KÖLI CAPITAL GESTORA DE RECURSOS S.A.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Janeiro/2024

1. INTRODUÇÃO E OBJETIVOS

1.1. O Plano de Contingência e Continuidade de Negócios ("Plano de Contingência") tem como objetivo definir os procedimentos a serem adotados pela equipe da **KÖLI CAPITAL GESTÃO DE RECURSOS LTDA.** ("Gestora"), no caso de contingência, de modo a impedir descontinuidade operacional por problemas que impactem no funcionamento da empresa. Foram estipuladas estratégias e planos de ação com o intuito de garantir que os serviços essenciais da Gestora sejam previamente identificados, e preservados mesmo na ocorrência de um imprevisto ou um desastre.

1.2. O modo contingencial 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, à Gestora e seus clientes.

1.3. As ações a serem tomadas quando uma situação dessas ocorre é chamada de Plano de Contingência.

1.4. O Plano de Contingência é compartilhado com todos os colaboradores da Gestora e faz parte da sua cultura. Os colaboradores são preparados para exercer suas funções em situações contingenciais e dessa forma os impactos serão minimizados.

2. ESTRUTURA

2.1. Para atendimento às necessidades mínimas de manutenção dos serviços/atividades da Gestora, foi definida uma estrutura física mínima e procedimentos que devem ser adotados toda a vez em que uma situação que caracterize uma contingência às operações da Gestora seja identificada.

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

(i) TI: fundamental para o funcionamento da Gestora, no sentido de que todas as comunicações com corretoras, administradores de fundos 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 investimento, transferência de recursos e pagamento de despesas da Gestora, dentro outros);

(ii) 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; 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, etc.

2.3. Tendo identificado essas 3 (três) áreas principais do ponto de vista da estrutura da Gestora e dos processos sob sua responsabilidade, os riscos 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, falha e/ou interrupção no fornecimento de serviços essenciais como a falta de energia elétrica, falta de água, falha nas conexões de rede, falha nos links de internet, falha nas linhas telefônicas, falhas nos sites das empresas que fornecem sistemas de uso da Gestora, etc.; e

(i) Problemas de 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 greves, por exemplo de transporte público, interdições pelas autoridades do prédio ou do entorno do escritório da Gestora etc.

2.4. 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.

2.5. Conforme avaliação de risco da Gestora foram definidos 2 (dois) ambientes básicos que devem ser considerados nas ações a serem tomadas quando da ativação do Plano de Contingência da Gestora. Esses ambientes são: Físico e o Tecnológico.

(i) Ambiente Físico

O ambiente físico é definido como o espaço onde as operações diárias da empresa são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e equipamentos necessários a essa operação, como também o acesso seguro a esses recursos.

Em ocorrendo situações de problemas de acesso às suas dependências, a equipe da Gestora deve continuar a desempenhar suas atividades através de Home Office, uma vez que todos os arquivos podem ser acessados pela nuvem. Além disso, há a vinculação dos e-mails e armazenamento no Microsoft Office 365. Na impossibilidade

de acesso ao ambiente físico da gestora, o plano de contingência é ativado para que os Colaboradores sigam as instruções da equipe de contingência sobre como agir, ou seja, permanecer trabalhando através de Home Office ou, caso necessário deslocar-se para a sala disponível na Rua do Carmo, nº 43, 8º andar, centro, RJ ("Escritório de Contingência").

Os equipamentos mínimos necessários para a manutenção das funcionalidades em caráter contingencial são: (i)1 Núcleo de processador; (ii) 3.5 Gb Ram; (iii) 100 GB de espaço em disco; (iv) Windows 7, 8 ou 10; (v) Internet de 4 Mb ou superior, Microsoft Office (versão 13 ou superior).

(ii) Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a Gestora possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela empresa em seu dia a dia e garantia de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da empresa, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, softwares e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares de Colaboradores da Gestora. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência da Gestora, de forma a que também estes tenham conhecimento da situação, de forma a impactar o mínimo possível a operação da Gestora.

O armazenamento de todo o banco de dados da Gestora é realizado na nuvem, de forma que o back-up das informações ocorre imediatamente.

E-mail

A Gestora utiliza um serviço de e-mail em *cloud* (nuvem) na modalidade de *Software as a Service* (SaaS) oferecido pela Microsoft (Exchange online Office 365). O serviço de e-mail pode ser acessado diretamente pela web através de senha. O Exchange Online protege as informações das caixas de correio utilizando recursos avançados, tais como: filtros antimalware e antispam, assim como a prevenção contra perda de dados. Os servidores possuem redundância global e recursos avançados de recuperação em caso de desastres. Além disso, para garantir o funcionamento ininterrupto do serviço de e-mail, a Microsoft oferece uma disponibilidade de 99,9%.

Dados e Sistemas

O backup só deve ser restaurado em caso de deleção, problema de corrupção ou edição incorreta. Em caso de restauração do backup, o colaborador deve validar os dados recuperados e prosseguir com as atividades. Caso haja alguma inconsistência na recuperação dos dados, o Coordenador de Contingência (conforme definido abaixo) deve ser comunicado imediatamente para que providências sejam tomadas em relação à nova restauração de dados.

3. EQUIPE DE CONTINGÊNCIA

3.1. 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, Risco e PLD (Coordenador de Contingência); e
- Diretor de Gestão.

3.2. Essas pessoas deverão tomar as decisões necessárias para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, na ausência de um dos diretores, isoladamente e deve ser comunicada imediatamente a todos os colaboradores da Gestora. O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com todos os colaboradores, e avaliará a necessidade de contato com algum cliente e/ou prestador de serviço, para comunicar o modo contingencial e tratar do acesso aos dados/sistemas, bem como efetuar o desvio das ligações dos telefones do escritório para linhas alternativas.

4. CENÁRIOS DE CONTINGÊNCIA

4.1. A ocorrência de eventos de contingência deverá ser avaliada pela Equipe de Contingência da Gestora e, com base nas informações disponíveis, deverá ser tomada uma decisão quanto ao acionamento do Plano de Contingência.

4.2. Com base na decisão tomada pela Equipe de Contingência, a Gestora deverá adotar os procedimentos a seguir listados.

Situação de Contingência

4.3. Neste cenário, considera-se basicamente a impossibilidade ou dificuldade em

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).

4.4. Nessa situação, o Diretor de Compliance, Risco e PLD 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, quais sejam:

(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) Caso seja verificada a necessidade de sair do escritório da Gestora, os colaboradores poderão continuar a desempenhar suas atividades através de Home Office, uma vez que todos os arquivos podem ser acessados pela nuvem. Em havendo necessidade, a equipe da Gestora irá se reunir no Escritório de Contingência, que dispõe de ambiente e infraestrutura para tanto e prosseguirá com a gestão remota dos fundos sob sua administração. 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.

4.5. O Diretor de Compliance, Risco e PLD 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.

5. ASPECTOS GERAIS

5.1. Este Plano de Contingência é de uso restrito dos colaboradores da Gestora e não pode ser divulgado para terceiros, exceto se autorizado pela Equipe de Contingência.

5.2. É responsabilidade do Diretor de Compliance, Risco e PLD manter este Plano atualizado, bem como a realização de validação a cada 12 (doze) meses dos procedimentos estabelecidos neste Plano de Contingência.

5.3. Ainda, o Diretor de Compliance, Risco e PLD realizará testes de contingências que possibilitem que a Gestora esteja preparada para eventos desta natureza, proporcionando à Gestora condições adequadas para continuar suas operações.

5.4. Sendo assim, 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.

5.5. O resultado do teste é registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

HISTÓRICO DAS ATUALIZAÇÕES DESTE PLANO DE CONTINGÊNCIA E CONTINUIDADE

Histórico das atualizações		
Data	**Versão**	**Responsáveis**
Agosto/2019	1ª Versão	Diretor de Compliance, Risco e PLD
Setembro/2020	2ª Versão	Diretor de Compliance, Risco e PLD
Julho/2021	3ª Versão	Diretor de Compliance, Risco e PLD
Agosto/2022	4ª Versão	Diretor de Compliance, Risco e PLD
Abril/2023	5ª Versão	Diretor de Compliance, Risco e PLD
Janeiro/2024	6ª e Atual	Diretor de Compliance, Risco e PLD