POLÍTICA DE CONTROLES INTERNOS

***Jun*/2022**

1. INTRODUÇÃO

A presente Política foi elaborada em conformidade com a Resolução n. 21 da Comissão de Valores Mobiliários (CVM), de 25 de fevereiro de 2021, ofícios e deliberações da matéria, para apresentar os mecanismos de Controles Internos adotados.

2. CONTROLES INTERNOS

2.1 Políticas

Com a finalidade de se manter sempre em conformidade com as normas regulamentadoras, a Gestora adota as seguintes políticas cujo conteúdo é objeto de treinamentos recorrentes de Compliance, e que ficam disponíveis para todos os colaboradores na rede interna, no site (https://spninvestimentos.com/) da Gestora e/ou no site da ANBIMA:

POLÍTICAS	DISPONÍVEL EM		
Manual Ética e Compliance	Site ANBIMA	Site SPN**	Rede SPN
Política de Confidencialidade	Site ANBIMA*	Site SPN**	Rede SPN
Política de Conflito de Interesse	Site ANBIMA*	Site SPN**	Rede SPN
Política de Investimentos Pessoais	Site ANBIMA*	Site SPN**	Rede SPN
Política de Segregação de atividades	Site ANBIMA*	Site SPN**	Rede SPN
Política de Treinamentos	Site ANBIMA*	Site SPN**	Rede SPN
Política de Vantagens e Presentes	Site ANBIMA*	Site SPN**	Rede SPN
Política de Capital Humano		Site SPN**	Rede SPN
Plano de Continuidade de Negócios	Site ANBIMA	Site SPN**	Rede SPN
Política de Certificações	Site ANBIMA	Site SPN**	Rede SPN
Política de Contratação de Terceiros	Site ANBIMA	Site SPN**	Rede SPN
Política de Controles internos	Site ANBIMA	Site SPN**	Rede SPN
Política de Custódia de Ativos		Site SPN**	Rede SPN
Política de Exercício do Direito de Voto	Site ANBIMA	Site SPN**	Rede SPN
Política de Gestão de Risco de Liquidez	Site ANBIMA	Site SPN**	Rede SPN
Política de Gestão de Risco	Site ANBIMA	Site SPN**	Rede SPN
Política de LGPD - Lei Geral de Proteção de Dados		Site SPN**	Rede SPN
Política de PLD/FTP - Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento das Proliferação das Armas de		Site SPN**	Rede SPN
Política de Rateio de Ordens		Site SPN**	Rede SPN
Política de Segurança Cibernética	Site ANBIMA	Site SPN**	Rede SPN
Política de Segurança da Informação	Site ANBIMA	Site SPN**	Rede SPN

** Parte integrante do Manual de Ética e Compliance*
*** https://spninvestimentos.com/*

As Políticas acima são atualizadas e revisadas anualmente com a finalidade de: *I)* verificar se atendem aos requisitos mínimos estabelecidos pela regulação e autorregulação *II)* se as versões publicadas no *website* da Gestora e SSM – Sistema de Supervisão de Mercado da ANBIMA estão atualizadas.

2.2 Investimentos Pessoais

A Gestora, por meio da Política de Investimentos Pessoais, autoriza que os Colaboradores e Sócios possuam investimentos pessoais, desde que: *I)* sejam totalmente segregados das operações realizadas em nome da ANIMA e não afetem adversamente a qualidade do trabalho desenvolvido na Gestora; *II)* não sejam utilizados recursos físicos, lógicos, humanos ou financeiros da ANIMA; *III)* não compitam com os

negócios da ANIMA; *IV)* não adquiram ou incentivem que terceiros não autorizados pela ANIMA adquiram títulos e valores mobiliários valendo-se de informação privilegiada; *V)* não negocie ou incentive que terceiros não autorizados pela ANIMA negociem ativos de empresas nos quais a Família Passos possua alguma influência.

A Área de Compliance circula mensalmente uma lista informando os ativos com restrições à negociação.

O controle de aderência é realizado por meio do processo de *Disclousure*, pelo qual todos os Sócios e Colaboradores são convidados a informar suas posições detidas ao final do ano anterior à declaração, com as seguintes informações: nome e ticker do valor mobiliário, quantidade detida e geografia de emissão.

De posse das informações fornecidas, o Compliance deverá verificar a conformidade dos Colaboradores à Política de Investimentos e a possibilidade de ocorrência de *insider trading* ou conflito de interesses.

2.3 Confidencialidade, Segurança da Informação e Segurança Cibernética

A Gestora não autoriza que informações confidenciais, definidas como informações de qualquer Companhia a que os Sócios e Colaboradores da SPN venham a ter acesso em decorrência de suas funções, circulem em ambientes externos à Gestora.

A fim de garantir a confidencialidade das informações, a Política de Segurança da informação classifica os dados que circulam na SPN em: público, onde as informações podem circular livremente, restrito, onde o acesso é restrito para determinadas funções e áreas dentro da gestora, sigiloso, em que o acesso/permissão é para pessoas específicas.

De acordo com essa classificação, a Gestora dispõe de um mapa de acessos, por meio do qual elenca todas as pastas da rede interna e o grupo de Sócios e Colaboradores que podem acessar as respectivas pastas, de acordo com as funções desempenhadas na SPN.

Na Política de Segurança Cibernética a Gestora estabelece os perímetros de segurança digital, classificando os locais em que há troca de informações em: Ambiente Seguro: que são as redes locais e virtuais, aplicativos móveis para acesso à informações da Gestora; Fronteira do Perímetro de Segurança: que são e-mails corporativos, acesso à internet pela rede local ou virtual, portas de acessos nas estações de trabalho e acesso via Remote Desktop; Ambiente Externo: aplicativos dos dispositivos móveis dos Sócios e Colaboradores, estações de trabalho pessoais.

É de igual obrigação dos Sócios e Colaboradores observar cada tipo de ambiente em que as informações podem circular.

A Gestora atualizará anualmente as Políticas de Segurança da Informação e Cibersegurança. As classificações do perímetro de segurança e o mapa de acessos deverão ser revisados semestralmente.

Somado a isso, a Gestora deverá contratar bianualmente auditoria especializada em cibersegurança que deverá testar risco de vazamento de dados internos e proteção contra ataques externos.

2.4 Gestão de Risco

Os riscos que são inerentes aos negócios da Gestora são divididos em: Risco de Mercado, Risco de Liquidez, Risco de Concentração, Risco de Crédito e Contraparte, Risco Operacional e Risco de Compliance.

O Risco de Mercado, assim compreendido como o risco de perda permanente de capital, deverá ser monitorado por meio da apresentação das teses investidas ao Comitê de *Equities* e prestações de contas do desempenho dos ativos investidos ao Comitê de Investimentos, Conselho Familiar, Comitê de Risco e Compliance e cotistas individuais.

A Gestora realizará o monitoramento de todos os fatos relevantes que envolvem os gestores e as companhias e que possam de alguma forma impactar as suas atividades e, por conseguinte, o valor dos ativos.

O Risco de Liquidez, que consiste no monitoramento da possibilidade de os fundos sob gestão não serem capazes de honrar suas obrigações esperadas e inesperadas, correntes e futuras, sem afetar suas operações diárias e sem incorrer em perdas significativas.

Risco de Concentração: a Gestora deverá evitar a concentração excessiva em ativos financeiros de um mesmo emissor. Para isso, os limites de concentração estabelecidos no *statement* de apetite de risco deverão ser revisados periodicamente

Risco de Crédito e Contraparte: são mitigados pelo fato de a Gestora adotar política que prevê que os ativos sob sua gestão não podem ser incorporados aos balanços das contrapartes, podendo, portanto, ser dados em garantia ou colateral de operações financeiras dessa contraparte.

Riscos Operacionais serão monitorados através de uma gestão por processos adotados por duas áreas da Gestora: Controladoria de Investimentos e Administrativo Financeira. A área de Controladoria de Investimentos realizará os seguintes processos de monitoramento:

1. Orçado x realizado das despesas dos Fundos
2. Batimento de cotas

3. Controle de enquadramentos
4. Controle de movimentações
5. Controle de Proventos
6. Controle de Custódia
7. Projeção de caixa nos veículos
8. Relatório de Erros

A área Administrativo-financeira mitigará riscos operacionais através de ferramentas como Mapa de Obrigações e Matriz Racin que mapeiam todas as obrigações ficais, trabalhistas, contábeis e financeiras da Gestora, sua periodicidade, data em que são devidas e responsáveis e envolvidos.

Será realizado ainda, semestralmente, um processo de reporting da Gestão de Riscos para o Comitê de Risco e Compliance que deverá conter: *I)*. *Statement* De Apetite a Risco, documento em que são explicitados os riscos que a SPN está disposta a se expor; *II)* Mapeamento de Risco, realizado com base no *statement* de apetite de risco, para identificar os riscos, seus fatores, limites/métricas e mitigadores; *III)* Dashboard de Risco, em que são detalhados os KPI´s e KRI´s, dos riscos levantadas no mapeamento de riscos; *IV)* Matriz de Risco, prioriza os riscos segundo sua probabilidade de ocorrência e impacto financeiro resultante estimado.

2.5 Plano de Continuidade de Negócios

A SPN possui um plano dos procedimentos e mecanismos a serem acionados para continuidade do negócio em caso de desastre ou dano que afete a infraestrutura da Gestora, em relação ao acesso às informações e aos sistemas e informações.

Para controlar a conformidade do procedimento em casos de descontinuidade do negócio, a Gestora conta com o apoio de uma consultoria especializada em Segurança

da Informação, que realizará trimestralmente o teste de contingência e testes de *backups*, redundância, *software* e *hardware*.

Além disso, com o apoio da consultoria especializada a Gestora fará o acompanhamento de KPI´s em relação à Disponibilidade, Capacidade e Cibersegurança, que passam por revisões trimestrais em reuniões entre a Área de Compliance e a consultoria especializada.

2.6 Treinamentos

A SPN Gestão possui um programa de treinamentos periódicos e recorrentes a que todos os Sócios ou Colaboradores são submetidos:

Treinamento de Integração em Compliance: O treinamento será ministrado pela Área de Compliance, individualmente, para todo colaboradores recém-admitido. O controle será realizado através de lista de presença e assinatura do Termo de Confidencialidade e Compromisso.

Treinamento Anual de Reciclagem em Compliance: Realizado, anualmente, por todos os colaboradores da SPN, por meio da plataforma Compliasset, com controle de aproveitamento.

Treinamento Anual em Cibersegurança: Realizado anualmente e ministrado por especialista da área, com a finalidade de manter o conteúdo atualizado. O controle é feito com lista de presença.

Treinamento Anual de PLDFTP – Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo: Realizado, anualmente, por todos os colaboradores da SPN, por meio da plataforma Compliasset, com controle de aproveitamento.

Treinamento Anual de LGPD: Lei Geral de Proteção de Dados: Realizado, anualmente, por todos os colaboradores da SPN, por meio da plataforma Compliasset, sem controle de aproveitamento, como parte do Treinamento Anual de Reciclagem em Compliance.

2.7 Vantagens, Benefícios e Presentes

A SPN Gestão orienta aos seus colaboradores que não recebam, direta ou indiretamente, solicitem, aceitem ou admitam dinheiro, benefícios, favores, presentes, para si ou terceiros, promessas ou quaisquer outras vantagens que possam influenciar o desempenho de suas funções ou como recompensa por ato ou omissão decorrente de seu trabalho.

Os Colaboradores poderão aceitar presentes, refeições ou outros benefícios sem prévia autorização do Coordenador de Compliance desde que não influencie nas condutas e/ou decisões profissionais.

A Área de Compliance deverá monitorar o recebimento das vantagens, benefícios e presentes pelos seus Sócios e Colaboradores, a fim de verificar a conformidade.

2.8 Conflito de Interesse

Os Colaboradores e Sócios têm o dever de agir com boa-fé e de acordo com os interesses da SPN com o intuito de não ferir a relação fiduciária com ela. Para tal, deverão estar atentos para uma possível situação de conflito de interesses, e sempre que tal situação ocorrer deverá informar, imediatamente, a área de Compliance sobre sua existência e abster-se de consumar o ato ou omissão originador do Conflito de Interesse até decisão em contrário.

Situações que podem ser caracterizadas como “conflitos de interesse” pessoais e profissionais incluem:

- Investimentos pessoais (vide item “7. Políticas de Investimentos Pessoais”);
- Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas ou fornecedores;
- Operação com empresas com cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
- Operação com empresas em que o Colaborador possua investimento pessoal;
- Participações em atividades políticas.

A Área de Compliance disponibiliza aos Sócios e Colaboradores um canal para denúncias anônimas, dentro da plataforma Compliasset e um canal de Compliance para o encaminhamento de dúvidas e obtenção de orientações, o compliance@animainvestimentos.com.br e deve analisar as informações recebidas, a fim de confirmar a existência de conflito de interesse.

2.9 Privacidade e Proteção de Dados

Conforme estabelecido na Política de LGPD e Privacidade, o tratamento de dados pessoais na SPN deve ser realizado em conformidade com a legislação vigente, em especial a Lei 13.709/2018 (Lei Geral de Proteção de Dados), de modo que os dados tratados devem ser mantidos sempre em sigilo, salvo disposição legal em contrário, e, após o tratamento, deve ser providenciado o descarte dos dados que não forem necessários.

Recomenda-se, ainda, que os dados pessoais sensíveis e de menores de idade não sejam coletados, salvo quando estritamente necessário.

Com a finalidade de dar amplo conhecimento a todos os Sócios e Colaboradores da SPN, ao serem admitidos, sobre a política de LGPD, cada colaborador deverá passar pelo treinamento individual de integração em Compliance. Além disso a área de Compliance deverá providenciar o treinamento de reciclagem anual de LGPD para todos os Colaboradores.

Os treinamentos deverão abordar os direitos e deveres dos Colaboradores e Sócios em relação aos seus próprios dados pessoais e de terceiros, tornando-os aptos para identificar e denunciar situação que viole a Política e legislação de LGPD vigentes.

Os Colaboradores e Sócios que passarem pelos treinamentos deverão assinar o Termo de Compromisso e Confidencialidade que, além de autorizar o tratamento dos dados colhidos, dá ciência dos deveres de cada um em relação a estes.

2.10 Prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa (PLD/FTP)

A fim de se manter em conformidade com a Resolução n. 50 da Comissão de Valores Mobiliários (CVM), a Gestora deverá designar uma Diretora de Risco e Compliance, que terá acesso amplo e irrestrito à todas as informações da Gestora, e será responsável pela implementação, manutenção e cumprimento das normas da referida Resolução.

A Diretora de Risco e Compliannce, para dar cumprimento às normas da Resolução n. 50 da CVM, deverá elaborar e revisar anualmente a Política de PLD/FTP, que deverá conter a classificação dos riscos com base na Abordagem Baseada em Risco (ABR), com a finalidade de adotar medidas preventivas adequadas.

Deverão ser classificados em baixo, médio e alto risco: *I*) Serviços prestados; *II*) Produtos oferecidos; *III*) canais de distribuição; *IV*) Clientes; *V*) Prestadores de serviços relevantes; *VI*) Agentes envolvidos nas operações, ambientes de negociação e registro.

Além disso, a Gestora deverá manter registros de todas as transações realizadas pelos produtos sob sua gestão para que possa monitorar toda e qualquer atipicidade que configure prática, indício ou mera suspeita de LD/FTP. Confirmada a existência de irregularidade, a Diretora de Compliance deverá comunicar ao COAF, no prazo de 24h (vinte e quatro horas).

A Área de Compliance é responsável por providenciar o treinamento anual, obrigatório, de PLD/FTP a todos os Sócios e Colaboradores, como medida preventiva.

Somado a isso, o Compliance é responsável pelo monitoramento periódico das listas divulgadas pelo Conselho Nacional das Nações Unidas (CSNU), Grupo de Ação Financeira Internacional (GAFI) e Comissão de Valores Mobiliários (CVM).

O controle de conformidade será realizado por meio dos testes de aderência que a Gestora realizará anualmente para medir a eficácia da Política de PLD/FTP, que analisará: I) as correspondências e operações que tenham sido objetos de notificação e comunicação; II) percentual de aderência dos treinamentos; III) análise do rendimento obtidos pelos Colaboradores em testes de PLDFTP; IV) cumprimento tempestivo dos prazos para detecção, análise e comunicação das operações atípicas; V) recebimento dos documentos solicitados para verificação de conformidade de PLD/FTP.

Os testes de aderência serão refletidos no Relatório de PLD/FTP, que será elaborado anualmente pela Área de Risco e Compliance.

2.11 Segregação das Atividades

A SPN desempenhará exclusivamente atividades voltadas à gestão de carteiras de títulos e valores mobiliários.

Tais atividades exigem credenciamento específico e estão condicionadas a uma série de providências, dentre elas a segregação total de suas atividades de gestão de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas pela SPN ou empresas controladoras, controladas, ligadas ou coligadas no âmbito do mercado de capitais.

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

Além disso, os serviços de gestão desempenhados pela SPN não se caracterizam como gestão de patrimônio, conforme definição do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.

2.12 Independência e Autonomia da Área de Compliance e Controles Internos

As atividades de Compliance, gestão de risco e PLD/FTP estão sob responsabilidade da Diretora Estatutária, que se reporta diretamente ao Conselho Familiar.

A Diretora responsável pela Gestão de Risco tem assento como convidada no Comitê de Equities realizado mensalmente, ocasião em que toma conhecimento das recomendações de alocações que serão encaminhadas ao Comitê de Investimentos.

Se, eventualmente, houver percepção de alguma não conformidade, ou risco envolvido nas recomendações propostas, a Diretora responsável se manifesta. Caso a dúvida ou desconforto persistam, a Diretora responsável pela Gestão de Risco inclui o assunto na pauta da reunião seguinte do Comitê de Gente.

Em persistindo ainda a dúvida/desconforto, a Diretora responsável pela Gestão de Risco leva o assunto à reunião bimensal do Conselho Familiar. Enquanto qualquer recomendação estiver sob análise e encaminhamento da Diretora Responsável pela Gestão de Riscos, ela não poderá ser implementada.

Os parâmetros de aderência ao mandato estratégico e controles de limites de alocação a teses, geografias e veículos são reportados semestralmente ao Comitê de Risco e Compliance.