MACRO CAPITAL GESTÃO DE RECURSOS LTDA.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

MAIO/2022

SUMÁRIO

1. OBJETIVO

1.1. Este Plano de Contingência e Continuidade dos Negócios ("Plano de Contingência") tem como objetivo estabelecer os procedimentos e as medidas a serem adotadas para identificar e prevenir as possíveis contingências que poderão trazer um impacto negativo sobre a condução das atividades da **MACRO CAPITAL GESTÃO DE RECURSOS LTDA. ("GESTORA")**. Dentre estas contingências se incluem, por exemplo, crises econômicas, falhas operacionais e/ou desastres naturais.

1.2. O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da GESTORA dentro do contexto de seu negócio.

1.3. O Plano de Contingência identifica duas variáveis para o funcionamento adequado da empresa: Infraestrutura e Processos.

1.4. A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática e sistemas internos. Para cada um dos itens que compõem a infraestrutura existe uma ação a ser tomada.

1.5. Os Processos são as ações realizadas na operação do negócio e são diretamente dependentes do funcionamento adequado da infraestrutura.

2. ESTRUTURA OPERACIONAL

2.1. A **GESTORA** é uma gestora de recursos de terceiros, e conta com uma estrutura operacional desenvolvida e preparada para situações emergenciais. O suporte para essa estrutura é formado por um corpo funcional com a competência necessária para a sua adequada atuação e por uma empresa responsável pela tecnologia de informação ("**Empresa de TI**"), devidamente contratada pela **GESTORA**.

3. AVALIAÇÃO DE RISCOS

Foram identificadas as seguintes áreas/atividades que necessitam estar contempladas no Plano de Contingência de forma a garantir o funcionamento da empresa:

(i) Escritório: espaço físico onde são realizadas as operações da **GESTORA**. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades;

(ii) TI: fundamental para o funcionamento da **GESTORA**, no sentido de que todas as comunicações com corretoras, administradores de Fundos de Investimentos e etc., são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios).

Também é fundamental para a realização de registros de operações (compras e vendas de títulos, aplicações e resgates em Fundos de Investimentos, transferência de recursos e pagamento de despesas da **GESTORA**, dentro outros); e

(iii) Pessoal: pessoas responsáveis pela operação da **GESTORA**, incluindo a análise e decisão para realização ou não de investimentos, equipe responsável pelo compliance e pela gestão de risco das carteiras dos Fundos de Investimentos e etc.

Tendo identificado essas 3 (três) áreas principais do ponto de vista da estrutura da **GESTORA** e dos processos sob sua responsabilidade, os riscos internos e externos que podem ocasionar o acionamento do Plano de Contingência foram identificados da seguinte forma:

(i) Problemas de Infraestrutura: os problemas dessa ordem são, dentre outros, falta de energia elétrica, falha nos links de internet, falha nas linhas telefônicas e na conexão à internet, falhas nos sites das empresas que fornecem sistemas de uso da **GESTORA**, falta de água etc.; e

(ii) Problemas de Infraestrutura predial e/ou acesso ao local/recursos: os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso ao local onde se localiza o escritório. Essa impossibilidade pode ser causada por eventos como, exemplificativamente, catástrofes naturais que impeçam o acesso ao prédio, cenários de greves em geral, interdições pelas autoridades do prédio ou do entorno do escritório da **GESTORA**, pane nos sistemas e *softwares* utilizados pelos Colaboradores da **GESTORA** etc.

Ainda, no âmbito de suas atividades, a **GESTORA** identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as informações confidenciais, incluindo informações a respeito de investidores, clientes ou clientes em potencial, e da própria **GESTORA**, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas), quaisquer documentos, contratos, gráficos, desenhos, segredos comerciais, informações comerciais, planilhas, estratégias e outros dados;
- Sistemas: informações sobre os sistemas utilizados pela **GESTORA** e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e suas vulnerabilidades;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da **GESTORA**; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pela **GESTORA** quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

No que se refere especificamente à segurança cibernética, a **GESTORA** identificou as seguintes ameaças:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
- Engenharia social – métodos de manipulação psicológica para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing* e *Acesso Pessoal*);
- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando tornar indisponível o acesso aos serviços ou sistemas da instituição; Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no levantamento da estrutura da **GESTORA** e no mapeamento de riscos, a **GESTORA** tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações e tomar ações de emergência para restabelecer a situação de atividade normal, através de ações traçadas neste Plano.

4. POLÍTICA E PROCEDIMENTOS PARA BACK-UP

4.1. A Empresa de TI disponibilizará aos servidores da **GESTORA** o serviço de *backup* e *restore* de arquivos, com o objetivo de garantir a segurança das informações, a recuperação das mesmas em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

4.2. Diariamente, às 23:00 horas, os arquivos armazenados em um servidor seguro, localizado na sede da **GESTORA**, são criptografados e copiados de maneira automática por meio de ferramenta de backup do Windows 2018 Server e Cloud, sendo salvos em disco externo e cloud.

4.2.1. O processo de back-up será conduzido, sistematicamente, da seguinte forma:

(i) os arquivos relativos à operação são armazenados no servidor da rede.

(ii) o *back-up* de dados armazenados nos servidores da rede corporativa é realizado de forma automatizada 1 vez por dia às 23:00 horas, de acordo com os procedimentos de *back-up* e *restore* definidos pela Empresa de TI; e

(iii) o *restore* de dados deve ser solicitado à Empresa de TI, sendo realizado de acordo com os procedimentos específicos.

4.3. Verificação e teste de restauração: mensalmente o *software* será configurado para verificar automaticamente o *back-up*. A verificação será realizada por meio da verifião do log do software de backup.

5. EQUIPE DE CONTINGÊNCIA

5.1. Para coordenar todas as ações necessárias em situações de contingência, bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da **GESTORA**, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance e Risco (Coordenador de Contingência);
- Diretor de Gestão;
- Encarregado pelo Tratamento de Dados Pessoais (DPO); e
- Gestor de TI.

5.2. Os membros dessa equipe tomarão as medidas cabíveis para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, na ausência de um dos diretores, isoladamente. Todos os colaboradores da **GESTORA** serão comunicados imediatamente sobre essa decisão.

5.3. O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com a Empresa de TI para comunicar o acionamento do Plano de Contingência e tratar do acesso aos dados/sistemas, bem como efetuar o desvio das ligações dos telefones do escritório para linhas alternativas.

6. EFETIVA CONTINGÊNCIA

6.1. O Plano de Contingência será acionado quando for identificada qualquer ocorrência ou situação que dificulte ou impeça a rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, aos clientes da **GESTORA** e à **GESTORA** propriamente dita.

6.2. Neste cenário, considera-se basicamente a impossibilidade ou dificuldade de manter o funcionamento normal da **GESTORA** devido a problemas de ordem técnica (*hardware*), física (acesso ao escritório), pessoal (ausência significativa de funcionários) e de infraestrutura (falta de energia).

6.3. Nessa situação, o Diretor de Compliance e Risco da **GESTORA** deverá acionar este Plano, em caráter imediato, e iniciar também imediatamente a avaliação das causas que geraram a contingência para providenciar sua solução o mais rapidamente

possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo:

(a) Comunicar imediatamente o ocorrido à toda a equipe interna, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição, indicando nessa oportunidade qual o procedimento a ser adotado por cada colaborador de acordo com a contingência ocorrida;

(b) Comunicar, em até 24 (vinte e quatro) horas, seus clientes/investidores via e-mail, celular ou aplicativo de troca de mensagens (ex: WhatsApp);

(c) Caso seja verificada a necessidade de sair do escritório da **GESTORA**, os colaboradores poderão continuar a desempenhar suas atividades através de H*ome Office*, uma vez que todos os arquivos podem ser acessados pela nuvem e seguirão as recomendações descritas no Ofício-Circular nº 2/2020-CVM/SMI[1], emitido pela Comissão de Valores Mobiliários, ou outra norma que eventualmente venha a substituí-lo. Ainda, as atividades operacionais da **GESTORA** deverão ser realizadas observando as disposições previstas nas políticas internas da **GESTORA**, principalmente a Política de Segurança da Informação e Segurança Cibernética e a Política de Home Office.

(d) A continuidade das operações da **GESTORA** deverá ser assegurada no próprio dia útil da ocorrência da contingência no escritório físico, de modo que as atividades diárias não sejam interrompidas ou gravemente impactadas.

6.4. O Diretor de Compliance e Risco da **GESTORA** deverá acompanhar todo o processo acima descrito até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela **GESTORA** e reportar eventuais alterações e atualizações da contingência aos demais Colaboradores.

6.5. O serviço de e-mail da **GESTORA** é garantido pela Microsoft, que provém suporte 24/7, serviço de *antispam*, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

6.6. A **GESTORA** conta com 3 (três) operadoras de telefone, i.e., Algar, Vivo e Mundivox. Em caso de falhas nas linhas telefônicas, os colaboradores da **GESTORA** ainda possuem celulares que podem substituir a telefonia fixa.

6.7. As informações do portfólio, além de estarem nos sistemas internos da **GESTORA,** são disponibilizadas diariamente pelo administrador, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos.

[1] https://conteudo.cvm.gov.br/legislacao/oficios-circulares/smi/oc-smi-0220.html

6.8. Em caso de falha de fornecimento de energia, a **GESTORA** possui *nobreak* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de outras duas estações de trabalho (*desktops*) na Empresa de TI para a efetiva continuidade dos negócios.

7. DOCUMENTAÇÃO

7.1. O serviço de e-mail da **GESTORA** está hospedado nos servidores da Microsoft. O serviço possui suporte 24/7, serviço de *antispam*, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A **GESTORA** detém uma conta corporativa, que é garantida com todos os serviços de segurança e *back-up*, sendo executadas funções de *firewall* e antivírus no nível do roteador. Além disso, o antivírus (*software*) é ativado em cada computador individual na rede do escritório da **GESTORA**.

7.2. Com seus procedimentos de *back-up* externo e acesso remoto a e-mails, a **GESTORA** continuará a funcionar, mesmo se não for possível ter acesso físico ao escritório. Além disso, todos os colaboradores têm acesso imediato a todas as informações contidas nos seus e-mails em qualquer situação de emergência.

7.3. Deverá ser mantida no servidor remoto uma lista com as informações de todos os integrantes da **GESTORA**, das corretoras com as quais se realizam negócios, dos clientes e dos prestadores de serviço contratados.

8. TESTES PERIÓDICOS

8.1. O Diretor de Compliance e Risco tem por obrigação manter este Plano de Contingência atualizado, bem como realizar a validação a cada **12 (doze) meses** dos procedimentos estabelecidos neste Plano de Contingência.

8.2. O Diretor de Compliance e Risco também é responsável por realizar testes de contingências que possibilitem que a **GESTORA** esteja preparada para eventos dessa natureza, proporcionando-lhe condições adequadas de continuidade de suas operações.

8.3. Anualmente, é realizado um teste de contingência para verificar:

a) Acesso aos sistemas;
b) Acesso ao e-mail corporativo;
c) Acesso aos dados armazenados; e
d) Qualquer outra atividade necessária para continuidade do negócio.

8.4. O resultado do teste é registrado em relatório, que serve como indicador para regularização das possíveis falhas, problemas e dificuldades encontradas, para que sejam providenciadas as correções ou adequações necessárias para as melhorias do Plano de Contingência.

8.5. Não obstante, este Plano deve ser atualizado toda vez que ocorrerem mudanças relevantes que altere a estrutura operacional de algum departamento da **GESTORA**, como por exemplo: inclusão/alteração/exclusão significativa de sistemas; abertura e/ou encerramento de filiais; modificação de locais alternativos ou sistemas de contingência; e resultados negativos nos testes do Plano.

8.6. Para realização dos testes de contingências mencionados no item 8.2. acima, o Diretor de Compliance e Risco contará com o apoio da Empresa de TI no que couber, podendo, inclusive, solicitar que a própria Empresa de TI realize e, adicionalmente, comprove a realização dos controles e procedimentos acima estabelecidos que lhe competem, respectivamente, monitorar e executar.

9. CONTROLE DE VERSÕES

Este Plano será revisado anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações		
Data	**Versão**	**Responsável**
Abril de 2019	1ª	Diretor de Compliance e Risco
Maio de 2022	2ª e Atual – Revisão anual	Diretor de Compliance e Risco