PARTE DO MANUAL DE COMPLIANCE E GESTÃO DE RISCOS

CONFIDENCIALIDADE E SEGURANÇA DE INFORMAÇÕES

A. Aspectos gerais

Confidencialidade é um princípio fundamental. Aplica-se a quaisquer informações não-públicas referentes aos negócios da Gestora, como também as informações recebidas de seus clientes, contrapartes ou fornecedores da Gestora, durante o processo natural de condução dos negócios. Os Colaboradores não devem transmitir nenhuma informação não-pública a terceiros.

Os Colaboradores da Gestora deverão guardar sigilo sobre qualquer informação relevante a qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Os Colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

O disposto no presente capítulo deve ser observado durante a vigência do relacionamento profissional do Colaborador com a Gestora e também após seu término, em linha com o disposto na Lei Geral de Proteção de Dados.

B. Políticas gerais

O acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Gestora.

Para acessar informações nos sistemas da Gestora, deverão ser utilizadas somente ferramentas e tecnologias homologadas pela empresa, de forma a permitir a identificação e rastreamento de quais usuários tiveram acesso a determinadas informações (os logs de acesso ficam armazenados nos sistemas).

Senhas são pessoais e intransferíveis e não devem, em hipótese alguma, ser disponibilizadas a terceiros ou compartilhadas com outros Colaboradores.

A Gestora conta com *firewall* de segurança para acesso a seus dados, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus será atualizado diariamente. O *backup* de arquivos será realizado, diariamente, na nuvem.

A Investcoop Asset dispõe, ainda, de sistema de gravação, o qual registra integralmente todas as ligações por um ou mais ramais. O acesso a essas gravações é restrito, sendo que as solicitações de acesso para escuta de tais

registros devem passar por aprovação do diretor da sua respectiva área com o registro de solicitação através do sistema de *workflow* da companhia (*jocker*).

Adicionalmente, informamos que a rede da gestora é composta por diretórios de dois níveis:

(i) diretórios de informações públicas, aos quais todos os sócios, Colaboradores e funcionários da Gestora têm acesso, contendo tão somente informações de natureza administrativa; e
(ii) diretórios de acesso restrito, cujo acesso é somente pré-autorizado pelo Diretor de *Compliance*, aos membros de alguns departamentos específicos, em todos os casos sendo necessário o *log-in* e senha de cada integrante.

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade da Gestora, pelo qual se obrigam, entre outras coisas, a protegerem a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando na Gestora e mesmo após terem deixado a empresa, por prazo indeterminado.

É importante ressaltar que os acessos acima referidos são imediatamente cancelados em caso de desligamento do Colaborador da Gestora.

C. Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora ("Informações" ou "Informação"), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de *Compliance* deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de *Compliance*, primeiramente, identificará se a Informação vazada refere-se ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de *Compliance* procederá da seguinte forma:

1. No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

2. No caso de vazamento de Informações relativas aos cotistas:

Neste caso, ao Diretor de *Compliance* procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de *Compliance* ficará à inteira disposição para auxiliar na solução da questão.

D. Testes Periódicos

Periodicamente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

- Verificação do Login dos Colaboradores;
- A cada 90 (noventa) dias, altera-se a senha de acesso dos Colaboradores;
- Testes no *firewall*;
- Testes nas restrições impostas aos diretórios;
- Manutenção trimestral de todo o *hardware*, por empresa especializada em consultoria de tecnologia de informação;
- Testes no meio físico (*on-premises*) de armazenamento dos dados, realizados diariamente.

SEGREGAÇÃO DE OPERAÇÕES

A Gestora manterá a devida segregação entre as suas diversas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

A. Segregação de atividades e funções

O primeiro nível de segregação refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de Gestor, Analistas, *Compliance*, Risco e Administrativo. Perfis de acesso físico e eletrônico e o controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas, quando necessário, nos comitês da Gestora, sendo que os participantes se responsabilizam pelo sigilo das informações.

B. Segregação física

A área destinada às atividades de administração de recursos será fisicamente segregada das demais áreas comuns da sociedade, como por exemplo, as áreas administrativas, salas de reunião, copa e banheiros, acessadas apenas pelos Colaboradores diretamente envolvidos com a atividade de administração de carteiras.

O acesso de pessoas que não fazem parte do quadro de Colaboradores será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio

conhecimento e autorização da administração e desde que acompanhadas de Colaboradores. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências da Gestora. O atendimento a clientes nas dependências da Gestora deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

C. Segregação eletrônica

Todos os Diretores da Gestora têm acesso à rede e aos sistemas corporativos, mas há restrição de acesso aos computadores pessoais, e-mails pessoais e áreas na rede dedicadas a arquivos pessoais.

RISCO CIBERNÉTICO

Em conformidade com a evolução tecnológica, a Gestora possui procedimentos visando a proteção e segurança da informação contra os Riscos Cibernéticos.

A gestora conta com controle de seus ativos de hardware e software, por meio de aplicações que identificam os riscos internos e externos. Posssui também sistema de avaliação contínua da efetividade do ambiente de controle para identificar riscos potenciais e determinar ações corretivas.

A identificação de ameaças e possíveis impactos nas operações é feita através de processo de prevenção e proteção que conta com equipes dedicadas ao monitoramento dessas ameaças em seu parque tecnológico.

Normas e políticas de segurança visam impedir a presença de usuários, componentes ou dispositivos não autorizados dentro do ambiente corporativo. Periodicamente são realizados testes de vulnerabilidades no ambiente interno e externo, com o objetivo de identificar possíveis ataques de intrusão.

A Gestora conta também com uma área dedicada à gestão de incidentes críticos e monitoração, com o objetivo de restabelecer os serviços impactados em menor tempo possível e garantir os melhores níveis de qualidade e disponibilidade de serviços, assegurando que os usuários tenham a disponibilidade de serviços de TI, necessários para suportar o negócio.

Por fim, são realizados anualmente treinamentos, com todos os nossos colaboradores, a fim de conscientiza-los sobre as possíveis ameaças internas e externas. Esses treinamentos ocorrem de forma presencial e por meio eletrônico, sendo parte desses treinamentos, mandatórios, inclusive o de segurança da informação.