POLÍTICA DE CONTROLES INTERNOS

Regras, procedimentos e descrição dos controles internos

Atualmente, a Instituição desempenha atividades voltadas tanto para a administração de carteiras de títulos e valores mobiliários e gestão de fundos de investimento.

No que se refere às funções de controles internos e conformidade da Instituição, as mesmas de responsabilidade do seu Diretor de *Compliance*, que possui atuação independente e reporta-se somente à diretoria, enquanto órgão societário da Gestora.

A área de *compliance* da Instituição atualmente é formada por seu Diretor de *Compliance* auxiliado por um analista. Dentre as atribuições da área de *Compliance*, destacam-se as seguintes:

- Zelar pela observância das normas, políticas e procedimentos aplicáveis;
- Esclarecer dúvidas dos demais colaboradores sobre as políticas internas;
- Produzir os relatórios aplicáveis;
- Monitorar as atividades dos demais colaboradores para averiguar a sua aderência à presente Política e normas legais e regulamentares aplicáveis.

Especialmente em relação ao Diretor de *Compliance*, o mesmo possui as seguintes obrigações e atribuições:

- Avaliar possíveis indícios de condutas contrárias a este Manual, inclusive conduzindo investigações, se entender necessário;
- Elaborar a revisão periódica deste Manual e demais políticas internas da Instituição;
- Promover a ampla divulgação das regras internas da Instituição;
- Apreciar os casos que cheguem a seu conhecimento sobre descumprimento de leis, do presente Manual e demais políticas internas da Instituição;
- Tratar todos os assuntos que cheguem a seu conhecimento com sigilo e preservando os interesses e a imagem institucional e corporativa da Instituição, assim como a dos Colaboradores envolvidos;
- Aplicar sanções, em conjunto com a Diretoria, quando aplicável e necessário.

→Controles Internos

O Diretor de *Compliance* é responsável pelos controles internos da Instituição. Como o Diretor de *Compliance* da Instituição concentra as atividades de *compliance*, controles internos, PLD e gestão de riscos, e o mesmo será responsável pela coordenação entre tais atividades, nos termos exigidos pela autorregulação aplicável.

A área de *Compliance* tem autonomia e autoridade para questionar os riscos assumidos nas operações realizadas pela instituição e, caso o faça, o colaborador responsável pela

atividade questionada deverá prontamente responder aos questionamentos da área de *Compliance*.

Dentre as formas de assegurar a independência da área de *Compliance* e ausência de conflitos de interesse com a administração de recursos de terceiros e distribuição, pode-se mencionar a segregação de atividades, a ser detalhada em item específico abaixo.

→Segregação de Atividades

Atualmente, a Instituição não exerce outras atividades que não a gestão de recursos de terceiros. Sem embargo, a Gestora conta com a presente política de segregação de atividades de modo a explicitar os cuidados tomados caso eventualmente a Gestora venha a exercer outras atividades.

(a) Segregação formal
A Instituição mantém a segregação lógica, funcional e de processos entre suas diversas áreas, implementando controles que monitoram a execução de suas atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

A Gestora conta com segregação formal de atribuições e responsabilidades, expressas em seus documentos societários (divisão de diretorias, por exemplo) e nos manuais e políticas por ela adotados.

(b) Segregação Física
O acesso ao público externo será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração, e desde que acompanhadas dos Colaboradores. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências da Instituição, exceto nos casos permitidos pela área de Recursos Humanos para processo de desligamento, de aposentadoria ou afins. O atendimento a clientes nas dependências da Instituição deve ocorrer, necessariamente, nas salas destinadas para reuniões e visitas.

(c) Segregação Eletrônica
Todos os Colaboradores têm acesso à rede e aos sistemas internos da Instituição, mas há restrição de acesso aos computadores pessoais, e-mails e áreas na rede dedicadas aos arquivos pessoais.

O *Compliance* da Instituição deverá se certificar, através do monitoramento e testes periódicos, da manutenção da segregação do acesso a pastas, sistemas e arquivos, conforme o perfil de cada Colaborador e sua respectiva área.

Os arquivos digitais da Instituição são restritos a cada área através de permissões por usuário, de forma que quando um colaborador é admitido ou transferido para uma área

na qual não possui acesso aos arquivos, o gestor responsável pela área e o responsável de *Compliance* precisam validar a liberação para o colaborador.

Todos os arquivos digitais que possuem algum tipo de cunho confidencial possuem acesso restrito, de forma que o colaborador permitido ao acesso precisa de uma senha para visualizar o arquivo. Além disso, os arquivos físicos das áreas ficam em locais distintos uns dos outros.

→Política de Confidencialidade e Segurança da Informação

Em complemento à segregação de atividades, nos termos da Resolução CVM nº 21, de 25 de fevereiro de 2021, especialmente o Artigo 27, III e Artigo 28, II, a Gestora adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Gestora é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

Para garantir a segurança da informação confidencial a Gestora mantém um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, diretórios de rede, planos de continuidade entre outros. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Em caso de determinado Colaborador passar a exercer atividade ligada a outra área da Gestora, tal Colaborador terá acesso apenas às informações relativas a esta área, das quais necessite para o exercício da nova atividade, deixando de ter permissão de acesso aos dados, arquivos, documentos e demais informações restritas à atividade exercida anteriormente. Em caso de desligamento da Gestora, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna da Gestora.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e Clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de *Compliance*.

Todos os Colaboradores, assim como todos os terceiros contratados pela Gestora, deverão assinar documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

Todos os computadores da Sociedade possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores utilizados pela Sociedade permitem a identificação do seu remetente/receptor.

As senhas são de caráter sigiloso, pessoal e intransferível e serão fornecidas aos Colaboradores da Sociedade. Em nenhuma hipótese as senhas deverão ser transmitidas a terceiros.

Os usuários e senhas são cadastrados e gerenciados de modo a controlar o acesso a pastas e arquivos da Sociedade. Quando o Colaborador da Sociedade é desligado, imediatamente através de comunicação do RH, é bloqueado o seu acesso a todos os sistemas da Sociedade (sistema aplicativo, e-mail, Intranet, pastas e arquivos da rede, etc.).

O acesso a todos os sistemas, incluindo os que controlam informações confidenciais, é liberado com base no princípio da necessidade da informação para a execução da função. O controle é feito por meio dos perfis de acesso, segregação da estrutura de arquivos que agrupam as funções. Cada colaborador possui um conjunto de perfis relacionados às suas atividades.

A equipe de TI promove testes periódicos para assegurar que os recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação e ao nível de confidencialidade e dos acessos às informações.

O plano de testes assegura a segregação lógica dos dados digitais, e que recursos computacionais de controle de acesso físico e lógico estejam protegidos. Assegura também, a manutenção de registros que permita auditorias e inspeções.

Em periodicidade mínima mensal serão validados arquivos e backups para assegurar o restore dos memos. O Diretor de Compliance e Risco receberá mensalmente reporte com lista de acessos de cada Colaborador para adoção de medidas cabíveis se detectadas quaisquer inconsistências.

No caso de vazamento de informações, serão analisados os logs de acessos e identificado o usuário que acessou a informação e realizou a ação, para que sejam adotadas as ações

necessárias.

A troca de informações entre os Colaboradores da Sociedade deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida, solicitar esclarecimento por e-mail ao gestor imediato, antes da revelação.

O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros em ambiente restrito aos Colaboradores que nela atuam, sendo o acesso de terceiros autorizado desde que acompanhados por responsável interno.

É recomendável nunca deixar documentos expostos nas mesas. Sempre que o usuário sair do seu posto de trabalho deve levar consigo ou guardar/ arquivar os documentos que eventualmente estejam nas mesas para que outros não tenham acesso às informações confidenciais.

→Treinamento

A Instituição realiza treinamentos periódicos com seus colaboradores no intuito de enfatizar e atualizar os princípios éticos e de conduta organizacional, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento.

O Diretor de *Compliance* deverá conduzir sessões de treinamento aos Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste manual, e deve estar frequentemente disponível para responder questões que possam surgir em relação aos termos deste Manual de *Compliance* e quaisquer regras relacionadas a *compliance*.

O treinamento também consiste na atualização do conhecimento dos Colaboradores sobre matéria relacionada ao mercado de capitais e legislação vigente, em treinamento sobre regras de controle de arquivos e acessos, sobre políticas de confidencialidade, segurança da informação, segregação de atividade e investimento pessoal.

Além disso, todo colaborador da Gestora, ao ser admitido, recebe orientações da área de *compliance* sobre os principais temas abordados nos manuais e políticas da Instituição.

O Colaborador deverá atestar por escrito aos Diretores ter lido e compreendido todos os seus termos e condições, obrigando-se a cumprir e respeitar o referido Código.