PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS DA GREENWICH GESTÃO DE RECUROS LTDA.

1. OBJETO

O propósito deste Plano de Contingência e Continuidade de Negócios ("Plano de Contingência") da **Greenwich Gestão de Recursos Ltda.** ("GREENWICH"), é permitir que a organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.

O Plano de Continuidade é ativado para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização. Ele será executado integral ou parcialmente e em qualquer etapa da resposta a um incidente.

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

O Plano de Contingência é compartilhado com todos os colaboradores da GREENWICH 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. PRINCÍPIOS GERAIS DE CONTINUIDADE DE NEGÓCIOS E ESTRUTURA

A GREENWICH não mantém sob sua guarda o cadastro de seus clientes, embora tenha acesso a diversas informações confidenciais, a guarda pertence ao administrador fiduciário dos Veículos. No entanto, conforme previsto no Manual de Ética e *Compliance* da GREENWICH, todas as informações de seus clientes são confidenciais e serão sempre mantidas em sigilo absoluto. Os desrespeitos em relação a esta política estão sujeitos à sanção.

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

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 GREENWICH, 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 GREENWICH, dentro outros);

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

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

Tendo identificado essas 3 (três) áreas principais do ponto de vista da estrutura da GREENWICH 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 GREENWICH, etc; e

(ii) 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 GREENWICH etc.

Com base no levantamento da estrutura da GREENWICH e no mapeamento de riscos, a GREENWICH tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações.

Conforme avaliação de risco da GREENWICH foram definidos 2 (dois) ambientes básicos que devem ser considerados nas ações a serem tomadas quando da ativação do Plano de Contingência da GREENWICH. 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 GREENWICH 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 Google Drive e o sistema aplicável 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 residência de um dos Diretores da GREENWICH ("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 10; (v) Internet de 4 Mb ou superior.

(ii) Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a GREENWICH 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 garantira 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 GREENWICH possui equipamentos de contingência em locais distintos do escritório central para uso emergencial. Este escritório tem uso permanente, por meio de um sistema de rodízio onde um ou mais colaboradores podem, de tempos em tempos, trabalhar no mesmo. Para garantir a confidencialidade das informações, a GREENWICH utiliza *Virtual Private Network* ("VPN"), que é uma rede segregada utilizada para criptografar dados que trafegam pela internet. Este modelo utiliza o sistema cliente/servidor, onde o servidor está online 24 horas por dia aguardando conexões do cliente.

A GREENWICH possui um Data Center que é equipado com *no-break's,* ar condicionado e com um servidores de alto desempenho, capacidade, disponibilidade

e redundância a falha que garante a continuidade dos negócios. O link de internet e telefonia possui um ponto de acesso no prédio e com contratos que garantem alto nível de disponibilidade anual dos serviços.

Todos os dados possuem back-up em duas diferentes localizações, localizados no Data Center e também em Nuvem (*Cloud*), este com contrato que garante confidencialidade e o nível de disponibilidade anual dos serviços de 99,9% e são gerados diariamente, sendo que o back-up é incremental durante toda semana, ou seja, apenas os dados que foram modificados são incrementados ao back-up *full* (completo) semanal, economizando assim espaço em disco e facilidade de gerenciamento. Adicionalmente é realizado um back-up *full* (completo) durante os finais de semana. São realizados testes frequentes para garantir o funcionamento em alguma falha, que seja necessária a utilização do recuperação da base de dados. Além disso, todas as ligações são gravadas e guardadas por dois anos, apesar da não obrigatoriedade.

A GREENWICH possui alternativas para monitorar e operar os mercados caso os sistemas de cotações deixem de funcionar, uma lista em local de fácil acesso com os nomes e telefones dos fornecedores de sistemas para solucionarem os problemas no menor tempo possível, bem como alternativas de comunicação caso ocorra algum problema de telefonia e internet.

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. Dessa forma, o Colaborador poderá ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

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

A empresa WeON Contact Center Omnichannel, com endereço na Rua R. Heitor Stockler de França, 396 - Centro Cívico, Curitiba - PR, 80030-030, Tel. (41) 3075-1375, presta os serviços de Tecnologia da Informação à GREENWICH, incluindo mas não se limitando a assistência de: rede interna, Firewall, Wireless, DHCP, Links de Internet, Hospedagem, CPUs \ Monitores \ Impressoras \ Scanners \ Fax,

Antivírus, Servidores, Rotinas de Backup, Controladores de Domínio, Acesso Remoto, Servidor de Arquivos, E-mail, CPD, Criação e Desligamento de Usuários.

Diariamente, às 00:00hr, é realizado o backup dos servidores utilizando o serviço de Data Center e também em Nuvem. Todos os dados possuem back-up em duas diferentes localizações, localizados no Data Center e também em Nuvem (Cloud), este com contrato que garante confidencialidade e o nível de disponibilidade anual dos serviços de 99,9% e são gerados diariamente, sendo que o back-up é incremental durante toda semana, ou seja, apenas os dados que foram modificados são incrementados ao back-up full (completo) semanal, economizando assim espaço em disco e facilidade de gerenciamento. Adicionalmente é realizado um back-up full (completo) durante os finais de semana.

3. EQUIPE DE CONTINGÊNCIA

Para coordenar as atividades relacionadas a este Plano, bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da GREENWICH, foram definidos os seguintes responsáveis pela Equipe de Contingência:

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

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 GREENWICH. O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com a empresa terceirizada responsável pela Tecnologia da Informação da GREENWICH, 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

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

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

Situação de Contingência

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

Nessa situação, o Diretor de Compliance e Risco da GREENWICH 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 GREENWICH, 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 GREENWICH irá se reunir no Escritório de Contingência localizado na residência de um dos Diretores da GREENWICH que dispõe de ambiente e infraestrutura para tanto e prosseguirá com a gestão remota dos fundos sob sua administração. A continuidade das operações da GREENWICH 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.

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

5. ASPECTOS GERAIS

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

É responsabilidade do Diretor de Compliance e Risco manter este Plano atualizado, bem como a realização de validação a cada **12 (doze) meses** dos procedimentos

estabelecidos neste Plano de Contingência.

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

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.

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.

Janeiro de 2019.