

Política de Supervisão e Controles Internos

Vostrum Gestão de Investimentos Ltda.

Sumário

1. Introdução	3
2. Comitê de Compliance	3
3. Responsabilidades do Diretor de Risco e Compliance	3
4. Supervisão	4
5. Identificação de Erros	4
6. Políticas Internas	5
6.1. Política de Segurança da Informação	5
6.1.1. Confidencialidade	5
6.1.2. Propriedade Intelectual	6
6.1.3. Segurança Cibernética	7
6.1.4. Plano de Continuidade de Negócios	7
6.1.5. Segregação das Atividades	9
6.2. Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo	9
7. Política de Treinamento	9

1. Introdução

Sob responsabilidade final do Diretor de Risco e Compliance indicado pela Gestora nos termos de seu contrato social, a área de Compliance é responsável pelas regras, procedimentos e controles internos que supervisionam as atividades da Vostrum Gestão de Investimentos garantindo o cumprimento do Código de Ética, auto regulação ANBIMA e normas legais.

2. Comitê de Compliance

Caberá ao Comitê de Compliance assessorar o Diretor de Risco e Compliance sobre questões relacionadas a diretrizes legais, manuais internos da Gestora e deste manual de compliance.

3. Responsabilidades do Diretor de Risco e Compliance

O Diretor de Risco e Compliance indicado pela Vostrum Gestão de Investimentos está incumbido de:

- zelar pelas informações da Gestora;
- gerir possíveis conflitos de interesse;
- revisar e divulgar os padrões e políticas da empresa;
- fazer cumprir os padrões e políticas da empresa;
- assegurar a realização da reunião periódica do Comitê de Compliance;
- implementar a cultura da empresa para garantir a execução dos controles internos e melhores práticas.

4. Supervisão

O monitoramento possui como objetivo avaliar se as atividades da Gestora estão em conformidade com as normas e procedimentos internos, bem como de acordo com o órgão regulador.

- Operações: monitorar constantemente as transferências financeiras para identificação de anormalidades, lavagem de dinheiro ou inconsistência patrimonial. A qualquer momento, sob a identificação de tais eventos, a área responsável poderá solicitar demais explicações ou comunicar ao órgão regulador as inconsistências devidas.
- Divulgação de informações: as partes envolvidas na execução do negócio devem direcionar os documentos de comunicação de caráter promocional para a área de Compliance anteriormente a sua divulgação.
- Condutas: avaliar e penalizar possíveis condutas de seus sócios ou colaboradores, pessoais ou profissionais, que possam prejudicar a imagem da Gestora.
- Conflitos de interesse: avaliar continuamente o modelo de negócio com o intuito de identificar conflitos de interesse.
- Equipamentos pessoais: é de responsabilidade dos sócios e colaboradores garantirem a segurança de informações e riscos associados à utilização de equipamentos pessoais.
- Autorregulação: a Gestora realizará revisões das suas políticas internas e procedimentos quando julgar necessário a fim de garantir a execução de melhores práticas.

5. Identificação de Erros

A partir da supervisão das atividades da Gestora, a área de Compliance deverá:

- comunicar aos responsáveis pelo compliance a identificação dos erros;
- corrigir as deficiências encontradas nos padrões internos da empresa;

- implantar soluções preventivas;
- divulgar aos sócios e colaboradores da Gestora todo processo desenvolvido para comunicação, correção e contenção.

Sócios e colaboradores devem comunicar ao Compliance da empresa qualquer situação que julguem desviar dos padrões desenvolvidos pela Gestora.

6. Políticas Internas

6.1. Política de Segurança da Informação

A política de segurança da informação visa proteger os sócios, colaboradores, clientes e outros *stakeholders* da organização sobre o tratamento incorreto de informações que possam vir a prejudicar o andamento das atividades da empresa.

6.1.1. Confidencialidade

A Vostrum Gestão de Investimentos adota as melhores práticas para atender as exigências da Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

A Vostrum mantém os dados cadastrais de seus clientes, bem como informações protegidas por sigilo bancário e fiscal, única e exclusivamente com o objetivo de cumprir suas obrigações contratuais e estabelecer a relação comercial entre as partes. A Vostrum não solicita, não coleta e não armazena nenhum tipo de dado pessoal sensível, nos termos da definição estabelecida pelo inciso II do artigo 5º da Lei 13.709 de 14 de agosto de 2018.

Adicionalmente, a Vostrum mantém um Acordo de Confidencialidade com todos os seus sócios e colaboradores, os quais se obrigam a

manter a segurança e o sigilo de todas as informações compartilhadas pelos e com os clientes.

Visando garantir a confidencialidade das informações estratégicas, tanto da empresa quanto de seus clientes, são implementados os seguintes níveis de acesso::

- a) Colaboradores sem acesso às decisões de investimento:
 - acesso apenas às informações necessárias para cumprir suas obrigações contratuais e estabelecer a relação comercial entre as partes, nos termos da LGPD.

- b) Colaboradores integrantes dos Comitês de Risco, Compliance e Gestão:
 - acesso a todas as informações do nível anterior
 - informações a respeito das estratégias de investimento adotadas pela Vostrum
 - informações específicas de cada carteira administrada
 - todas as informações cadastrais dos clientes
 - formulário de suitability

- c) Sócios e administradores:
 - acesso a todas as informações do nível anterior
 - informações estratégicas da empresa e seu modelo de negócios

6.1.2. Propriedade Intelectual

Todo material de divulgação e análise produzido internamente para atender as necessidades específicas das atividades do negócio são de propriedade da Gestora. Os materiais utilizados de terceiros são de propriedade dos seus respectivos autores. A utilização do conteúdo desenvolvido além de sua finalidade acima citada, ficará sujeita a permissão do Conselho de Administração.

6.1.3. Segurança Cibernética

Todos os sistemas utilizados pela Vostrum permitem a definição de níveis de permissões de acesso, a depender da atividade e necessidade. Os documentos e dados confidenciais são armazenados em servidores cloud, via serviço Google Workspace, em uma estrutura de backup permanente. Além disso, os sistemas mantêm logs de acesso, garantindo a rastreabilidade de todo o processo.

Todo colaborador possui seu login e senha pessoais, permitindo acesso aos documentos, informações e sistemas pertinentes à sua atividade com rastreabilidade. A política de senhas é definida por sistema gerenciador de senhas, o qual permite habilitar e desabilitar o acesso dos usuários aos sistemas contratados.

Periodicamente, são realizados testes de validação e integridade de dados para fins de *disaster recovery*.

6.1.4. Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios é um conjunto de sistemas e protocolos para garantir que a empresa consiga evitar a interrupção de suas atividades ou se recuperar rapidamente de uma interrupção significativa. Para isso, é importante conscientizar os integrantes da empresa sobre possíveis contingências que poderão alterar a rotina usual da sociedade causando perdas e prejuízos. Todos os membros da empresa devem estar cientes sobre os procedimentos de backup e salvaguarda de informações de suas atividades, evacuação de instalações físicas e conceitos de melhores práticas para segurança no ambiente de trabalho.

Como forma de minimizar impactos imprevistos, o Plano de Continuidade de Negócios da Vostrum trata de 2 pilares:

Tecnologia:

A empresa mantém sistema centralizado de controle de senhas, o que permite garantir o acesso aos sistemas de apoio e gestão apenas às pessoas autorizadas. Os dispositivos utilizados pelos colaboradores (hardware) são móveis (notebooks e smartphones), o que permite que suas atividades possam ser realizadas de locais remotos. Adicionalmente, a infraestrutura de comunicação é composta por links de internet redundantes.

Em caso de evento que possa comprometer o acesso físico às instalações e equipamentos da empresa, a manutenção dos negócios será preservada, uma vez que todos os documentos, informações e sistemas operam em ambiente de cloud computing, permitindo o acesso remoto a esta estrutura.

Fornecimento de Serviços:

Pela natureza de sua atividade ser exclusivamente a gestão de recursos, todos os serviços de custódia, precificação de ativos, registro de operações, dentre outros, são realizados por fornecedores contratados. Parte destes serviços são realizados por instituições financeiras e parte por fornecedores de soluções tecnológicas. Em ambos os casos, são estruturas que fogem do alcance de uma ação da Vostrum para garantia de continuidade de suas operações.

Diante disso, além de adotar um rígido critério de seleção de fornecedores, a Vostrum mantém um canal de comunicação permanente com eles, por vários meios (e-mail, sistemas de chat e telefone), a fim de minimizar os impactos que eventos adversos em terceiros possam causar em sua própria operação.

6.1.5. Segregação das Atividades

A Vostrum Gestão de Investimentos, em cumprimento com a regulação vigente, disponibiliza aos seus colaboradores a Política de Segregação de Atividades, com maior profundidade do tema abordado.

6.2. Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo

A Vostrum Gestão de Investimentos, em cumprimento com a regulamentação vigente, disponibiliza aos seus colaboradores a Política de Prevenção à Lavagem de Dinheiro, com maiores detalhes sobre o tema.

7. Política de Treinamento

Em vista do Artigo 24º, inciso III da instrução CVM 21/2021, todo sócio, colaborador e/ou empregado que participa do processo de decisão de investimento ou acesse informações confidenciais deverá receber treinamento adequado quanto às normas e regulamentos da CVM, melhores práticas da Anbima, bem como sobre os manuais e práticas observadas pela própria Vostrum.

Através de um programa interno de educação continuada, a Vostrum Gestão de Investimentos incentivará seus colaboradores e sócios a adquirirem certificações específicas do mercado financeiro. Cabe à Diretoria Executiva a definição de cronograma periódico de treinamento e atualização para as pessoas envolvidas.