PLANO DE CONTINUIDADE DE NEGÓCIOS
MATA INVESTIMENTOS LTDA.

("Sociedade")

CAPÍTULO I
OBJETIVO

1.1 O Plano de Continuidade de Negócios da Sociedade tem como objetivo assegurar a continuidade das operações na eventualidade de uma indisponibilidade prolongada dos recursos essenciais (pessoas, dados, sistemas de informação, equipamentos e instalações).

1.2. Este Plano é aplicável a todos os colaboradores que deverão conhecer os procedimentos descritos abaixo, sendo que sua implementação será coordenada pela Área de Compliance, a qual contará com o auxílio do TI.

CAPÍTULO II
ESTRUTURA ADMINISTRATIVA, OPERACIONAL E ESTRATÉGICA

2.1. Para assegurar a manutenção da continuidade dos negócios, a Sociedade mantém de forma atualizada uma estrutura de tecnologia da informação e cibernética compatível com o volume e complexidade de suas operações, além de sistemas que assegurem a proteção integral contra adulterações e com redundância.

CAPÍTULO III
IDENTIFICAÇÃO E ANÁLISE DOS POTENCIAIS RISCOS

3.1. A Sociedade monitorará todos os potenciais riscos que sejam capazes de impactar a continuidade de seus negócios. Para fins deste Plano, a Sociedade considera como potenciais riscos e incidentes que podem resultar em descontinuidade operacional, tais como, mas não limitado, aos listados abaixo:

(i) Inacessibilidade temporária e/ou permanente às dependências do escritório decorrentes de catástrofes naturais como incêndios e enchentes, quedas de energia, além de questões relacionadas à saúde pública;

(ii) Acidentes ou eventos como roubos, greves, interrupção dos transportes, guerras e acidentes relevantes que também acarretem em bloqueios ou impossibilidade de acesso ao edifício;

(iii) Ataques relacionados à segurança cibernética como invasão de *hackers*, vírus de computador; e

(iv) Falhas sistêmicas, incluindo a falta de energia, e técnicas oriundas de sabotagem e erros humanos, falha grave no link de internet e sua redundância, hardware ou software.

3.2. No caso de ocorrência de qualquer das situações descritas no item 3.1., a Sociedade executará o Plano de Continuidade Operacional, descrito abaixo, que conta com o processo de identificação, comunicação aos colaboradores e ativação do Plano visando a mitigação dos impactos causados.

CAPÍTULO IV
PLANO DE CONTINGÊNCIA OPERACIONAL

4.1. A O Plano de Contingência Operacional da Sociedade é composto pelas seguintes fases:

a) Identificação das atividades essenciais à consecução da atividade de gestão profissional de recursos de terceiros:

As atividades essenciais ao objeto social da Sociedade são todas aquelas que compõem o processo de seleção de ativos e tomada de decisão de investimentos e desinvestimentos.

b) Identificação da interrupção do funcionamento dos recursos:

Uma situação de emergência é configurada sempre que houver uma descontinuidade operacional, assim entendida como o impedimento à execução de qualquer atividade essencial da Sociedade, ou processo do qual dependa uma atividade essencial.

Uma vez identificada a interrupção de quaisquer dos recursos essenciais às atividades da Sociedade, a Diretora de Risco, Compliance e PLD deve ser imediatamente comunicada e ativará o Plano de Continuidade de Negócios, orientando os colaboradores sobre a postura e providências cabíveis, de acordo com a natureza e gravidade da contingência.

Todos os colaboradores devem possuir os contatos telefônicos e e-mail da responsável pelo Compliance, de modo a possibilitar a comunicação da contingência ocorrida.

Para que seja caracterizada uma situação de emergência, o impedimento à execução da atividade essencial deve ser por tempo prolongado ou indeterminado. Considera-se tempo prolongado sempre que o tempo transcorrido desde a interrupção da atividade alcance 48 (quarenta e oito) horas, a expectativa de tempo até a solução da interrupção for superior 48 (quarenta e oito), quando o tempo remanescente para a conclusão da atividade for insuficiente para sua execução no mesmo dia ou se a não execução imediata da atividade puder provocar prejuízo para as atividades sociais.

c) Comunicação aos colaboradores

O Compliance manterá atualizada uma lista contendo os telefones e e-mails de todos os colaboradores da Sociedade.

Compete à Diretora de Risco, Compliance e PLD, ou colaborador por ela designado, a comunicação da contingência aos demais colaboradores, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e gravidade da contingência, sendo

responsável pela implementação da ativação e operacionalização do Plano abaixo apresentado no prazo máximo de 48 (quarenta e oito) da identificação da interrupção do funcionamento normal dos recursos, conforme item acima.

d) Ativação do Plano e acesso às informações para continuidade das operações críticas:

A ativação do Plano de Continuidade consiste no acesso pelos colaboradores aos dados e informações necessárias ao desempenho das respectivas atividades através de local diverso da sede social, podendo tal acesso ser realizado remotamente pela internet.

Todos os sistemas e veículos de informação contratados para auxiliar no processo de análise e gestão das carteiras são passíveis de serem acessados de qualquer localidade, bastando apenas a conexão com a rede mundial de computadores. Estes sistemas possuem mecanismos próprios de redundância e segurança.

A continuidade das atividades essenciais é garantida mediante o arquivamento das informações relacionadas a estes processos em ambiente seguro, com acesso restrito aos integrantes da equipe da Sociedade, e objeto de backup na nuvem em tempo real, possibilitando o acesso às citadas informações de qualquer outro computador através da senha de acesso, bem como a redundância de armazenamento para salvaguarda em caso de eventual sinistro.

e) Testes Periódicos:

Anualmente, são realizados testes de ativação do referido Plano pela Diretora de Compliance, ou em prazo inferior se exigido pela regulação em vigor e/ou se identificada a necessidade pela Sociedade.

Os testes possuem como objetivo avaliar a eficácia do presente Plano, de modo a suportar de forma satisfatória os processos operacionais para a continuidade dos negócios da Sociedade. Portanto, serão realizados testes de acesso aos e-mails e sistemas de forma remota, de modo a verificar o acesso, segurança e integridade dos dados armazenados e funcionamento do backup das informações. Sem prejuízo, a Sociedade também realiza testes periódicos de segurança cibernética para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados nos termos definidos pela Política de Segurança da Informação, Segurança Cibernética e Proteção de Dados.

A efetividade dos testes é ainda consolidada no Relatório de Conformidade a ser desenvolvido anualmente pela Diretora de Risco, Compliance e PLD, para fins de atendimento da Resolução CVM nº 21.

CAPÍTULO V
PLANO DE RECUPERAÇÃO

5.1. Este Plano tem o propósito de definir um guia de recuperação e restauração das funcionalidades afetadas que suportam o processo de tomada de decisões de investimentos, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível.

5.2. Assim, cabe ao Compliance elaborar relatórios acerca dos danos ocorridos, percentual das atividades afetadas, potenciais impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tal relatório deverá ser submetido à Diretoria da Sociedade para que sejam promovidas as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

5.3. Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a Sociedade estudará procedimentos preventivos a serem implementados e incluídos neste Plano de Continuidade de Negócios.

CAPÍTULO VI
DISPOSIÇÕES GERAIS

6.1. O presente Plano prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da Sociedade aos seus termos e condições.

6.2. A título de *enforcement*, vale notar que a não observância dos dispositivos deste Plano resultará em advertência, suspensão, ou demissão/exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.

6.3. A presente Política será revisada a cada 2 (dois) anos, sendo mantido o controle das versões, e será protocolada no SSM ANBIMA após a sua aprovação pela Diretoria.