

## PARTE C – CÓDIGO DE ÉTICA E CONDUTA

### I. CONSIDERAÇÕES GERAIS

O Código de Ética e Conduta da Gestora reflete a visão, a missão e os valores que estão presentes no dia a dia da Gestora. Visa a integrar os Colaboradores à filosofia da empresa, criando uma cultura corporativa onde todos vejam a expansão dos negócios e o exercício da ética como complementares e inter-relacionados. Deste modo, a Gestora pode proteger sua reputação e seu patrimônio intangível, construindo e consolidando-se como empresa íntegra, diligente e sólida.

A Gestora defende o desempenho de suas atividades com o fim principal de proteger e rentabilizar o patrimônio dos seus clientes, utilizando sempre das melhores práticas do mercado e selecionando os ativos/gestores comprometidos com os mais altos valores éticos.

A Gestora não admite qualquer forma de discriminação (“Discriminação”), assédio moral ou sexual (“Assédio”), praticado por ou contra qualquer Colaborador ou terceiro. A discriminação no ambiente de trabalho não favorece a diversidade onde as diferenças entre os Colaboradores devem ser valorizadas e respeitadas, seja com base em raça, cor, religião, idade, estado civil, deficiência e orientação sexual. O Assédio se caracteriza pelo abuso de poder, humilhando, desqualificando, menosprezando o outro.

Tanto a Discriminação como o Assédio são considerados infrações graves que não serão tolerados no ambiente de trabalho da Gestora.

### II. REPRESENTAÇÃO DA GESTORA

#### A. *Comunicação com a Imprensa*

Visando a resguardar os interesses da Gestora em função das informações de seus clientes, da confidencialidade dos negócios, e da alta sensibilidade das informações relacionadas ao mercado financeiro e de capitais, somente o diretor responsável pela área de gestão de recursos de terceiros da Lifetime Asset (“Diretor de Gestão”) ou o Diretor de Compliance podem manter qualquer tipo de comunicação com jornalistas, repórteres, entrevistadores ou agentes da imprensa falada ou escrita (a “Imprensa”).

Com prévia autorização do Diretor de Gestão ou do Diretor de Compliance, eventualmente um Colaborador poderá participar de entrevistas e assembléias. Neste caso, deverá restringir-se a fazer comentários estritamente técnicos, evitando-se o uso de juízos de valor desnecessários. É esperado do Colaborador que participar de entrevistas o uso de bom senso e educação quando estiver representando Gestora.

## **B. Comunicação com clientes**

A comunicação com clientes deve ser pautada pela cordialidade, eficiência e precisão. É vedada qualquer representação que garanta ou insinue garantia de performance. O Colaborador deverá claramente separar opinião e fatos. Toda e qualquer informação não-pública obtida a partir de diálogo com clientes é considerada confidencial e, portanto, regida por este Manual.

## **C. Comunicação com terceiros**

A comunicação e relacionamento com terceiros – fornecedores, concorrentes, outras entidades de mercado -, deve ser pautada pela ética, profissionalismo, cortesia e discrição. É vedado aos Colaboradores assumir qualquer compromisso em nome da Gestora, formal ou informalmente, sem que detenha autonomia para tal ou consentimento de um sócio.

# **III. BENS E PROPRIEDADE DAS GESTORAS**

## **A. Propriedade da Gestora**

Os ativos e bens da Gestora devem ser utilizados de forma ética, parcimoniosa e visando tão-somente o interesse da Gestora. Bens e serviços contratados como e-mail, internet, telefones, entre outros são considerados ferramentas de trabalho, que não devem ser utilizados de forma particular. É terminantemente proibida a recepção ou envio de imagens ou vídeos de conteúdo pornográfico, racista, ou que remeta a qualquer forma de preconceito.

O Diretor de Compliance se reserva o direito de monitorar o uso dos ativos e bens da Gestora sem o prévio consentimento do Colaborador e relatar ao Comitê de Compliance quaisquer incidências de uso indevido.

## **B. Propriedade intelectual**

A lei de propriedade intelectual dispõe claramente que toda invenção e modelo de utilidade pertencem exclusivamente ao empregador quando decorrerem de trabalho cuja execução se deu durante o período de vínculo do Colaborador.

Todo material e documentos que estão na sede da Gestora, na rede corporativa ou nos computadores pessoais usados para trabalho pelos seus Colaboradores são de propriedade da Lifetime Asset. O uso de qualquer informação que consta nesse material deve ser exclusivamente relacionado às atividades da Gestora, e a informação não pode de forma alguma ser disseminada ou retransmitida.

Nenhum Colaborador será remunerado além da remuneração previamente acordada, por qualquer trabalho que constitua invenção ou modelo de utilidade. No caso específico de estudos criados internamente, sejam eles relacionados ou não à estratégia de investimento da empresa, não permitido divulgar sem autorização quaisquer informações.

### **C. Alçada de despesas e reembolsos**

Os reembolsos são definidos nas alçadas superiores Gestor. Solicitações devem obedecer à regra do bom senso de cada integrante da Gestora.

A manipulação de reembolsos de despesas, tais como almoços, jantares, táxis, estacionamento, viagens, entre outros, é considerada falta grave e, se comprovada, resultará em penalidade a ser julgada pelo Diretor de Compliance ou Comitê de Compliance, conforme o caso. Qualquer reembolso acima da alçada permitida poderá ser solicitado sempre que o Colaborador tiver obtido aprovação prévia do Diretor de Compliance para tal despesa.

## **IV. CONFIDENCIALIDADE**

A confidencialidade é um princípio fundamental para a Gestora e aplica-se a quaisquer informações não públicas, referentes aos negócios da Gestora, assim como informações recebidas de seus clientes, contrapartes ou fornecedores, durante o processo natural de condução de negócios. Os Colaboradores não devem transmitir informação não pública alguma a terceiros.

Os Colaboradores da Gestora deverão guardar sigilo sobre qualquer informação relevante à 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. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Gestora, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

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.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Lifetime Asset, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Lifetime Asset. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito ao Diretor de Compliance da Lifetime Asset, para que sejam tomadas as medidas cabíveis.

Para fins de manutenção das informações confidenciais, a Lifetime Asset recomenda que seus Colaboradores (i) bloqueiem o computador quando o mesmo não estiver sendo utilizado ou estiverem ausentes da sua estação de trabalho; (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha pessoal de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

O disposto no presente capítulo deve ser observado durante a vigência do relacionamento profissional do Colaborador com a Gestora e após seu término.

Todo Colaborador, ao receber o presente Manual, assinará um Termo de Confidencialidade, que trata da obrigação de observância das políticas de confidencialidade e segurança da informação da Gestora, detalhada ao longo deste Manual. Por esse documento, cada Colaborador declara ciência da existência das referidas políticas e das regras e princípios ora expostos, seguidos pela Gestora.

#### **A. 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 neste Manual (“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.

## **V. SEGURANÇA DA INFORMAÇÃO**

No que diz respeito à infraestrutura tecnológica, destacamos que há um servidor trabalhando nas instalações da Gestora, o qual conta com sistema de rede com acesso por usuário limitado a arquivos que são armazenados somente nos servidores para evitar redundância de arquivos e informações. O *backup* é feito automaticamente duas vezes ao dia.

Ademais, a Lifetime Asset conta com um servidor de arquivos por políticas de acesso à arquivos por usuários. Este servidor conta com RAID1 (Espelhamento de disco), para evitar a interrupção da operação caso um dos discos apresente problemas. Além disso, o mesmo possui *backup* diário realizado em disco externo, além do armazenamento de histórico de versões de arquivos que é realizado 2 (duas) vezes ao dia.

Todo software disponibilizado aos Colaboradores deverá ser utilizado somente para os negócios da Lifetime Asset, em consonância com os acordos de licenciamento firmados.

O acesso aos sistemas de informação da Lifetime Asset é feito por meio de um par “usuário/senha”. 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. O controle desses dados é de domínio da Lifetime Asset, uma vez que o armazenamento dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

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

Adicionalmente, informamos que a rede da Lifetime Asset é segregada de acordo com as diferenças funcionais de atuação e autoridades definidas para as posições de gestor de recursos, *Compliance*, gestão de risco e administrativo. Perfis de acesso físico (leitura biométrica) e eletrônico (login e senha) e o respectivo controle de tais acessos são realizados com base nessas divisões. Dessa forma, cada Colaborador possui acesso à rede com senha, e o perfil de acesso é definido segundo sua área de atuação na Lifetime Asset. Assim, o acesso a diretórios é configurado por grupos de segurança, de forma a garantir o devido sigilo e confidencialidade das informações.

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

É terminantemente proibido que os Colaboradores copiem, imprimam e/ou compartilhem os arquivos utilizados, gerados ou disponíveis na rede da Gestora, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

Tal proibição não se aplica quando as cópias ou a impressão dos arquivos forem em prol e do desenvolvimento dos negócios e dos interesses da Gestora e de seus clientes. Nestes casos, o Colaborador que estiver com a cópia ou a impressão do arquivo que contenha informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Em nenhuma hipótese um Colaborador pode emitir opinião por e-mail em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos.

A Gestora se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador.

O Diretor de Compliance poderá monitorar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente.

#### **A. 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;
- Anualmente, 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; e
- Testes no *backup* (salvamento de informações) diário, realizado em um HD externo além do servidor.

## **VI. 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 entre empresas do grupo**

O primeiro nível de segregação é externo. Além da Gestora, o Grupo Lifetime (“Grupo”) é formado por empresas atuando no ramo educacional e exercendo atividades de agente autônomo. Por essa razão, o Grupo decidiu segregar as atividades das empresas. Implementou, assim, três níveis de separação de fluxos entre elas: (i) segregação física, em que os membros de uma empresa não terão acesso às dependências de outra, (ii) segregação de pessoal, em que as equipes das empresas são diferentes, e não há identidade entre os membros de uma empresa e de outra, com exceção dos sócios, no caso da empresa que atua no ramo educacional, sendo certo que nenhum membro que atua na Gestora atua na empresa de agente autônomo, e (iii) segregação eletrônica, em que os sistemas são segregados, e a infraestrutura tecnológica é independente e não poder ser compartilhada entre as empresas.

Além dos mecanismos ora descritos de mitigação de conflitos de interesses, a Gestora adota as medidas destacadas na seção “Conflitos de Interesse” deste Manual.

## **B. Segregação de atividades e funções**

O segundo nível de segregação é interno, e refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de gestor, compliance, gestão de risco e administrativo. Perfis de acesso físico e eletrônico, e o respectivo controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade (“*as-needed basis*”) nos comitês instituídos pela Gestora, sendo que os participantes se responsabilizam pelo sigilo das informações.

## **C. Segregação física**

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

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. O atendimento a clientes nas dependências da Gestora deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

## **D. Segregação eletrônica**

Cada Colaborador possui acesso à rede com senha, e o perfil de acesso é definido segundo sua área de atuação. Assim, o acesso a diretórios é configurado por grupos de segurança.