Política de Contingência e Continuidade de Negócios

I. Objetivo

Esta Política de Contingência e Continuidade de Negócios ("Política") da A3 Performance Gestão de Recursos Ltda. ("A3 Performance" ou "Gestora") tem por objetivo estabelecer o Plano de Contingência e Continuidade de Negócios da Gestora ("Plano"), com medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a condução das atividades da Gestora.

Adotou-se visão pragmática dos eventos com maior possibilidade de ocorrência, dada a localização e características das instalações da edificação em que se encontra a sede da Gestora. Assim, buscou-se conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos.

Dessa forma, é possível conhecer e minimizar os danos no período pós-contingência, minimizar os prejuízos para a Gestora, seus Clientes e seus Colaboradores que possam decorrer da interrupção não programada de suas atividades, e reduzir o tempo para a sua normalização.

II. Princípios Básicos

Para a eficaz implementação do Plano, a Gestora busca conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para tal finalidade, são tomadas medidas que permitem:

- Conhecer e minimizar os danos no período posterior a eventos;
- Minimizar as perdas para seus Clientes, seu negócio e seus Colaboradores originados pela interrupção abrupta de suas atividades; e
- Normalizar o mais rápido possível as atividades de gestão.

Para redução e controle de eventuais perdas com contingências, todos os Colaboradores são instruídos e atualizados constantemente sobre processos de procedimentos de backup e salvaguarda de informações relacionados as suas atividades. Para tanto, a Gestora mantém um conjunto de procedimentos alternativos a serem adotados pelas áreas de suporte técnico quando da inoperância de um recurso técnico (sistemas, comunicações, componentes, etc.), objetivando a sua recuperação após o evento.

III. Eventos/Ameaças potenciais

Após análise de potenciais ameaças à continuidade de negócios da Gestora, seguem abaixo os principais eventos aferidos:

- Baixa conectividade ou perda de conectividade com a internet, falha no sinal ou

hardware de telecom (incluindo voz) ou na rede de celular;

- Falta de energia (apagão), falta local de energia ou Falha de circuito / terminal;
- Interrupção dos transportes, greves, protestos ou guerras ou acidentes relevantes;
- Clima extremo, fogo, inundação, explosão, vazamento de gás ou alerta de segurança;
- Invasão sistêmica que prejudique dados internos;
- Inacessibilidade temporária do escritório;
- Qualquer outra situação que ameace o ambiente da Gestora, que não descrita acima.

A lista de cenários de crise acima não tem pretensão de ser exaustiva. Na ocorrência de um evento listado ou outra situação de crise não previsível ("Crise"), a Gestora se depara geralmente com a combinação de um ou mais dos seguintes desdobramentos:

1. Perda de Acesso ao Prédio: significa que todos os Colaboradores da Gestora que estiverem no prédio no momento do incidente deverão evacuá-lo e quem estiver fora não poderá entrar.
2. Perda de Pessoal: afeta os profissionais da Gestora e em geral inclui ferimentos, doenças, morte e incapacidade de chegar no escritório (ou potencialmente trabalhar de casa).
3. Perda de Infraestrutura de TI: inclui falha parcial ou completa da rede de TI, incluindo hardware e softwares essenciais, sendo essencial os prestadores de serviços assim que possível para instaurar os sistemas de back-up conforme abaixo.
4. Perda de Infraestrutura de Telecom: inclui falha parcial ou completa da rede de telecomunicações, incluindo equipamentos, telefones fixos, celulares e a internet).
5. Perda de Energia Elétrica: Falta de energia devido a apagões ou interrupção da rede elétrica devido a chuvas e/ou quedas de árvores.

IV. Retomada das atividades

A Gestora empenhará seus melhores esforços para manter atualizados os processos relacionados com as atividades fins que, por sua natureza, possam ser considerados críticos. Assim, em caso de ocorrência de determinados eventos, dependendo da magnitude e extensão destes, pode ser possível retomar as operações com tempo e custo reduzidos.

Nesse sentido, para armazenar e permitir a recuperação de informações necessárias para a realização das atividades diárias, a Gestora adota um procedimento de backup diário de seus arquivos sendo um backup mantido na sede e outro externo à sede da Gestora, cujo acesso, é de acordo com as diretrizes de segurança de informação especificadas na Política de Segurança de Informação e de Segurança Cibernética.

A Gestora conta com equipamento de *no-break* que suporta as unidades de trabalho e servidor, instalado para manter estável e suprir o fornecimento de energia elétrico em caso de flutuação e/ou interrupção não programada.

Na impossibilidade de acesso ao local de sede da Gestora, procedimentos para acesso VPN e web dos sistemas serão efetuados, de modo que os trabalhos sejam retomados de maneira breve e sem prejuízo.

V. Procedimentos de Ativação do Plano

O Diretor de *Compliance* será o principal responsável pela operacionalização do Plano da A3 Performance ("Líder do Plano").

A Gestora desenvolveu uma lista de Contatos de Emergência que inclui os nomes, telefones, endereços de e-mail dentre outras informações críticas para o negócio. Esta lista inclui colaboradores-chave, distribuidores de fundos, contrapartes prestadores de serviços essenciais dentre outros contatos. Esta lista será revista e atualizada ao menos anualmente.

- **Procedimento em caso de Crise**

Uma vez que o Líder do Plano tenha sido acionado devido a uma potencial Crise, este deverá convocar os Colaboradores-chave da Gestora para formar um grupo de trabalho e avaliar conjuntamente a situação e próximos passos. Caso não seja possível devido à situação emergência, poderá tomar as decisões para gerir a crise individualmente.

Na etapa inicial, aspectos e decisões fundamentais deverão analisadas e tomadas após o incidente. O foco da reunião do grupo ou, se for o caso, do Líder do Plano deverá compreender uma análise do que aconteceu, motivos e extensão, consequências imediatas e gravidade da situação, segurança dos Colaboradores e medidas imediatas, devendo decidir pela formalização ou não da Crise.

Se for caracterizado um cenário de Crise, devem os membros do grupo ou o Líder do Plano efetuar a comunicação ao restante dos Colaboradores, informando as medidas imediatas, que poderão abranger a evacuação do prédio, acionar assistência médica imediata, notificação dos serviços de emergência, realocação de Colaboradores internos, definindo se o local alternativo será utilizado e por quem, formas de comunicações e notificação de parceiros-chave estratégicos.

Com relação à parte de segurança cibernética, a Gestora, em conjunto com a empresa ENDEV, prestador de serviços de TI, deverá definir medidas a serem tomadas, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

A fase de recuperação começa após a Crise inicial ter sido contornada, já tendo eventuais Colaboradores sido recolocados, a redundância de TI acionada e terceiros-chave notificados.

Será realizado um call diário ou em outra periodicidade discutida para acompanhamento pelo grupo de trabalho, com um sumário elaborado pelo Líder do Plano contendo as medidas a serem tomadas, responsável e prazos. O Comitê de Riscos e *Compliance* deverá se reunir também para avaliar o impacto do incidente nos diversos riscos (mercado, crédito,

operacional, dentre outros) e caso necessário tomar as devidas ações, enquanto que o Diretor de Gestão verificará se todas as informações necessárias ao portfólio estão seguras e a área de Gestão definirá se decisões de investimento são requeridas embora o trading discricionário deva ser minimizado de acordo com as novas condições operacionais da empresa.

Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados ao grupo de trabalho de crise. Colaboradores externos relevantes deverão ser mantidos atualizados na forma definida pelo referido comitê.

Já a fase da retomada refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao full compliance, reconstrução de eventuais sistemas, reformas do escritório e eventuais mudanças.

- **Comunicação Externa**

Caso ocorra um evento/ameaça cujo resultado seja a inacessibilidade temporária ou permanente do escritório ou em um cenário de Crise, a área de Compliance é responsável por elaborar comunicado formal aos investidores e terceiros contratados. Na impossibilidade de atuação da área de *Compliance*, somente a Diretoria está autorizada a realizar esta função, sendo absolutamente vedado aos demais Colaboradores a comunicação pública sobre o ocorrido.

VI. Testes de Contingência

Será planejada a realização de testes de contingências em periodicidade a ser determinada, de modo a possibilitar que a Sociedade esteja preparada para a continuação de suas atividades. Tais testes devem ser realizados ao menos uma vez a cada 12 (doze) meses ou em prazo inferior se exigido pela regulação em vigor, para verificar o seguinte:

- Acesso aos sistemas;
- Acesso ao e-mail corporativo;
- Acesso aos dados armazenados em procedimento de backup;
- Outros necessários à continuidade das atividades.

O teste terá como objetivo também avaliar se o Plano é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se pode ser ativados tempestivamente.

VII. Disposições Finais

Este Plano será revisado anualmente, e será alterado quando necessário e sem aviso prévio. As alterações serão divulgadas a todos os Colaboradores da Sociedade pela Área de *Compliance*.