REDPOINT EVENTURES GESTÃO DE RECURSOS LTDA.

Política de Gestão de Riscos
(Maio de 2019)

I. Da Gestão de Riscos

1. A atuação da Redpoint Eventures Gestão de Recursos Ltda. ("**Redpoint eventures**" 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 eventures, 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 Sociedade, 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 eventures são essenciais, de modo que o tipo e a sofisticação de tais controles devem ser consistentes com os padrões de tolerância estabelecidos pela Redpoint eventures. 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 eventures é um de seus principais

recursos de controle de riscos, ou seja, aquele ligado aos controles administrativos e tecnológicos da Sociedade, 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 eventures 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 Sociedade 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 a Sra. Paula Dainese, além dos demais membros que compõem e que venham a compor o Departamento de Compliance e Gestão de Risco, cujas funções são exercidas de forma independentemente em relação às demais áreas e departamentos da Sociedade, não havendo subordinação do Departamento de Compliance e Gestão de Risco da Redpoint eventures a nenhum outro profissional além da Sra. Paula Dainese. A Sra. Paula, ainda, tem independência para apontar aos administradores da Redpoint eventures quaisquer questões que lhe pareçam em desacordo com normas, leis e regulamentos internos.

6. Sem prejuízo das demais funções descritas nas políticas da Sociedade, as principais atividades realizadas pelo Departamento de Compliance e Gestão de Risco da Redpoint eventures consistem: (i) no cadastramento de clientes (que engloba também os procedimentos de *Know Your Client – KYC)*, (ii) na realização de procedimentos de Prevenção e Combate à Lavagem de Dinheiro (PLD), conforme descrito na política aplicável; (iii) na verificação do enquadramento dos fundos; (iv) na verificação do mandato dos fundos; (v) no monitoramentos dos riscos dos fundos; (vi) na implementação do Programa de Treinamento, conforme descrito no Manual de Compliance; e (vii) na revisão, em conjunto com assessoria jurídica externa, das políticas aplicáveis à Redpoint eventures.

II. Ocorrência de Fraudes Internas ou Externas

7. 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

eventures, 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.

8. 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.

9. 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 eventures passam por um processo de avaliação que inclui entrevistas pessoais, análise de currículo e referências de empregadores anteriores.

III. Segurança do Local de Trabalho

10. A sede da Redpoint eventures 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. Além disso, os centros de processamento de dados (*data centers*) da Sociedade também contarão com mecanismos de controle de acesso, a fim de mitigar o acesso digital aos sistemas relacionados por pessoas não autorizadas. Sob o ponto de vista de segurança virtual, a Redpoint eventures possuirá sistemas de antivírus constantemente atualizados e *firewall*, de modo a garantir a integridade das informações armazenadas nos computadores da Sociedade, além do controle lógico que ocorrerá por meio da existência de senhas de acesso a todos os computadores.

IV. Práticas Inadequadas Relativas a Clientes, Produtos e Serviços

11. Além do acompanhamento pessoal e diário pelo responsável designado, a Redpoint eventures 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 Sociedade de gestão de investimentos), a Sociedade 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

12. O monitoramento contínuo das posições assumidas pela Redpoint eventures 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. Os resultados das avaliações realizadas pelo Departamento de Compliance e Gestão de Riscos mencionadas acima são diariamente reportadas ao responsável pela gestão.

13. A Redpoint eventures realizará supervisões pré e/ou pós-liquidação para verificar irregularidades ativas ou passivas nas carteiras de valores mobiliários sempre que houver alteração na carteira. Se a supervisão pré-liquidação detectar a possibilidade de ocorrência de uma irregularidade ativa em decorrência de uma operação selecionada pela Sociedade, o responsável pela gestão deverá ser imediatamente notificado, por meio de uma ligação telefônica ou por um e-mail, de modo que a Redpoint eventures tomará todas as medidas efetivas para o cancelamento, no máximo até o próximo mês, e/ou impedirá a liquidação da referida operação irregular diretamente ou, se aplicável, por meio dos terceiros prestadores serviços autorizados. Se a supervisão pós-liquidação pela Redpoint eventures 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.

14. Conforme descrito acima, caso sejam identificadas eventuais irregularidades, estas serão imediatamente informadas ao responsável pela gestão, e este, por sua vez, informará a todo o Departamento Técnico e à administração da Redpoint eventures nas reuniões semanais. Tais irregularidades, acompanhadas dos demais riscos identificados pelo Departamento de Compliance e Gestão de Riscos, serão incluídos no relatório mensal de exposição de risco a ser enviado para a administração e Departamento Técnico.

VI. Limites de Concentração

15. As atividades da Redpoint eventures 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

16. Por se tratarem de investimentos em venture capital de estágio inicial com horizonte de desinvestimento podendo ser superior a 10 anos e sem liquidez no mercado secundário, os ativos que compõem as carteiras da Redpoint eventures são de baixíssima liquidez, de forma que não se torna necessário nem relevante um controle periódico de liquidez da carteira.

VIII. Risco de Contraparte

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

IX. Falhas de Sistemas

18. A Redpoint eventures 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 eventures 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 eventures.

X. Verificação de Cumprimento dos Deveres Legais

19. De modo a mitigar o risco legal, a Sociedade conta com assessoria jurídica de escritório de advocacia de renome, o qual mantém a Redpoint eventures 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 Sociedade

20. Pela natureza do negócio, além dos riscos operacionais elencados acima, quais sejam: (i) limites de concentração, (ii) liquidez, (iii) contraparte, e (iv) falhas de sistema, a Redpoint eventures também está sujeita a riscos de interrupção e de necessidade de contingencimento, os quais estarão relacionados principalmente a (i) falta de pessoal; e (ii) falhas de sistema, que podem ocasionar ataques cibernéticos e vazamentos de informações confidenciais. Este plano tem, como principal objetivo, prever algumas situações de emergência que possam vir a interromper ou prejudicar os negócios da Sociedade, 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 Sociedade e seus clientes.

21. 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 Sociedade 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 à normalidade.

22. Com relação ao primeiro item, a Sociedade possuirá arquivos físicos, com *backup* eletrônicos, divididos por cliente e trabalhos relevantes que estiverem em desenvolvimento, os quais serão atualizados mensalmente e armazenados no sitema Google Drive, com segregação de controle de acesso por departamento e responsável, criptografia e 2Fa, conforme detalhado na Política de Segurança da Informação. 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

Sociedade.

23. Os processos de arquivamento e organização de informações fazem parte da Política de Treinamento da Sociedade, 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 Sociedade, e estará em contato constante com os seus profissionais.

24. Com relação às estratégias de recuperação das atividades, a Redpoint eventures adota, no prazo máximo de 24 horas, as seguintes medidas para implementar o plano e retornar às atividades após alguma interrupção: (i) recuperação do local de trabalho, contando com instalações alternativas e temporárias capazes de acomodar os Membros e as instalações da Sociedade capazes de dar andamento às atividades; (ii) utilização de acesso remoto (*home office*), haja vista que os Membros possuem autonomia suficiente para, dentro dos limites de segurança, desempenharem suas atividades por meio do sistema de acesso remoto da Sociedade; e (iii) utilização de centro de dados compartilhados, de forma que a Redpoint eventures manterá tal centro de dados completo, contendo as informações detidas por cada um dos Membros, que sejam necessárias ao pleno funcionamento da Sociedade, respeitados os limites de segurança das informações confidenciais. O procedimento acima viabiliza o acesso a tais informações e possibilita e retomada imediata das atividades da Redpoint eventures após algum incidente.

25. Para garantir a eficácia das medidas indicadas acima, a Sociedade conduzirá testes, ao menos anualmente. Tais testes avaliarão a velocidade de resposta dos Membros frente às adversidades, bem como a solidez das respostas apresentadas. Dentre outros pontos, os testes avaliarão a capacidade de operacionalização do trabalho em outros locais, a conectividade do sistema de acesso remoto e consistência do centro de dados compartilhados.

26. O acionamento do Plano de Continuidade dos Negócios da Sociedade ocorrerá mediante a ciência do Departamento de Compliance e Gestão de Risco acerca de quaisquer incidentes, ou por meio da comunicação de qualquer Membro a este departamento.

XII. Revisão da Política

27. A Política de Gestão de Riscos deve ser revista, pelo menos, anualmente.