LOGOS GESTÃO DE RECURSOS LTDA.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Janeiro de 2022

1. Objetivo

Este Plano de Contingência e Continuidade de Negócios (“Plano de Contingência”) tem como objetivo definir os procedimentos a serem adotados pela equipe da LOGOS GESTÃO DE RECURSOS LTDA. (“Gestora”), em Eventos de Contingência, de modo a impedir descontinuidade operacional por problemasque impactem no funcionamento da Gestora no âmbito da sua atividade de gestão de recursos.

Os Eventos de Contingência são definidos como qualquer evento que implica na alteração da rotina diária de operação, como por exemplo: suspensão total ou interrupção temporária na prestação de serviços por provedores de energia, acesso à internet, serviços de telefonia, catástrofes naturais que impeçam o acesso ao prédio, dentre outros.

2. Estrutura

A Gestora dispõe de infraestrutura *Cloud-First*, portanto todos os seus sistemas críticos se encontram hospedados em nuvem, podendo ser acessados remotamente e ambientes de alta disponibilidade.

2.1 Sistemas Críticos

Para fins deste Plano de Contingência, os Sistemas Críticos são definidos como se segue:

a) E-mails;

b) Sistema de Risco e Gestao do Ativo;

c) Sistema de trade e compliance: Order Management System (OMS); e

d) Terminais Bloomberg

3. Testes de Contingência

Os testes de contingências serão realizados em periodicidade a ser determinada, sob responsabilidade do Diretor de Riscos e de Compliance, de modo a possibilitar que a Gestora esteja preparada para a continuação de suas atividades. Os testes devem ser realizados ao menos 1 (uma) vez a cada 12 (doze) meses com o objetivo de verificar as condições para os sistemas críticos e demais serviços:

a) Acesso aos sistemas internos;

b) Acesso ao e-mail corporativo;

c) Acesso aos dados armazenados em procedimento de backup; e

d) Máquinas físicas e servidores virtuais em nuvem.

4. Equipe De Contingência

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 como Equipe de Contingência:

- Diretor de Risco e Compliance (Coordenador de Contingência);

- Suporte/Analista de TI

Essas pessoas deverão tomar as decisões necessárias para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, no caso de impossibilidade, com os demais administradores da Gestora.

5. Procedimentos

Na ocorrência de um Evento de Contingência será estabelecido um Comitê de Contingência, composto essencialmente pela Equipe de Contingência, que será responsável por:

a) avaliar os impactos diretos e indiretos;

b) elaborar e implementar um plano de ação para recuperação dos serviços impactados;

c) comunicar aos colaboradores o referido plano de ação;

6. Principais Contingências Mapeadas

Backup e Recuperação de Dados

A Gestora mantém backup de todos os seus dados na nuvem, possibilitando o acesso às últimas versões de cada arquivo para restauração. Todas as informações estratégicas da Gestora são armazenadosem nuvem, com redundância e backup real time, possibilitando imediata disponibilidade de recuperação.

Sistemas Críticos

Os sistemas necessários para o imediato processamento dos negócios e gerenciamento dos limitesde risco, enquadramento, precificação, pre-matching de operações e boletagem são considerados SistemasCríticos e, portanto, devem apresentar alta disponibilidade e pequeno tempo de subida no ambiente de produção. Os sistemas críticos são definidos conforme o item 2.1.

Queda de energia e infraestrutura

Em caso de queda de energia, o escritório da Gestora possui gerador para as áreas privadas. Caso ogerador não funcione ou deixe de operar, a Gestora possui no-breaks de até 1 (uma) hora. No caso do gerador falhar o acesso aos Sistemas Críticos da Gestora será feito de forma remota, por meio do armazenamento na nuvem ou no site de contingência.

Queda do link para acesso à internet

A Gestora conta com link redundante de internet. Caso ambos os links deixem de funcionar, o acessoaos arquivos da Gestora poderá ser feito remotamente por meio dos arquivos gravados na nuvem.

Contingências com servidor de e-mail

O serviço de e-mail da Gestora é hospedado em nuvem, garantindo a continuidade do acessoremoto.

7. Disseminação do Plano

Para redução e controle de eventuais perdas com contingências, todos os colaboradores deverão conhecer os procedimentos básicos de backup e salvaguarda de informações (confidenciais ou não), planosde evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho.

8. Disposições Gerais

Em cumprimento a Instrução CVM n.º 558/15, o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, o presente Plano de Continuidade de Negócios descreve todos os procedimentos adotados pela instituição em caso de contingências e desastres.