REDPOINT EVENTURES GESTÃO DE RECURSOS E CONSULTORIA LTDA.

Política de Gestão de Riscos

(Outubro de 2018)

I. Da Gestão de Riscos

1. A atuação da Redpoint Eventures Gestão de Recursos e Consultoria Ltda. ("**Redpoint**" ou "**Sociedade**") no mercado financeiro e de capitais, exercendo atividades como uma administradora de carteira de valores mobiliários, é sujeita a riscos, inevitáveis e inerentes à natureza do serviço prestado, em especial:

(i) *Risco de imagem* (*ou reputação*): tendo em vista que uma simples informação pode causar danos irreparáveis à reputação da Redpoint, é importante a consciência de todos sobre a necessidade de se prezar pela imagem da Sociedade. Assim, todos devem ter sempre em mente a importância de seguir as regras de *compliance* e de quaisquer políticas e diretrizes impostas pelo Departamento de Compliance e Gestão de Risco;

(ii) *Risco operacional* (*operational risk*): é o risco ligado aos controles administrativos e tecnológicos da Companhia, bem como erros humanos que possam, de alguma forma, atrasar ou impedir a condução de seus negócios (*e.g.*, decorrentes de atos ou omissões dolosos ou culposos), dentre os quais os principais são: (a) risco de obsolescência; (b) risco de equipamento; (c) risco de tecnologia; (d) risco nos mercados eletrônicos; (e) risco de erro não intencional; (f) risco de fraudes; (g) risco da qualificação de pessoal; (h) risco de lavagem de dinheiro; e (i) risco de acesso; e

(iii) *Risco legal* (*legal risk*): é o risco decorrente da inadequação da estrutura regulatória ou legal, manifestada ainda pela incerteza do cumprimento de tal estrutura; ou pelas falhas na formalização de negócios causadores de insegurança quanto ao seu cumprimento ou existência.

2. Em decorrência deste fato, os controles de mitigação de riscos da Redpoint são essenciais, de modo que o tipo e a sofisticação de tais controles devem ser consistentes com os padrões de tolerância estabelecidos pela Redpoint. A fim de evitar ou minimizar os riscos inerentes que permeiam a atividade da Sociedade, busca-se o aprimoramento de seus controles internos (*compliance*) e de treinamento de pessoal.

3. O planejamento estratégico da Redpoint é um de seus principais recursos de

controle de riscos, ou seja, aquele ligado aos controles administrativos e tecnológicos da Companhia, bem como erros humanos que possam, de alguma forma, atrasar ou impedir a condução de seus negócios (*e.g.*, decorrentes de atos ou omissões dolosos ou culposos). A fim de evitar ou minimizar estes riscos, a Sociedade busca aprimorar seus controles internos (*compliance*) e treinamento de pessoal. De tal forma, a Redpoint implementa uma gestão integrada de riscos, que são avaliados em todas as etapas do processo de investimento da Sociedade.

4. Quaisquer dúvidas, esclarecimentos ou aconselhamento sobre que ações ou investimentos possam gerar riscos para a Companhia devem ser, imediatamente, direcionados ao responsável designado, responsáveis pelo follow-up destes riscos através do monitoramento das atividades, com geração de reportes diários, bem como de planos de contingência e continuidade específicos para tecnologia.

5. O responsável pelo compliance e pelo monitoramento de riscos é o Sr. Fábio Schenberg Frascino, além dos demais membros que compõem e que venham a compor o Departamento de Compliance e Gestão de Risco.

II. Ocorrência de Fraudes Internas ou Externas

6. Além do acompanhamento pessoal e diário pelo responsável designado e por todo o Departamento de Compliance e Gestão de Risco, a Sociedade irá manter relatórios do cumprimento de suas políticas. Além disso, as políticas da Redpoint, em especial a Política de Segurança, a Política de Confidencialidade e a Política de Negociação, expostas no Manual de Compliance, auxiliarão no tratamento do risco de fraude.

7. Dentre estes mecanismos, cabe ressaltar que a Sociedade obterá mandatos de seus clientes com poderes específicos de movimentação de recursos, ou seja, a movimentação apenas poderá ser feita entre contas previamente autorizadas e reconhecidas pelos clientes, evitando assim um possível desvio de recursos.

8. A Sociedade fornecerá ainda a seus clientes relatórios mensais com uma prestação de contas de todas as negociações efetuadas em seu nome. Por fim, todos os profissionais contratados pela Redpoint passam por um processo de avaliação que inclui entrevistas pessoais, análise de currículo e referências de empregadores anteriores.

III. Segurança do Local de Trabalho

9. A sede da Redpoint está localizada em um prédio comercial em área nobre da cidade de São Paulo, com controle de acesso tanto na recepção do edifício como na entrada da Sociedade, por meio de registro eletrônico de presença e segurança particular. Sob o ponto de vista de segurança virtual, a Redpoint possuirá sistemas de antivírus constantemente atualizados e *firewall*, de modo a garantir a integridade das informações armazenadas nos computadores da Sociedade.

IV. Práticas Inadequadas Relativas a Clientes, Produtos e Serviços

10. Além do acompanhamento pessoal e diário pelo responsável designado, a Redpoint irá manter relatórios do cumprimento de suas políticas. Além disso, nos termos da Política de Treinamento, todos os profissionais da Sociedade receberão treinamento adequado no momento da admissão, e posteriormente sempre que necessário. Salvo exceções, o responsável designado estará sempre diretamente envolvido na comunicação com os clientes da Sociedade. Com relação aos produtos e serviços oferecidos (que estão relacionados diretamente à atividade da Companhia de gestão de investimentos), a Companhia promoverá o acompanhamento e análise dos riscos inerentes aos ativos que comporão as carteiras dos fundos de investimento de forma ativa.

V. Conformidade das Operações e Produtos e Exposição a Riscos

11. O monitoramento contínuo das posições assumidas pela Redpoint visa verificar se as respectivas carteiras estão ajustadas, em adequação, e em cumprimento com a política de investimento do produto específico e com as leis aplicáveis. A Sociedade buscará avaliar e mitigar os seguintes riscos inerentes à suas operações e produtos: riscos de mercado, riscos de crédito, riscos de liquidez, risco de concentração de carteiras e risco de desenquadramento das carteiras de valores mobiliários.

12. A Redpoint realizará supervisões pré- e/ou pós-liquidação diárias para verificar irregularidades ativas ou passivas nas carteiras de valores mobiliários. Se a supervisão pré-liquidação diária detectar a possibilidade de ocorrência de uma irregularidade ativa em decorrência de uma operação selecionada pela Sociedade, o profissional designado deverá ser imediatamente notificado, através de uma ligação telefônica ou por um e-mail, bem como a Redpoint tomará todas as medidas efetivas para o cancelamento imediato ou no máximo até o próximo dia útil ao de tal operação irregular e/ou impedirá a liquidação da referida operação irregular diretamente ou, se aplicável, por meio dos terceiros prestadores serviços autorizados.

13. Se a supervisão pós-liquidação pela Redpoint detectar uma irregularidade passiva nas carteiras de valores mobiliários, a Sociedade deverá imediatamente adotar a melhor alternativa para a eliminação da irregularidade em questão, observando os procedimentos e os termos previstos na lei aplicável. A Redpoint deverá semanalmente gerar relatórios sobre qualquer irregularidade ativa ou passiva, se aplicável.

14. Ainda, a Sociedade deverá realizar testes frequentes de modelos de risco, visando o controle de exposições máximas de risco e os limites de risco de cada um de seus produtos. A Redpoint irá realizar estes testes para monitorar o nível de exposição aos riscos nas carteiras de valores mobiliários quanto aos seus limites específicos de riscos de cada produto. Tais testes deverão também gerar relatórios semanais.

15. Para fins de cálculo de cada um dos riscos, a Sociedade deverá considerar, nos modelos de riscos, as metodologias usualmente utilizadas nas práticas locais e internacionais, estritamente confidenciais, destinadas a criar modelos matemáticos e estatísticos que utilizam dados históricos e premissas em um esforço para prever o futuro comportamento econômico.

VI. Limites de Concentração

16. As atividades da Redpoint atualmente tem como foco a gestão de fundos de investimento com políticas de investimento que podem expor os fundos a uma concentração significativa em ativos financeiros de poucos emissores com os riscos daí decorrente. Tais investimentos também poderão ser alocados em ativos offshore.

VII. Risco de Liquidez

17. Nas operações no mercado de valores mobiliários, a Redpoint trata com muito cuidado o risco de liquidez. O risco de liquidez é o risco de perdas incorridas em operações que, se executadas no horizonte de tempo planejado, devido à liquidez insuficiente, só possam acontecer a um preço desfavorável.

18. Para as carteiras compostas por ativos líquidos e listados, o risco de liquidez é disponibilizado às áreas envolvidas com base diária através do sistema de risco e monitorado diariamente de diferentes formas:

(i) Risco de liquidez das posições do fundo: monitorado com base na comparação entre a estimativa de dias necessários para liquidar os ativos sem incorrer em

impacto negativo nos preços. Essa estimativa é um percentual da média do volume de negociação diário dos últimos dias. O limite indicativo para avaliação da liquidez de um ativo que compõe a carteira de um fundo é o prazo de resgate estabelecido pelo regulamento de cada fundo.

(ii) Concentrações de contas: monitorado o grau de dispersão de propriedade das cotas computando os percentuais detidos pelos grupos de investidores de acordo com a sua representatividade no patrimônio do fundo (curva ABC).

VIII. Risco de Contraparte

19. Procuramos gerenciar e minimizar esses riscos atuando somente com grandes players do mercado e que apresentem sólida situação financeira. A Redpoint adota ainda rigorosa prática de seleção de contrapartes que exigem a avaliação da qualidade na prestação do serviço e preço.

IX. Falhas de Sistemas

20. A Redpoint utiliza em suas atividades softwares de empresas reconhecidas, que passam por testes rigorosos de implementação e são objeto de manutenção regular. A Sociedade adota ainda sistemas de backup de informações que armazenam todas as informações necessárias, por meio de software que promove a identificação de toda documentação contida no sistema. Além disso, a Redpoint mantém também sistemas de antivírus e *firewall*, a fim de evitar invasões que possam comprometer a integridade dos sistemas e das informações armazenadas pela Sociedade. A Política de Segurança descreve práticas adicionais de controle dos sistemas da Redpoint.

X. Verificação de Cumprimento dos Deveres Legais

21. De modo a mitigar o risco legal, a Sociedade conta com assessoria jurídica de escritório de advocacia de renome, o qual mantém a Redpoint devidamente informada sobre novidades relacionadas às regras de *compliance* e cumprimento de obrigações legais, e que envia publicações regulares, que visam atualizar a Sociedade ante as contínuas mudanças na legislação, normas e regulamentos brasileiros, com especial foco nos setores do mercado de capitais ligados às atividades exercidas pela Sociedade.

XI. Plano de Continuidade dos Negócios da Companhia

22. Pela natureza do negócio, os riscos de interrupção estarão relacionados

principalmente a (i) falta de pessoal; e (ii) falhas de sistema. Este plano tem, como principal objetivo, prever algumas situações de emergência que possam vir a interromper os negócios da Companhia, bem como traçar as estratégias e planejamento para retomada das atividades em um curto espaço de tempo, minimizando assim, o impacto negativo de um possível desastre ou situação de contingência para a Companhia e seus clientes.

23. A análise de impacto nos negócios é elaborada através de um questionário anual elaborada pelo responsável designado, que tem como principal objetivo o de mensurar os efeitos sobre a Companhia no caso de ocorrência de algum desastre ou interrupção dos negócios. Tal formulário servirá como base para relacionar o funcionamento das equipes (recursos humanos) antes, durante e depois da ocorrência do evento. Através desta análise são definidas as ações e responsabilidades no período de retorno a normalidade.

24. Com relação ao primeiro item, a Companhia possuirá arquivos físicos, com *backup* eletrônicos, divididos por cliente e trabalhos relevantes que estiverem em desenvolvimento. Cada profissional terá o dever de manter tais arquivos organizados e atualizados a todo momento para que, caso um determinado profissional fique impossibilitado de finalizar determinado trabalho por qualquer motivo, outro profissional poderá facilmente retomar o trabalho com base nos arquivos da Companhia.

25. Os processos de arquivamento e organização de informações fazem parte da Política de Treinamento da Companhia, e também são mencionados nas Políticas de Segurança e Política de Confidencialidade. Além disso, o responsável designado será responsável por organizar e dividir os trabalhos dos profissionais da Companhia, e estará em contato constante com os seus profissionais.

XII. Revisão da Política

26. A Política de Gestão de Riscos deve ser revisto, pelo menos, anualmente.