investimentos Pessoais
- Política de Gestão de Riscos
- Outras políticas internas relevantes

10.5. Atualizações. Esta política será atualizada conforme necessário para refletir:

- Mudanças na regulamentação
- Evolução das melhores práticas
- Lições aprendidas de incidentes
- Feedback de stakeholders
- Mudanças na estrutura da Gestora

10.6. Responsabilidade Individual. Cada colaborador é responsável por:

- Conhecer e cumprir esta política
- Reportar violações ou suspeitas
- Manter confidencialidade de informações
- Participar de treinamentos
- Cooperar com investigações

10.7. Casos Omissos. Situações não previstas nesta política devem ser submetidas ao Diretor de Compliance para análise e orientação, sempre considerando os princípios de segregação, confidencialidade e proteção dos investidores.

10.8. Documentação. Todas as atividades relacionadas a esta política devem ser adequadamente documentadas, incluindo:

- Declarações de conflito de interesse
- Investigações de violações
- Treinamentos realizados
- Testes de controles
- Ações corretivas implementadas

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