POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS

(Incluindo Política de Segurança de Informação, e Cybersegurança, Plano de Continuidade de Negócios e Controles de Certificação)

SP GESTAO DE RECURSOS

Política de Compliance e Controles Internos
Fevereiro 2020

INTRODUÇÃO

A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a SP Gestão (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de *Compliance*.

ABRANGÊNCIA E ADESÃO

Esta Política é aplicável a todos os Colaboradores e sócios da SP Gestão. Os Colaboradores devem atender a esta Política ao ingressar na companhia ou sempre que as alterações forem consideradas pela Diretoria de *Compliance* como relevantes e/ou demandarem obrigações adicionais aos Colaboradores, sendo obrigatória por parte de todos.

Esta Política é parte integrante das normas que guiam as relações da SP Gestão e de seus colaboradores, os quais, ao assinar o *Protocolo de Recebimento e Leitura das Políticas Internas*, concordam absolutamente com as diretrizes nela fixadas. A desobediência a qualquer das normas aqui expostas é tida como infração contratual, sujeitando seu autor às sanções cabíveis.

ESTRUTURA E RESPONSABILIDADE

Cabe à SP Gestão garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento à legislação, regulação, autorregulação e políticas internas vigentes.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à SP Gestão contidas nesta Política, zelando para que todas as normas éticas, legais, regulatórias e autorregulatórias sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação ou indício de violação ao Diretor de *Compliance*.

Cabe à alta administração da SP Gestão:

- ✓ **A responsabilidade pelos controles internos e o gerenciamento dos riscos de *compliance*;**
- ✓ **Indicar um diretor estatutário responsável por compliance e controles internos[1], devendo tal profissional ter acesso a todas as informações e pessoas na SP Gestão quando do exercício de suas atribuições;**
- ✓ **Aprovar, estabelecer e divulgar esta Política; e**
- ✓ **Garantir a efetividade do gerenciamento do risco de compliance.**

O Diretor de *Compliance* deve:

[1] Com capacidade técnica e função independente das relacionadas à administração de carteiras de valores mobiliários, ou em qualquer atividade que limite a sua independência, na instituição ou fora dela.

- ✓ **Auxiliar a alta administração a assegurar a efetividade do Sistema de Controles Internos e *Compliance* da SP Gestão, atuando no gerenciamento efetivo de tais atividades no seu dia-a-dia;**
- ✓ **Gerenciar o Comitê de *Compliance* e Riscos e o Conselho de Ética, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;**
- ✓ **Designar os secretários das reuniões do Comitê de *Compliance* e Riscos e do Conselho de Ética;**
- ✓ **Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas.**

É responsabilidade de todos os Colaboradores o cumprimento das normas legais, regulatórias e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da SP Gestão.

Qualquer suspeita, indício e/ou evidência de desconformidade por eles verificada deve ser imediatamente comunicada ao Diretor de *Compliance*.

O Diretor de *Compliance* se reporta apenas à alta administração da SP Gestão, com autonomia e independência para indagar a respeito de práticas e procedimentos adotados nas suas operações/atividades, devendo adotar medidas que coíbam ou mitiguem as eventuais inadequações, incorreções e/ou inaplicabilidades.

Os controles e monitoramentos determinados nesta Política são prerrogativa exclusiva dos integrantes da Área de *Compliance* da SP Gestão, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade: o Diretor de *Compliance* tem poder de veto – mas não de voto – nos Comitês de negócios da SP Gestão.

A Área de *Compliance* é formada pelo diretor estatutário responsável e por analista(s) interno(s), o qual(ais) se dedica(m) com exclusividade ao exercício das atividades de cumprimento de regras, políticas, procedimentos e controles internos, incluindo o cumprimento das normas relativas ao combate e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção.

REVISÃO E ATUALIZAÇÃO

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

ESCOPO E ATRIBUIÇÕES DO COMPLIANCE

A atuação do Diretor de ***Compliance*** tem por escopo:

Temas Normativos

- ✓ **Controlar a aderência a novas leis, regulação e normas de autorregulação aplicáveis à SP Gestão e às suas atividades, e**

apresentar o resultado de suas verificações no Comitê de Risco e *Compliance*;

- ✓ **Controlar e monitorar as licenças legais e certificações necessárias, e a sua obtenção/renovação/manutenção junto às autoridades reguladoras/autorreguladoras competentes;**
- ✓ **Auxiliar a alta administração da SP Gestão no relacionamento com órgãos reguladores, e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;**
- ✓ **Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação, regulação e autorregulação em vigor.**

Boas Práticas

- ✓ **Disseminar e promover as informações necessárias para o cumprimento das políticas internas e das normas legais, regulatórias e de autorregulação aplicáveis;**
- ✓ **Exercer seu controle, garantindo que as políticas e manuais pertinentes estejam atualizados e mantidos em diretório acessível a todos que delas devam ter conhecimento;**
- ✓ **Disponibilizar aos novos Colaboradores as políticas internas aplicáveis, e coletar os termos de ciência e aderência por eles assinados;**
- ✓ **Estabelecer controles para que todos os Colaboradores da SP Gestão que desempenhem funções ligadas à gestão de fundos de investimento ou de carteiras administradas atuem com independência[2];**
- ✓ **Garantir que os controles internos sejam compatíveis com os riscos da SP Gestão em suas atividades[3];**
- ✓ **Analisar informações, indícios ou identificar, administrar e, se necessário, levar temas para análise e deliberação no Comitê de Risco e *Compliance* e/ou no Conselho de Ética;**
- ✓ **Orientar previamente e/ou acompanhar o responsável pela comunicação à imprensa em contatos telefônicos, entrevistas, publicação de artigos ou qualquer outra forma de manifestação de opinião através de veículo público (inclusive na internet).**

Governança

- ✓ **Aprovar novas políticas internas no Comitê de Risco e *Compliance*, ou a sua revisão, por força de mudanças na legislação, regulação ou autorregulação aplicáveis, ou ainda, de decisões internas da SP**

[2] E atentem ao seu dever fiduciário para com os clientes, e que os interesses comerciais - ou aqueles de seus clientes - não desviem o foco de seu trabalho.

[3] Bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários.

Gestão;

- ✓ **Aprovar a oferta de novos produtos e prestação de novos serviços pela SP Gestão, a partir de inputs técnicos do Comitê de Investimento;**
- ✓ **Atuar para que haja efetividade na segregação física de atividades conflitantes;**
- ✓ **Apresentar o resultado de seus controles e verificações no Comitê de Risco e *Compliance*;**
- ✓ **Monitorar e buscar a efetiva aplicação dos documentos de compliance e controles internos abaixo listados;**
- ✓ **Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da SP Gestão e às demais políticas da SP Gestão;**
- ✓ **Convocar, gerenciar, organizar e secretariar o Comitê de Risco e *Compliance*, registrando suas decisões em atas;**
- ✓ **Implementação de Regras e Guarda de Evidências – monitoramento da implementação de procedimentos, de cumprimento das normas e políticas internas, bem como de mecanismos de guarda de evidências;**
- ✓ **Salvaguarda de Informações - devem ser mantidos, pelo prazo mínimo de 5 (cinco) anos[4], os documentos e informações exigidos pela regulação aplicável[5].**

ANÁLISE E COMUNICAÇÃO AOS ÓRGÃOS COMPETENTES

Toda desconformidade em temas de conduta pessoal e profissional - e a sua respectiva análise efetuada pelo *Compliance* - deve ser submetida ao Conselho de Ética da SP Gestão para conclusão e deliberação dos passos a serem dados a tal respeito.

Nos casos aplicáveis de desvio da norma específica das atividades reguladas, o Diretor de Compliance deve comunicar os respectivos órgãos competentes, nos prazos regulatórios, como seguem:

- ✓ **A CVM deve ser comunicada no prazo máximo de 10 (dez) dias da verificação da respectiva ocorrência ou sua identificação, ou em prazo menor, se assim exigido pela regulação aplicável;**
- ✓ **O COAF deve ser comunicado no prazo de 24 (vinte e quatro) horas da verificação da respectiva ocorrência ou sua identificação.**

[4] Ou prazo superior por determinação expressa da CVM.
[5] Bem como correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções. Os documentos e informações podem ser guardados em meio físico ou eletrônico, admitindo-se a substituição de documentos originais por imagens digitalizadas.

Os demais prazos aplicáveis à SP Gestão encontram-se previstos no Anexo a esta Política.

TESTE E RELATÓRIO ANUAL

Para verificação dos controles internos, sua efetividade e consistência com a natureza, complexidade e riscos das operações realizadas pela SP Gestão, é realizado um teste anual de aderência, o qual deve ser formalizado em um relatório formal[6].

O relatório é de responsabilidade do Diretor de Compliance, e, após ratificação pelo Comitê de Risco *Compliance*, é encaminhado à alta administração da SP Gestão anualmente, até o último dia útil de abril de cada ano[7].

O Relatório Anual fica disponível para consulta da CVM, na sede da SP Gestão.

Tal relatório contém:

- ✓ **As conclusões dos exames efetuados relativos aos controles internos e *compliance*, inclusive o Teste Anual dos Sistemas de Informações - os testes periódicos dos sistemas de informações, em especial para os mantidos em meio eletrônico, efetuados pela Diretoria de *Compliance*[8];**
- ✓ **As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e**
- ✓ **A manifestação do Diretor de Gestão, ou, quando for o caso, dos Diretores de Risco e de *Compliance* a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.**

Organismos Relacionados a *Compliance* e Controles Internos

Comitê de Risco e *Compliance*

O Comitê de Risco e *Compliance* é responsável por avaliar o descumprimento das normas legais, regulatórias, autorregulatórias e das políticas, manuais e procedimentos internos da SP Gestão.

Ademais, cabe ao Comitê de Risco e *Compliance* avaliar, do ponto de vista normativo, a atividade da SP Gestão e dos veículos de investimento sob sua responsabilidade, a fim de garantir a aderência à legislação e normas regulatórias e autorregulatórias em vigor, bem como aprovar ações de correção

---

[6] (v. modelo no Anexo, e orientação sobre o respectivo conteúdo).

[7] Com conteúdo relativo ao ano civil imediatamente anterior.

[8] Devem: (i) assegurar que os recursos humanos e computacionais estão adequados ao porte e à área de atuação da SP GESTÃO, (ii) garantir o adequado nível de confidencialidade e acessos às informações confidenciais, (iii) assegurar que os recursos computacionais estão protegidos contra adulterações e (iv) assegurar que a manutenção de registros permite a realização de auditorias e inspeções.

nestas matérias, além de:

- ✓ **Avaliar os processos internos da SP Gestão do ponto de vista de melhores práticas, bem como avaliar as ocorrências do período;**
- ✓ **Concluir por eventuais apontamentos de situações irregulares ao Conselho de Ética e/ou à alta administração da SP Gestão;**
- ✓ **Analisar eventuais situações ocorridas de desenquadramento de mandato no mês anterior, procedimentos adotados, e recomendações de controle futuro;**
- ✓ **Elaborar e distribuir a Lista Restrita de Ativos da SP Gestão fazendo seu acompanhamento e monitoramento; e**
- ✓ **Monitorar mudanças regulatórias e coordenar ajustes e adaptações necessárias na SP Gestão e seus produtos.**

Periodicidade: bimestral.

Participantes: Diretores, sempre com a presença do Diretor de Risco e *Compliance.*

Convidados: podem ser convidados outros Colaboradores da SP Gestão, porém sem direito a voto.

Quórum mínimo: Necessária a presença de ao menos três membros, sendo obrigatória a presença do Diretor de Risco e *Compliance* (ou representante por ele designado).

Formalização das decisões: atas do Comitê sob responsabilidade da Área de Risco e *Compliance*.

As atribuições do Comitê no que diz respeito a controle de Riscos, estão descritas na Política de Gestão de Riscos da SP Gestão.

Conselho de Ética

O Conselho de Ética tem suas atribuições descritas na forma definida no Código de Ética e Conduta Profissional da SP Gestão.

Segregação de Atividades

Cabe ao Diretor de *Compliance* assegurar e verificar que sejam devidamente segregadas da atividade de gestão todas e quaisquer atividades eventualmente desempenhadas pela da SP Gestão que com aquela guarde qualquer tipo de conflito, real ou potencial, em qualquer grau, aspecto, medida, tempo e/ou forma.

Contratações Externas

A SP Gestão não realiza quaisquer contratações de prestadores de serviço em

nome dos fundos sob sua gestão[9], seja de atividades reguladas pela CVM ou autorreguladas pela ANBIMA, cabendo tais contratações aos respectivos administradores dos referidos fundos.

Esta Política se aplica somente às contratações feitas pela própria SP Gestão em seu próprio nome e benefício.

A contratação de serviços de terceiros deve ser precedida das seguintes providências[10] :

- ✓ **Exigência de documentos e das certidões reputadas convenientes, seguindo, quando aplicável, procedimentos semelhantes aos descritos na Política de Prevenção à Lavagem de Dinheiro;**
- ✓ **De acordo com a avaliação de conveniência dos profissionais envolvidos, solicitar a assinatura, pelos terceiros a serem contratados, de "Acordo de Não Divulgação" (Non-Disclosure Agreement ou NDA); e**
- ✓ **Nos processos de negociação de qualquer contrato a ser celebrado pela SP Gestão, o Colaborador envolvido na negociação deverá informar ao Comitê de Compliance sobre qualquer relacionamento familiar ou pessoal, sejam laços de amizade ou negocial, que tenha com membros do potencial contratado.**

Após a contratação dos respectivos serviços, a área de Compliance da SP Gestão poderá, a seu critério, supervisionar os contratados[11] .

O processo para contratação de terceiros poderá vir acompanhado ou não de concorrência prévia, visando a obter o melhor "custo x benefício" dos melhores prestadores de serviço do mercado. Cabe a área responsável pela contratação definir ou não se será adotado este procedimento, sendo responsável inclusive por dar as devidas justificativas pelo "não uso", na hipótese de questionamento.

Qualquer eventual exceção às normas acima deverá ser reportada no Comitê de Compliance.

- ✓ **A contratação de terceiros deverá ser orientada pelas seguintes diretrizes:**
- ✓ **O critério principal para escolha e contratação de terceiros será a modalidade menor preço, mediante a obtenção de orçamentos em número determinado pelo Diretor de Compliance para escolha do fornecedor ou prestador de serviços;**
- ✓ **Em casos excepcionais em que um fornecedor mais caro seja escolhido, a contratação deverá ser justificada com os outros critérios (por exemplo: prazo, qualidade, expertise, menor impacto ambiental**

[9] Portanto, não são previstas neste documento regras de Supervisão Baseada em Risco, conforme previstas na autorregulação da ANBIMA.

[10] O Compliance poderá demandar medidas adicionais pré-contratação, tais como visita às dependências do prestador de serviço, clippings de mídia impressa/internet, além de outras medidas reputadas cabíveis/convenientes à contratação.

[11] A supervisão poderá ser realizada mediante procedimentos diversos a critério do Compliance, tais como visitas in loco, clippings de mídia impressa/internet, requisição periódica de certidões administrativas/judiciais, além de outras medidas reputadas cabíveis/convenientes à contratação.

etc.);

- ✓ **Não haverá exigência de concorrência nos seguintes casos:**
  - Compras e contratações para valores inferiores a R$ 10.000,00 (dez mil reais), desde que os pagamentos não se refiram a parcelas de um mesmo serviço;
  - Quando já houver um contrato com prestadores de serviços recorrentes. Neste caso, não será necessário realizar concorrência a cada contratação ou compra;
  - Compras e contratações em casos de especialidade do fornecedor/prestador;
  - Compras e contratações em casos emergenciais, que será caracterizado devido à urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer o trabalho e que não pôde ser previsto antecipadamente.

Soft Dollar

A prática de *soft dollar* é vedada na SP Gestão, salvo exceções expressas e circunstanciadas pelo Diretor de Compliance, e apenas se comprovada a conveniência da ferramenta permutada na eficiência da gestão de fundos e carteiras a cargo da SP Gestão.

Política de Segurança da Informação e Cybersegurança

A Política de Segurança da Informação e Cibernética foi elaborada com o objetivo de identificar e definir os princípios, conceitos e diretrizes relacionados à segurança da informação e à segurança cibernética, os quais deverão ser adotados por funcionários e sócios da SP Gestão, bem como terceirizados que possuirem acesso a suas informações confidenciais.

Os Colaboradores deverão obrigatoriamente aderir a esta Política ao ingressar na SP Gestão, bem como concordar com suas posteriores e eventuais alterações. Tal adesão será realizada por meio de assinatura de um Termo de Adesão e Compromisso que prevê, dentre diversas obrigações, a necessidade de os Colaboradores manterem confidenciais as informações a que tiverem acesso quando da realização de suas atividades profissionais.

Esta Política foi elaborada e deve ser interpretada em consonância com os demais manuais e políticas da SP Gestão, e deverá ser revisada e atualizada a partir da operacionalização da empresa e, posteriormente, anualmente pelas Áreas de TI e *Compliance,* a fim de incorporar medidas relacionadas a eventuais atividades e riscos novos ou anteriormente não abordados.

Anualmente, após sua revisão, esta Política será divulgada, por e-mail, aos sócios, funcionários e colaboradores.

A estrutura da presente Política tem início nos princípios norteadores e diretrizes gerais que igualmente regem a segurança cibernética e a segurança da

informação, e se desenvolve a partir da identificação e definição de contingências e procedimentos de engajamento direcionados especificamente aos respectivos objetos desta Política.

PRINCÍPIOS NORTEADORES

Em linha com as melhores práticas atinentes à segurança da informação e à segurança cibernética, a presente Política considera que seus princípios norteadores básicos consistem em (i) confidencialidade, (ii) integridade, (iii) disponibilidade e continuidade e (iv) acesso controlado. Como será abordado nos itens seguintes, sua observância reflete em benefícios evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e outros problemas que possam comprometer os objetos específicos desta Política.

- ✓ **Confidencialidade:** Proteção compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo, permitindo que sejam expostos voluntaria ou involuntariamente dados restritos e que devam ser acessíveis apenas por um determinado grupo de usuários.
- ✓ **Integridade:** Garantia da veracidade de dados, pois estes não deverão ser alterados enquanto forem transferidos ou armazenados. Ameaça à segurança acontece quando um determinado dado (físico ou não) fica exposto ao manuseio por uma pessoa não autorizada, que efetua divulgações e/ou alterações não aprovadas e sem o controle de seu proprietário (corporativo ou privado).
- ✓ **Disponibilidade e Continuidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluirão um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.
- ✓ **Acesso controlado:** O acesso dos usuários a dados será restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

DIRETRIZES GERAIS

Em consonância com os princípios norteadores acima expostos e com as funções usualmente designadas aos mecanismos de controles internos que tenham como objeto a segurança cibernética e a segurança da informação, identificamos abaixo as diretrizes gerais que devem permear os procedimentos de engajamento definidos nesta Política:

- ✓ **Identificação/avaliação de riscos (*risk assessment*):** Identificar os riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção.
- ✓ **Ações de prevenção e proteção:** Estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.
- ✓ **Monitoramento e testes:** Detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.
- ✓ **Criação do plano de resposta:** Ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.
- ✓ **Reciclagem e revisão:** Manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

COMITÊ EXECUTIVO

Tendo em vista a implementação das Diretrizes Gerais, a SP Gestão contará com o Comitê Executivo, composto por pelo menos dois (2) Diretores que é um órgão não-estatutário, de caráter permanente, com poderes deliberativos e tem por objetivo:

- ✓ **Aprovar as políticas e normas corporativos relacionados à Segurança da Informação;**
- ✓ **Assegurar o atendimento as melhores práticas, procedimentos e normas, incluindo a pertinente legislação;**
- ✓ **Avaliar e aprovar propostas e projetos, incluindo a alocação de recursos necessários a investimentos e custos referentes à Segurança da Informação;**
- ✓ **Orientar a adoção de medidas e providências para eliminação ou mitigação de riscos relacionados à Segurança da Informação;**
- ✓ **Posicionar regularmente os administradores, sócios e diretores sobre as atividades do Comitê e fazer as recomendações que julgar apropriadas reportando as respectivas deliberações e orientações incluindo sanções e punições;**
- ✓ **Deliberar sobre a política de sanções referentes às violações de normas de Segurança da Informação; e**
- ✓ **Atribuir responsabilidades de forma a garantir a efetividade e conformidade das decisões e recomendar, quando necessária, a contratação de serviços profissionais especializados em Segurança**

da Informação.

As decisões do Comitê Executivo deverão ser tomadas por maioria dos Diretores e fundamentadas, deverão ser registradas por escrito.
As reuniões do comitê são trimestrais, ou sob demanda.

SEGURANÇA DA INFORMAÇÃO

CONCEITOS ESPECÍFICOS

As regras e procedimentos de controle da segurança da informação serão estruturadas a partir dos seguintes conceitos específicos:

- ✓ **Ambiente físico: dependências físicas da empresa;**
- ✓ **Ambiente lógico: ambiente controlado, eletrônico, onde circularão e serão armazenadas informações e documentos confidenciais, softwares e sistemas;**
- ✓ **Segregação: garante que a informação, por meio de ambiente lógico ou físico, esteja disponível apenas para as pessoas que necessitarem do acesso àquela informação para a realização de suas atividades – conceito "need to know".**

RESPONSABILIDADES

De forma geral, caberá a todos os Colaboradores:

- ✓ **Conhecer e cumprir fielmente esta Política e outros documentos normativos que venham a ser divulgados;**
- ✓ **Evitar situações que possam caracterizar negligência ou que estiverem diretamente violando o Código de Ética, as políticas e diretrizes internas, ou qualquer lei ou regulamento, sob pena de sofrer sanções;**
- ✓ **Assegurar que os recursos tecnológicos e informações disponibilizados sejam utilizados em conformidade às políticas internas;**
- ✓ **Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizadas;**
- ✓ **Procurar a Área de Compliance e/ou a Área de TI quando julgar necessário.**

COMPORTAMENTO SEGURO E CONFIDENCIALIDADE

A SP Gestão se compromete a adotar ferramentas e tecnologias de segurança da informação com o objetivo de garantir a integridade das informações e impedir: (i) acesso e transmissão de informações e arquivos confidenciais a pessoas não autorizadas; (ii) liberação de senhas e códigos de identificação de usuários; e (iii) ocorrência de ataques cibernéticos. A SP Gestão disponibilizará aos

Colaboradores as ferramentas tecnológicas necessárias para o exercício de suas funções incluindo rede interna de arquivos com backup diário e sistema em cloud.

CLASSIFICAÇÃO DE INFORMAÇÕES

A SP Gestão classificará suas informações de acordo com o grau de confidencialidade e criticidade para seus negócios. Todas as informações precisarão estar protegidas durante seu ciclo de vida, conforme aplicável: geração, manuseio, armazenamento, transporte e descarte.

- ✓ **Informações Públicas**: são aquelas destinadas ao público em geral, que poderão ser de caráter informativo. Exemplos: informações disponíveis no website da SP Gestão; comunicados e apresentações institucionais destinadas aos clientes e parceiros; informações genéricas sobre os fundos geridos e companhias investidas (desde que não sejam consideradas como informações internas e/ou confidenciais).
- ✓ **Informações Internas:** são aquelas destinadas ao uso dos Colaboradores da SP Gestão, que só deverão circular e ser compartilhadas internamente a quem tem necessidade de ter acesso (need to know). A divulgação externa não intencional não causaria danos à SP Gestão, a seus clientes ou Colaboradores. Exemplos: atas de comitês internos; relatóriosinternos; cartas e notificações de órgãos reguladores e autorreguladores cujo conteúdo não seja crítico para os negócios da empresa.
- ✓ **Informações Confidenciais:** correspondem a mais alta classificação de segurança para as informações que transitarem na Sp Gestão. Refere-se a informações cuja divulgação não autorizada poderia potencialmente causar danos substanciais, constrangimentos ou penalidades à SP Gestão, seus investidores, Colaboradores, companhias investidas ou mesmo companhias alvo dos fundos geridos. São também as informações cuja divulgação só é permitida a órgãos reguladores ou autorreguladores, Receita Federal, advogados, contadores, consultores especializados, sócios ou investidores. As pessoas que tratarem essas informações têm a responsabilidade de protegê-las e, sempre que possível, somente divulgá-las mediante assinatura de acordos de confidencialidade. Exemplos: informação antecipada e não autorizada de operações, tais como fusões e aquisições; novos produtos e/ou serviços; informações protegidas por sigilo legal; informações relativas aos fundos, companhias investidas e/ou seus negócios; informações societárias e/ou de remuneração dos Colaboradores; etc.

POLÍTICA DE ACESSO (FÍSICO E LÓGICO)

A SP Gestão possui sistema de controle de acesso de pessoas autorizadas às dependências do escritório por cartões magnéticos com possibilidade de utilização de logs e histórico de acesso, com o objetivo de garantir a segregação física das instalações, preservar informações confidenciais e permitir a

identificação das pessoas que tenham acesso a elas; restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais.

No ambiente lógico, a SP Gestão contará com infraestrutura tecnológica que permitirá acesso por perfil de usuário com base no princípio da necessidade da informação para execução das atividades do Colaborador. Além disso, cada Colaborador possuirá um identificador (ID de Colaborador) registrado de forma a assegurar a responsabilidade por suas ações. O sistema proprietário estará integrado e contará com ferramenta de gerenciamento de controle de acesso.

A Área de *Compliance* é responsável por aprovar a liberação e restrição de acesso aos Sistemas de Informação e a outros ambientes lógicos. Os acessos serão periodicamente revisados pela Área de TI, em conjunto com o Compliance.

A qualquer momento, o Colaborador que precisar ter acesso à informação ou à sistema restrito, deverá solicitar a aprovação da Área de Compliance.

Em caso de desligamento de Colaborador, o responsável da área deverá comunicar o respectivo desligamento à Área de TI, com cópia à Área de Compliance, que deverá bloquear imediatamente o acesso do Colaborador a todos os documentos e sistemas da SP Gestão.

DIRETRIZ DE CONTROLE DE ACESSO

Cada Colaborador será responsável pelo uso adequado das informações que possui acesso, o que incluirá as senhas de acesso aos sistemas de informações e crachás de identificação.

O acesso ao Centro de Processamento de Dados (CPD) da SP Gestão é restrito às Áreas de TI, Compliance e Administrativo.

DIRETRIZ PARA SENHA

A senha é a chave de acesso pessoal que garantirá que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Por isso, caberá aos usuários alguns procedimentos de segurança.

- ✓ **Não compartilhar senha, não anotar em arquivos físicos ou de fácil acesso;**
- ✓ **Não utilizar códigos comuns, como próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário ou números sequenciais;**
- ✓ **As senhas precisarão ser diferentes entre si, como as de sites de administradores, bancos, sistemas internos e externos;**
- ✓ **Utilizar preferencialmente senhas distintas para uso corporativo e para uso pessoal; e**
- ✓ **Trocar as senhas periodicamente e sempre que suspeitar de algo.**

POLÍTICA DE BACKUP

A SP Gestão contará com um backup local dos diretórios da rede realizado de segunda a sexta-feira com possibilidade de recuperação de até 5 (cinco) anos com restrições de datas específicas. Será contratada uma empresa de armazenamento de midia digital especializada para guarda dos backups mensais e anuais. Além das plataformas de backup, a SP Gestão contará com um versionamento local de aproximadamente 30 (trinta) dias em dispositivos de *storage.* As rotinas de backup serão validadas diariamentepela equipe de TI. Serão aplicados testes de restore mensais e anuais.

PRIVACIDADE

DIRETRIZ DE UTILIZAÇÃO DE E-MAIL

A SP Gestão possui servidores de e-mail configurados com camadas de proteção de segurança para prevenir vírus ou a execução de códigos maliciosos. Os usuários serão frequentemente orientados a utilizar o serviço de e-mail de forma segura. Seguem diretrizes para utilização de e-mail na SP Gestão.

- ✓ **As contas de e-mail pessoal serão bloqueadas na rede da SP Gestão.**
- ✓ **O e-mail corporativo deverá estar ativo sempre que o usuário estiver trabalhando no computador.**
- ✓ **Não utilizar contas de e-mail pessoal para enviar qualquer tipo de informação confidencial ou interna.**
- ✓ **Ao receber e-mails com links, verificar se o mesmo corresponde ao endereço que aparece na tela. Para tanto, posicionar o ponteiro do mouse sobre o link (não clicar).**
- ✓ **Não abrir, em hipótese alguma, caso não tenha certeza da procedência do envio e da legitimidade do e-mail.**

DIRETRIZ DE UTILIZAÇÃO DE TELEFONE

- ✓ **Número do telefone do usuário:** A SP Gestão disponibilizará telefones para utilização do usuário no desempenho de suas funções profissionais.
- ✓ **Propriedades do número do telefone:** O telefone disponibilizado para o usuário e as conversas associadas a esse número serão de propriedade da SP Gestão e, portanto, poderão ser gravadas. Não deverá ser mantida, portanto, expectativa de privacidade pessoal.
- ✓ **Responsabilidades e forma de uso**: O usuário que utilizar um telefone será responsável por todo conteúdo da conversa e só deverá utilizar o telefone para o seu desempenho profissional na empresa. Será proibido utilizar o telefone para conversas que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Defendam ou possibilitem a realização de atividades ilegais;
- Possam prejudicar a imagem da SP Gestão; ou
- Sejam incoerentes com o nosso Código de Ética.

DIRETRIZ DE UTILIZAÇÃO DE INTERNET

A Área de TI deverá manter os acessos à internet configurados conforme uma política de bloqueios a ser estabelecida pela Área de Compliance.

A Área de TI deverá manter bloqueados os cloud services (como Dropbox, OneDrive e Google Drive), por não ser permitido o uso desse tipo de serviço pelos Colaboradores. O compartilhamento de documentos por meio de cloud services, quando necessário, deverá ser realizado pela Área de TI, com anuência da Área de Compliance.

- ✓ **A instalação de softwares será de responsabilidade da Área de TI e bloqueada por senha.**
- ✓ **É proibido fazer upload ou download de softwares ou dados ilegais (pirataria)**
- ✓ **Não será permitido enviar ou fazer download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.**
- ✓ **Não será permitido o uso de compartilhadores de informações como redes Peer-to-Peer, também conhecidas como redes P2P dentro da SP Gestão. As mesmas serão bloqueadas pelos serviços de firewall.**
- ✓ **A internet disponibilizada aos visitantes será acessível somente por uma rede de visitantes. Essa rede será totalmente segregada da rede interna da SP Gestão e não terá acesso aos servidores da Empresa.**
- ✓ **No caso de perda ou roubo de dispositivos móveis que contenham acesso ao e-mail corporativo, a Área de TI juntamente com a Área de Compliance deverão ser comunicadas imediatamente para fins de bloqueio.**

DIRETRIZ DE UTILIZAÇÃO DA REDE INTERNA

A SP Gestão possui segregação de pastas na rede interna. Cada área possui um perfil de acesso, e todos os perfis terão dois níveis de segurança - leitura e edição.

É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade da empresa.

Dispositivos externos, como pendrives e HD externos não são permitidos devido ao bloqueio das portas USB dos computadores. Em caso de necessidade, a Área de Compliance deverá aprovar a exceção mediante solicitação do responsável da área do Colaborador solicitante.

O usuário não deve obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados à rede interna.

Computadores particulares, de Colaboradores da SP Gestão ou de visitantes, não podemo ser conectados à rede interna da empresa, salvo em situações com prévia autorização da Área de *Compliance*.

OUTRAS DIRETRIZES

Não deixar papéis ou mídias removíveis da empresa contendo informações confidenciais sem o devido armazenamento (política de mesa limpa). Essas informações precisam estar guardadas em armários/gavetas com chave.

Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora.

Os Dados Pessoais dos clientes da SP Gestão devem ser tratados com o devido sigilo e cuidado, devendo ser observado o disposto na Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Em hipótese alguma serão fornecidos a terceiros, sem consentimento do cliente ou previsão legal.

EXCEÇÕES PONTUAIS

Em caráter excepcional, e em função de suas atividades, alguns Colaboradores poderão ter acessos especiais concedidos. Nessas hipóteses, o Colaborador deverá fundamentar por e-mail as razões pela qual entende ser necessário o referido acesso especial, encaminhar a solicitação para a Área de *Compliance* e para o respectivo responsável pela área do colaborador. Nesses casos, ao assinar esta Política, o colaborador se comprometerá de antemão a manter todas as informações que tiver acesso sob sigilo e se responsabiliza no caso de eventual vazamento.

A Área de *Compliance*, depois de verificar as informações, e eventualmente consultar o responsável pela área, poderá solicitar o desbloqueio das ferramentas solicitadas junto a Área de TI ou poderá, alternativamente, escalar o assunto para decisão final do Comitê Executivo.

GESTÃO DE INCIDENTES DE SEGURANÇA

Qualquer suspeita de um incidente de segurança deverá ser imediatamente reportada à Área de TI e à Área de *Compliance*. Nenhum Colaborador deverá investigar por conta própria, ou tomar ações para se defender do ataque, a não ser que seja instruído para tal pela Área de TI, que está capacitada para conter as exposições, analisar os impactos e conduzir investigações, coletando evidências para possíveis ações jurídicas.

Incidentes relevantes que possam causar prejuízos financeiros ou materiais precisarão ser reportados ao Comitê Executivo para que delibere quais ações corretivas deverão ser tomadas.

TESTES PERIÓDICOS

A SP Gesão realizao de testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades. A Área de *Compliance* deverá monitorar os resultados desses testes e manter os registros em caso de falhas e violações desta Política.

Os testes, realizados internamente, e, por prestadores de serviço, consideram:

- ✓ **Atualização constante de inventário de hardware e software, e sua regularidade de licenças e atualização tecnológica;**
- ✓ **Amplitude, cobertura e eficiência das rotinas de backup (evitar que desconfigurações, falhas de acesso, login, etc. gerem diretórios/drivers/máquinas que não estejam realizando backup de rotina);**
- ✓ **Teste de restauro regular de dados de backup;**
- ✓ **Tentativas de invasão, acesso com login e senha em máquinas desprotegidas, etc.;**
- ✓ **Auditar eventos suspeitos de login e alteração de senha;**
- ✓ **Verificação/mapeamento de acessos locais ou remotos;**
- ✓ **Revisão e avaliação de limites de acesso, alçadas de poder, concessão de acesso e revogação;**
- ✓ **Verificação de configurações seguras de equipamentos;**
- ✓ **Verificação e auditoria de diretórios, pastas, arquivos, etc (verificando principalmente arquivos de foto, vídeo, downloads, acesso a sites suspeitos, links recorrentes, etc.);**
- ✓ **Revisão e diligência de prestadores de serviço terceirizados;**
- ✓ **Revisão e dligiência de aplicativos e ferramentas de mercado, parceiros, prestadores de serviço em que haja troca de dados e**

intercâmbio constante;

- ✓ **Verificação de contratos e nível de proteção de cláusulas de confidencialidade, requisitos de prestação de serviço, frequência de report e atendimento a requisitos de segurança por estes;**
- ✓ **Outras mudanças na estrutura de tecnologia, prestadores de serviço, hardware, software, clientes, pareceiros, funcionários, etc. que possam expor a riscos.**

Apontamentos dos testes que forem considerados relevantes, e que demandem revisão dos procedimentos devem ser apontados no Comitê de *Compliance*, bem como as melhorias implementadas. Caso tenham representatividade, devem ser apontados no Relatório Anual de *Compliance*, com foco nos riscos trazidos, e os aprimoramentos propostos para melhoria do ambiente tecnológico e de segurança da gestora.

TREINAMENTO

A Área de *Compliance*, será responsável por difundir as melhores práticas dentro da SP Gestão, por meio de treinamentos, sempre que houver uma atualização nas diretrizes de segurança ou demais políticas internas.

A frequência e renovação destes treinamentos presenciais dependerá da velocidade de crescimento e novas contratações da gestora, e será considerado pela diretoria. Independentemente de novos treinamentos, cada novo colaborador tem acesso a todas as políticas e manuais internos para aculturamento das regras definidas pela gestora.

Sempre que houver mudanças significativas nas políticas (motivadas por decisão interna, ou adaptação a novos normativos), ou tópicos de segurança, serão promovidos treinamentos de reciclagem, mesmo se não houverem novos colaboradores contratados.

A SP Gestão pode fazer uso de suas consultorias externas para apoio profissional em treinamentos e reciclagens. Os treinamentos contam com lista de presença. Os treinamentos tem periodicidade anual, caso haja mudança nos quadros de colaboradores, ou, atualizações significativas de políticas e procedimentos.

SEGURANÇA CIBERNÉTICA

Em consonância com as Diretrizes Gerais apresentadas acima, a SP Gestão adotará procedimentos de Segurança Cibernética, listados abaixo, sendo certo que a supervisão desses procedimentos e desta Política cabem à Área de TI, com o apoio da Área de *Compliance*. A Área de *Compliance* deverá apresentar o resultado dos testes e monitoramento periódicos realizados com base nessa Política ao Comitê Executivo e ao Comitê de Risco e de Compliance. O Comitê Executivo e o Comitê de Risco e de *Compliance*, com base nesses relatórios, poderão propor (i) ajustes na presente Política, assim como (ii) planos de ação específicos.

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS (RISK ASSESSMENT)

A SP Gestão identifica e avalia os principais riscos cibernéticos aos quais está exposta. O Guia de Cibersegurança da Anbima define os ataques mais comuns de criminosos cibernéticos (cybercriminals):

http://www.anbima.com.br/data/files/F5/62/AB/91/FBC206101703E9F5A8A80AC2/Guia-de- Ciberseguranca-ANBIMA.pdf.:

- ✓ **Malware (e.g. vírus, cavalo de troia, spyware e ransomware);**
- ✓ **Engenharia Social;**
- ✓ **Pharming;**
- ✓ **Phishing scam;**
- ✓ **Vishing;**
- ✓ **Smishing;**
- ✓ **Acesso pessoal;**
- ✓ **Ataques de DDoS e botnets; e**
- ✓ **Invasões (advanced persistent threats).**

AÇÕES DE PREVENÇÃO E PROTEÇÃO

Em complemento aos procedimentos de Segurança da Informação previstos acima, ao incluir os novos equipamentos e sistemas em produção, a SP Gestão contará com recursos anti- malware em estações e servidores de rede, como antivírus e firewall. Da mesma maneira, monitorará o acesso a websites e restringirá a execução de softwares e/ou aplicações não autorizadas.

Adicionalmente, a SP Gestão disporá de recursos para (i) realizar verificação de configurações, de modo a mitigar vulnerabilidades que possam surgir em razão da inclusão de novos equipamentos e sistemas em produção, incluindo a realização de testes prévios quando novos equipamentos e sistemas forem implementados em ambientes de homologação e de prova de conceito, (ii) implementar anti-malware em estações e servidores de rede, como antivírus e firewall, permitindo, também, a verificação do acesso a websites e restrição a execução de softwares e/ou aplicações não autorizadas, bem como (iii) realizar backup das informações e dos diversos ativos da instituição, conforme as disposições do Plano de Continuidade do Negócio.

MONITORAMENTO

Os sistemas, serviços, dados, informações disponíveis na SP Gestão ou por esta disponibilizados, para serem usados pelos Colaboradores, não deverão ser interpretados como sendo de uso pessoal. Todos os Colaboradores deverão ter ciência de que o uso estrá sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente da SP Gestão, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pelas Áreas de TI, Compliance e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da SP Gestão, e, conforme o caso, servirá como evidência em processos administrativos, arbitrais e/ou judiciais.

A Área de TI da SP Gestão elaborará roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade.

Da mesma maneira deverá diligenciar de modo a manter inventários atualizados de hardware e software, bem como os sistemas operacionais e softwares de uso atualizados.

Periodicamente, a Área de TI realizará testes de segurança no seu sistema de segurança da informação e proteção de dados. Dentre as medidas, serão incluídas, mas sem se limitar:

- ✓ **Verificação dos logs dos Colaboradores;**
- ✓ **Alteração periódica de senha de acesso dos Colaboradores;**
- ✓ **Segregação de acessos;**
- ✓ **Manutenção periódica de hardwares; e**
- ✓ **Backup diário, realizado em dispositivos de armazenamento locais e redundância em nuvem.**

Sem prejuízo dos testes realizados, a SP Gestão realizará, de tempos em tempos, simulações de ataques e respostas possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da SP Gestão, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

Essa política de segurança cibernética será revisada quano do inicio da sua operação e, periodicamente, em prazo não superior à 12 (doze) meses.

PLANO DE RESPOSTA

Havendo indícios ou suspeita fundamentada, a Área de TI deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento. Na hipótese de vazamento de informações sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater o evento identificado. Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade. Eventos que envolverem a segurança das informações sigilosas ou que forem decorrentes de quebra de segurança cibernética deverão ser formalizados pela Área de TI para deliberação do Comitê Executivo.

AÇÕES EM CASO DE NÃO CONFORMIDADE

Os descumprimentos à esta Política serão submetidos ao Diretor responsável pela Área de Compliance, que endereçará o referido descumprimento e suas eventuais consequências ao Comitê Executivo.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão, desassociação, desligamento ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

A omissão diante da violação conhecida da lei ou de qualquer disposição desta Política não é uma atitude correta e constitui uma violação ao Código de Ética da SP Gestão. No caso de conhecimento sobre o descumprimento a esta Política, o Colaborador deverá informar tal descumprimento a qualquer membro da Área de *Compliance*, que terá o dever de analisar e recomendar as respectivas ações corretivas para o Comitê Executivo.

CONSIDERAÇÕES FINAIS

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justificará desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, deverão ser consultadas as Áreas de *Compliance* e/ou TI.

A determinação da alta administração da SP Gestão é que, por ocasião da decisão pela respectiva operacionalização, este documento deverá ser devidamente revisado.

A SP Gestão está comprometida em lidar com informações pessoais não públicas sobre seus clientes, de forma responsável e transparente. Sendo assim, as políticas, controles e estruturas da SP Gestão estarão aderentes à LGPD quando de sua entrada em vigor, em agosto de 2020, e serão continuamente aprimorados.

PLANO DE CONTINUIDADE DE NEGÓCIOS

O Plano de Continuidade de Negócios foi elaborado com o objetivo de identificar e definir os princípios, conceitos e diretrizes relacionados à continuidade de negócios, os quais deverão ser adotados por todos os funcionários e sócios da SP Gestão, bem como terceirizados que possuírem acesso ao escritório, rede interna e sistemas.

Os Colaboradores deverão obrigatoriamente aderir a esta Política ao ingressar na SP Gestão, bem como concordar com suas posteriores e eventuais alterações. Tal adesão será realizada por meio de assinatura eletrônica de um Termo de Adesão e Compromisso que prevê, dentre diversas obrigações, a necessidade de os Colaboradores manterem confidenciais as informações a que tiverem acesso quando da realização de suas atividades profissionais.

Esta Política foi elaborada e deve ser interpretada em consonância com os

demais manuais e políticas da SP Gestão, e deverá ser revisada e atualizada a partir da operacionalização da empresa e, posteriormente, anualmente pelas Áreas de TI e *Compliance*, a fim de incorporar medidas relacionadas a eventuais atividades e riscos novos ou anteriormente não abordados.

Anualmente, após sua revisão, esta Política será divulgada, por e-mail, aos sócios, funcionários e colaboradores.

A estrutura da presente Política tem início no princípio norteador que rege a continuidade dos negócios. Se desenvolve a partir da identificação de contingências e procedimentos de engajamento direcionados especificamente aos respectivos objetos desta Política.

PRINCÍPIO NORTEADOR

Em linha com as melhores práticas atinentes à continuidade de negócios, a presente Política considera que seu princípio norteador básico consiste em disponibilidade e continuidade. A observância do item detalhado abaixo reflete em benefícios evidentes ao reduzir os riscos que possam comprometer o objeto específico desta Política.

Disponibilidade e Continuidade: Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluirão um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à continuidade acontecem quando a informação deixa de estar acessível para quem necessita dela.

O PCN é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los no prazo previamente estabelecido.

Para identificação das posições e sistemas críticos, devem ser considerados os riscos a seguir, no caso de interrupção do processo:

- ✓ **impacto financeiro** – situações em que a descontinuidade de negócios possa atingir as carteiras ou fundos sob gestão, ou a situação financeira e patrimonial da SP Gestão;
- ✓ **impacto legal** – descontinuidade de negócios passível de gerar consequências legais aos fundos e carteiras sob gestão, seus cotistas, ou mesmo à própria SP Gestão;
- ✓ **impacto de imagem** – risco de a descontinuidade de negócios impactar a reputação e confiabilidade da SP Gestão perante seus clientes e/ou o público investidor;
- ✓ **acidentes, casos fortuitos e força maior** – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle da SP Gestão, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes

proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

CONTINUIDADE DE NEGÓCIOS

RESPONSABILIDADES

A Área de Compliance deverá se certificar da implementação do Plano de Continuidade de Negócios para garantir a continuidade dos processos críticos da SP Gestão em casos de eventos inesperados que afetem parcial ou integralmente a sua capacidade operacional, assegurando a realização de testes periódicos, conforme aplicáveis, que atestem sua efetividade. Este documento tem por objetivo informar, treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais.

À Área de Compliance caberá (i) manter este PCN sempre atualizado; e (ii) treinar os Colaboradores para casos de necessidade de acionamento do PCN.

Os detalhamentos do PCN constam em documento específico.

AÇÕES EM CASO DE NÃO CONFORMIDADE

Os descumprimentos à esta Política serão submetidos ao Diretor responsável pela Área de *Compliance*, que endereçará o referido descumprimento e suas eventuais consequências ao Comitê Executivo.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão, desassociação, desligamento ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

A omissão diante da violação conhecida da lei ou de qualquer disposição desta Política não é uma atitude correta e constitui uma violação ao Código de Ética da SP Gestão. No caso de conhecimento sobre o descumprimento a esta Política, o Colaborador deverá informar tal descumprimento a qualquer membro da Área de Compliance, que terá o dever de analisar e recomendar as respectivas ações corretivas para o Comitê Executivo.

POLÍTICA DE CERTIFICAÇÃO

A quem se aplica?

Sócios, diretores e funcionários da SP Gestão, que desempenhem atividades diretas de gestão profissional de carteiras de títulos e valores mobiliários, com alçada de decisão sobre o investimento, desinvestimento e manutenção dos recursos dos veículos a cargo da SP Gestão (“Colaboradores”).

Assim sendo, a SP Gestão requer dos profissionais elencados acima a “Certificação de

Gestores ANBIMA" (CGA), sempre que aplicável às suas atividades.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de *Compliance*.

Responsabilidades

O Diretor de *Compliance* é responsável pelos controles que garantem o atendimento às demandas relativas à necessidade ou não de certificação dos profissionais da SP Gestão.

Revisão e Atualização

Esta política deverá ser revisada a atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

Controles

O Diretor de *Compliance* mantém controle dos Colaboradores da SP Gestão com as seguintes informações:

- ✓ **dados profissionais;**
- ✓ **data de admissão;**
- ✓ **data de desligamento, quando aplicável;**
- ✓ **atividade exercida;**
- ✓ **área de atuação;**
- ✓ **cargo;**
- ✓ **tipo de gestor, quando aplicável;**
- ✓ **endereço eletrônico individual;**
- ✓ **se dispõe de certificação ANBIMA e a sua validade.**

O Diretor de *Compliance* é responsável por verificar que todos os Colaboradores elegíveis à CGA sejam certificados e que as respectivas certificações estejam válidas.

A CGA é válida por prazo indeterminado, desde que o profissional esteja exercendo atividades que dela sejam objeto.

Compete ao Diretor de *Compliance* garantir que um Colaborador não certificado não exerça função que pressuponha certificação ou que a obtenha nos termos ditados pela ANBIMA.

Caso o Colaborador não disponha da certificação aplicável, a Diretoria de Compliance é responsável por manter a documentação formal que evidencie o afastamento do **Colaborador das atividades elegíveis à certificação.**

Cabe ao Diretor de *Compliance* monitorar o cumprimento das demais diretrizes estabelecidas no Código de Certificação.

As certificações pendentes e o afastamento das funções elegíveis devem ser reportadas

ao Comitê de *Compliance*, que deve monitorar a sua devida regularização.

Quaisquer outras situações identificadas aplicáveis à matéria devem ser objeto de análise, aprovação, formalização ou eventual assunção de risco no âmbito do Comitê de *Compliance*.

Admissões de Colaboradores

O Diretor de *Compliance* deve acompanhar as informações sobre novas admissões e transferências internas, e se os novos Colaboradores possuem a respectiva certificação ANBIMA eventualmente aplicável.

Os candidatos a cargos que pressupõem certificação CGA devem ser contratados com certificações válidas. Eventuais exceções deverão ser avaliadas pelo Diretor de Compliance e reportadas ao Comitê de Compliance para controle das respectivas atividades e possível afastamento das funções até a efetiva obtenção da certificação aplicável.

Compete à Área de Compliance cadastrar, no site da ANBIMA, o novo funcionário e/ou Colaborador transferido internamente, o que deve ocorrer no mesmo mês da contratação/transferência. Além disso, deve manter sempre atualizados os seus controles internos.

Licenças e Desligamentos

No caso de licenças e desligamentos, o Diretor de *Compliance* deve verificar se o Colaborador está vinculado à SP Gestão no site da ANBIMA, e, nesse caso, desvincular o profissional, o que deve ocorrer impreterivelmente no mesmo mês de licença e/ou desligamento.

Os profissionais em licença não devem continuar vinculados no período em que estiverem de licença. Quando retornarem, deverá ser efetuado o vínculo novamente.

Banco de Dados da ANBIMA

O Diretor de *Compliance* é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado.

O controle de admissão, licença e demissão consta na agenda regulatória do Comitê de *Compliance*, onde são formalizados tais registros, devendo as eventuais atualizações junto à entidade ocorrer até o último dia do mês subsequente ao evento.

Código de Ética e Conduta Profissional

Cabe ao Diretor de Compliance requerer dos novos Colaboradores a assinatura formal do Termo de Conhecimento e Adesão ao Código de Ética e Conduta Profissional e das demais políticas da SP Gestão, até o último dia do mês subsequente à sua contratação.

CONSIDERAÇÕES FINAIS

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justificará desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, deverão ser consultadas as Áreas de Compliance e/ou TI.

A determinação da alta administração da SP Gestão é que, por ocasião da decisão pela respectiva operacionalização, este documento deverá ser devidamente revisado.

A SP Gestão está comprometida em lidar com informações pessoais não públicas sobre seus clientes, de forma responsável e transparente.

Nesse contexto, as políticas, controles e estruturas da SP Gestão estarão aderentes à LGPD quando de sua entrada em vigor, em agosto de 2020, e serão continuamente aprimorados.

Esta política de Controles Internos é parte integrante das políticas e normas que guiam as relações da SP Gestão e de seus colaboradores, os quais, ao assinar o Protocolo de Recebimento e Leitura, concordam absolutamente com as diretrizes nela fixadas. A desobediência a qualquer das normas aqui expostas é tida como infração contratual, sujeitando seu autor às sanções cabíveis.

ANEXO I

Quadro de Obrigações Periódicas da GESTORA

Informações Periódicas

Norma	**Artigo**	**Tema**	**Obrigação**	**Período**
ICVM 558	22, *caput*	Relatório Anual	Entrega do relatório à administração da GESTORA	Último dia útil de abril a cada ano (data base 31/12)
ICVM 558	15, *caput*, I e II	Formulário de Referência	Envio do FR pelo CVMWeb	Anualmente, até 31/03 (data base 31/12)
ICVM 510	1.º, II	Declaração Eletrônica de Conformidade	Envio pelo CVMWeb	Anualmente, até 31/03

				(data base 31/12)
ICVM 301	3.º, § 2.º	Política de PLD	Atualização dos dados cadastrais dos clientes/investidores e/ou verificação da efetiva atualização dos citados dados pelo administrador/distribuidor	No máximo a cada 24 (vinte e quatro) meses
ICVM 301	7.º - A, *caput*	Política de PLD	Declaração Negativa através da CVMWeb à CVM ou ao órgão que esta indicar, desde que não tenha sido prestada nenhuma comunicação durante exercício anterior ao COAF acerca de operações ou propostas de operações com indícios de lavagem de dinheiro	Anualmente, até o último dia útil do mês de janeiro
Código Certificação ANBIMA	23, § 2.º	Base de Dados ANBIMA	Inclusão e atualização no banco de dados administrado pela ANBIMA das informações relativas aos colaboradores certificados, em processo de certificação, com a certificação vencida, e/ou em processo de atualização da certificação	Mensalmente, até o último dia do mês subsequente à data do evento

Informações Eventuais

Norma	**Artigo**	**Tema**	**Obrigação**	**Período**
ICVM 510	1.º, I	Atualização de dados cadastrais	Atualização via CVMWeb	7 (sete) dias úteis contados do evento que

				deu causa à alteração
ICVM 301	7.º, *caput*, I e II	Política de PLD	Comunicar ao COAF todas as transações, ou propostas de transação, que possam ser consideradas sérios indícios de crimes de lavagem ou ocultação de bens, direitos e valores provenientes de infração penal	24 (vinte e quatro) horas a contar da ocorrência
ICVM 558	16, VIII	Violação à regulação	Informar à CVM a ocorrência ou indícios de violação da sua regulação	10 (dez) dias úteis da ocorrência ou sua identificação
Ofício Circular CVM/SIN 10/15	Item 37	Atualização cadastral	Envio à CVM do contrato social atualizado, no caso de mudança de denominação social ou de substituição de diretor responsável pela gestão	7 (sete) dias úteis do fato que deu causa à alteração

ANEXO II

Modelo de Relatório de Aderência

Ilmos. Srs.

Sócios e Diretores da

[GESTORA]

Ref.: Relatório Anual – Instrução CVM nº 558, de [ano]

Prezados Senhores,

Em cumprimento ao disposto no art. 22 da Instrução CVM n.º 558, de 26 de março de 2015 ("ICVM 558"), vimos apresentar a V.Sas. o relatório pertinente às atividades da **[GESTORA]**, ("GESTORA") no ano de [•] ("Relatório").

De acordo com a ICVM 558, o mencionado Relatório contém:

- ✓ As conclusões dos exames efetuados;
- ✓ As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
- ✓ A manifestação do diretor responsável pela administração de carteiras de valores mobiliários, ou, quando for o caso, pelo diretor responsável pela gestão de risco, a respeito das eventuais deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las (cf. art. 22, I, II e III, da ICVM 558).

Este relatório ficará à disposição da Comissão de Valores Mobiliários ("CVM") na sede da GESTORA, para eventuais posteriores checagens, verificações e/ou fiscalizações por parte da CVM.

Além dos aspectos acima, V.Sas. encontrarão também, no corpo do presente Relatório, os resultados do Teste de Aderência determinado na Política de *Compliance* e Controles Internos da GESTORA, e o correspondente parecer final do Diretor *Compliance* e Controles Internos, que assina o presente documento.

Assim sendo, passamos abaixo à exposição dos elementos pertinentes do presente Relatório.

I. Conclusão dos Exames Efetuados (ICVM 558, art. 22, I)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

II. **Recomendações sobre as Deficiências Encontradas e Cronogramas de Saneamento (ICVM 558, art. 22, II)**

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo estimativas de datas de acompanhamento e conclusão das soluções)

III. **Manifestações dos Diretores Correspondentes de Gestão e de Risco sobre as Verificações Anteriores e Respectivas Medidas Planejadas (ICVM 558, art. 22, III)**

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo os resultados esperados e os efetivamente alcançados)

IV. **Parecer Final do Diretor de Risco, *Compliance* e Controles Internos**

(enumerar detalhadamente)

Sendo então o que nos cumpria para o momento, aproveitamos o ensejo desta correspondência para nos colocarmos à disposição de V.Sas. para os eventuais esclarecimentos porventura reputados necessários.

Atenciosamente,

[•]

[GESTORA]

Diretor de *Compliance* e Controles Internos

ANEXO III

Orientações Gerais sobre o Conteúdo Técnico do Teste de Aderência

A **Diretoria de *Compliance* e Controles Internos** deve estruturar registro e controle **ativo, ao longo do ano,** para composição do Relatório Anual (descrito no Anexo I), ao menos sobre as seguintes matérias relacionadas abaixo.

Tais temas devem – ao longo do ano – ser endereçados e monitorados no Comitê de *Compliance*, Controles Internos e Ética, e, quando necessário, ser objeto de acompanhamento próximo da alta gestão (sócios e diretores) da GESTORA.

Tal controle deve ser feito em planilhas específicas, servindo como ferramenta de *compliance* e controle de risco operacional.

O controle ao longo do ano dos eventos abaixo, e seu registro é uma das obrigações centrais do Comitê de *Compliance*, Controles Internos e Ética.

I. Conclusão dos Exames Efetuados (ICVM 558, art. 22, I)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

→ Deve constar em planilha de controle o registro dos seguintes eventos (ao menos) ocorridos ao longo do ano, suas consequências / perdas e as atitudes corretivas adotadas:

- ✓ **erros operacionais atinentes a operações dos fundos;**
- ✓ **erros relativos a movimentação financeira de clientes;**
- ✓ **falhas em pagamentos de remuneração de distribuidores ou corretagem de fundos pagas a corretoras ou quaisquer prestadores de serviço;**
- ✓ **desenquadramentos de carteiras, comunicação com administrador e reenquadramento;**
- ✓ **qualquer outro descumprimento de norma legal constatado;**
- ✓ **eventos de liquidez dos fundos;**
- ✓ **falhas operacionais relativas à infraestrutura tecnológica e plano de correção implementado;**
- ✓ **acionamentos do plano de contingência e continuidade de negócios;**
- ✓ **falhas de fornecedores;**
- ✓ **falhas relativas a quaisquer políticas internas ou normas legais e plano de correção implementado;**
- ✓ **mudanças expressivas em parâmetros de liquidez dos fundos;**
- ✓ **eventos relacionados ao gerenciamento de risco, com especial atenção a risco**

de crédito e liquidez;

- ✓ **ofícios ou qualquer outro alerta e comunicação recebidos de reguladores, ou processos administrativos junto à CVM, ANBIMA e demais reguladores aplicáveis, ou em alçadas do poder judiciário;**
- ✓ **descumprimento de obrigações relativas à certificação;**
- ✓ **descumprimento de contratos quaisquer;**
- ✓ **quebra de dever de sigilo contratual;**
- ✓ **quaisquer eventos adicionais considerados relevantes pelo *compliance* e que tenham colocado em risco a empresa, seus colaboradores, clientes, carteiras sob gestão ou as boas práticas de mercado.**