ALGARVE GESTÃO DE INVESTIMENTOS LTDA.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS DA ALGARVE GESTÃO DE INVESTIMENTOS LTDA.

Responsáveis: Diretores da **ALGARVE GESTÃO DE INVESTIMENTOS LTDA.**
Área: *Compliance*

O presente Plano de Contingência e Continuidade dos Negócios ("Pleno de Contingência") tem como objetivo definir os procedimentos que deverão ser seguidos pela **ALGARVE GESTÃO DE INVESTIMENTOS LTDA.** ("**ALGARVE**"), no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipuladas estratégias e planos de ação com o intuito de garantir que os serviços essenciais da **ALGARVE** sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

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

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

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.

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

1. Estrutura Operacional

1.1. A **ALGARVE** é uma gestora de recursos de terceiros, de modo que precisa contar com uma estrutura operacional desenvolvida e preparada para eventuais emergências. O suporte para essa estrutura operacional é um corpo funcional capacitado com áreas de apoio.

2. Política e procedimentos para *backup*

2.1. Diariamente, sempre às 00h00min, todos os arquivos armazenados em um servidor seguro, localizado na sede da Algarve, são criptografados e copiados de maneira automática para um HD externo e para um servidor remoto da empresa Amazon Web Services.

2.2. Pela norma interna, o *back-up* se dará da seguinte forma:

De acordo com norma interna da gestora, os arquivos relativos à operação são armazenados no servidor da rede.

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

(ii) o *restore* de dados deve ser solicitado ao departamento de TI e será realizado de acordo com os procedimentos específicos
(iii) as mídias de *back-up* serão armazenadas em local apropriado dentro da **ALGARVE**, sendo que semanalmente uma mídia será enviado para fora da sede da empresa, retornando na semana seguinte, quando uma nova mídia será enviada e serão auditadas mensalmente, conforme item 2.3.
(iv) as mídias (suprimentos) serão adquiridas pela **ALGARVE**, sempre que necessário.

2.3. Verificação e teste de restauração: mensalmente o *software* será configurado para verificar automaticamente o *backup*. A verificação será realizada por meio da comparação do conteúdo da cópia de segurança com os dados no disco.

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 **ALGARVE**, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance (Coordenador de Contingência);
- Diretor de Risco; 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 **ALGARVE**. O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com os Colaboradores que prestam serviço de Tecnologia da Informação na **ALGARVE**, 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.

4. Efetiva Contingência

4.1. 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 **ALGARVE** e à **ALGARVE**.

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

4.3. Nessa situação, o Diretor de Compliance da **ALGARVE** 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 **ALGARVE**, os colaboradores poderão continuar a desempenhar suas atividades através de Home Office, uma vez que todos os arquivos podem ser acessados pela nuvem. Todos os integrantes da equipe de gestão possuem a alternativa de utilização do *Bloomberg Anywhere*, o que permitirá a continuidade da gestão das carteiras através de qualquer conexão de internet. A continuidade das operações da **ALGARVE** 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.

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

4.5. O serviço de e-mail da **ALGARVE** é garantido pela Google, que provém suporte 24/7, serviço de **anti spam, antivírus**, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

4.6. A **ALGARVE** conta com 2 (duas) operadoras de telefone. Em caso de falhas nas linhas telefônicas, os colaboradores da **ALGARVE** ainda possuem celulares que podem substituir a telefonia fixa.

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

4.8. Em caso de falha de fornecimento de energia, a **ALGARVE** possui nobreak para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de outras quatro estações de trabalho (desktops) para a efetiva continuidade dos negócios.

5. Aspectos Gerais

5.1. O serviço de e-mail da **ALGARVE** está hospedado nos servidores do Google, onde detém uma conta corporativa, que é garantido por todos os serviços de segurança é backup de uma das maiores empresas do mundo, dando acesso imediato a todas as informações contidas nos e-mails dos colaboradores em qualquer situação de emergência que se apresente na operação.

5.2. Com seus procedimentos de *back-up* externo e acesso remoto a e-mails, a **ALGARVE** pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório.

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

6. Documentação

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

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

6.3. 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.

6.4. 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.

Última atualização: Janeiro/2019