PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

GARDE ASSET MANAGEMENT GESTÃO DE RECURSOS LTDA.
CNPJ/ MF 18.511.433/0001-77

E DA

GARDE PREVIDÊNCIA ADMINISTRAÇÃO DE RECURSOS LTDA.
CNPJ/ MF 30.701.673/0001-30

Data: 31 de dezembro de 2018

Esse Plano de Contingência e Continuidade dos Negócios ("Plano de Contingência") tem como objetivo definir os procedimentos que deverão ser seguidos pela Garde Asset Management Gestão de Recursos Ltda. ("Garde Asset") e pela Garde Previdência Administração de Recursos Ltda. ("Garde Previdência" e, quando em conjunto com a Garde Asset, "Garde"), no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da Garde 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 Garde dentro do contexto de seu negócio.

O Plano de Contingência, ainda, identifica duas variáveis para o funcionamento adequado da Garde: 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.

Já os processos são as atividades realizadas para operar os negócios da Garde. Os processos dependem da infraestrutura toda ou de parte da estrutura em funcionamento. Somente com os processos em andamento pode-se definir que o plano de ação foi bem executado.

1. Estrutura Operacional

1.1. A Garde Asset e a Garde Previdência são gestoras de recursos de terceiros, de modo que precisam 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. O *backup* dos servidores e sistemas será feito usando o método mais adequado e atual.

2.2. Os meios de armazenamento poderão variar entre fita, *online* pela Internet ou espelhando servidores em um local remoto. *Backups* serão realizados utilizando um *software* de *backup* dedicado apropriado para o sistema operacional utilizado.

2.3. Procedimentos de *backup & restore*: o *backup* dos servidores e sistemas será realizado utilizando-se as instalações padrões disponíveis dentro do software de *backup*. A documentação será produzida com detalhes suficientes para permitir que um usuário experiente do *software* de *backup* possa restaurar os dados.

2.4. Status do *backup*: o *software* de *backup* será configurado para alertar automaticamente o administrador para o status de qualquer *backup* realizado. O status do *backup* será analisado em uma base diária e quaisquer falhas identificadas serão corrigidas.

2.5. Verificação e teste de restauração: sempre que possível o *software* de *backup* 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.

2.6. A restauração de informações a partir do *backup* será testada periodicamente.

2.7. Ciclos de backup:

(i) Repositório de Dados - O *backup* completo dos sistemas importantes será realizado periodicamente, com *backups* incrementais todos os dias.

(ii) Esquema de rotação - Será utilizado o método simples de rotação diária, sendo que, no mínimo, 10 (dez) *backups* serão mantidos.

(iii) Backups diários - O *backup* será feito todos os dias, como parte de uma rotação diária simples. Um *backup* diário será composto de um *backup* completo ou um *backup* incremental/diferencial.

(iv) Backups semanais - Será composto de um grupo de 5 (cinco) fitas, com a fita sendo alterada em base semanal. Um *backup* semanal será composto de um *backup* completo.

(v) Configuração de *backups* mensais - A configuração dos *backups* mensais consistirá em exportar ou fazer *backup* das definições de configuração de uma aplicação. A configuração será armazenada em um servidor em que é feito um *backup* diário.

2.8. Armazenamento de *backup*: As mídias de *backup* serão armazenadas de forma segura quando não estiverem em uso. *Backups on-line* e de espelhamento de disco remoto serão realizados em um centro de dados a pelo menos 2 (dois) quilômetros de distância do centro de dados que contém a informação objeto do *backup*. Mídias removíveis, como fitas, serão armazenadas de forma segura em um cofre blindado e anti-incêndio quando não estiverem em uso. Para resiliência, várias mídias removíveis serão armazenadas fora do local. No mínimo, duas cópias do mais atualizado *backup* de dados serão armazenadas fora do local duas vezes por semana. A programação para o armazenamento externo será detalhado em um log.

2.9. Limpeza dos Drives de Fita: As unidades de fita usados para *backups* serão limpas numa base regular. Unidades de fita *autoloader* serão limpas semanalmente através de uma fita de limpeza no dispositivo. Outras unidades de fita serão limpas mensalmente.

2.10. Backup de aplicativos: Técnicas de *backup on-line* serão utilizadas para minimizar o tempo de inatividade. *Backups off-line* completos serão utilizados onde os *backups on-line* não estão disponíveis.

3. Efetiva Contingência

3.1. Na impossibilidade de se utilizar o espaço físico do escritório, a Garde poderá continuar a funcionar em qualquer centro de negócios da Regus no Brasil.

3.2. A Garde contratou junto à Regus um serviço que dá direito a 5 diárias por mês de escritório privativo com capacidade para 6 pessoas.

3.3. O serviço de e-mail da Garde é fornecido pela Mandic, com suporte 24/7, serviço de anti-spam, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A Garde utiliza ainda o Exchange da Microsoft que possibilita, via webmail, o acesso remoto de todas as mensagens pelos Colaboradores[1].

3.4. A Garde conta com links redundantes tanto de voz quanto de dados em caso de contingência.

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

3.6. Em caso de falha de fornecimento de energia, a Garde possui *nobreak* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e estações de trabalho. A unidade de quebra de fornecimento de energia conta com capacidade de processamento ininterrupto das operações (unidades de UPS - *Uninterruptiple Power Supply*).

4. Estrutura de Suporte

4.1. Além dos mecanismos convencionais para garantir a integridade das informações, como *backup* em servidores com *hardware* redundante, a Garde replica diariamente todos os seus sistemas operacionais (banco de dados, arquivos e e-mails) em servidores externos. Neste site, as empresas parceiras da Garde possuem sistemas de armazenamento de alta disponibilidade para *backup* e arquivamento, além de servidores para a operação contínua *fail-over*. No caso de falha, o *hardware* redundante passa a operar automaticamente.

4.2. Tal *hardware* redundante está à disposição para substituição, assim que o original apresentar qualquer problema. No caso de ocorrer uma falha, o monitoramento automático irá detectar o problema e alertar os diretores da Garde.

[1] Nos termos do Manual de Ética e *Compliance* da GARDE, Colaborador é aquele que possui cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança na GARDE.

4.3. A detecção automática de falhas em *hardware* permite a recuperação automática de todo o hardware. O plano de recuperação de desastres permite o gerenciamento de crises. Além disso, os fornecedores (Tecnoqualify e Mandic) possuem contratos de suporte em seu nível máximo.

4.4. Em caso de efetiva necessidade de utilização da estrutura de contingência, deverão ser encaminhadas para o local de contingência um Colaborador da área de Risco e *Middle Office* e dois gestores de carteiras.

Com os procedimentos descritos acima, a Garde pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório.

5. Procedimentos de contingência

5.1. Na impossibilidade de se utilizar o espaço físico da Garde, os colaboradores envolvidos no processo de contingência (um Colaborador da área de Risco e *Middle Office*, três gestores de carteiras e um Colaborador da área de Clientes, em conjunto com o CEO ou o CIO da Garde) deverão comparecer ao centro de negócios da Regus em São Paulo, a ser definido pelo Comitê Executivo da Garde.

5.2. A localização de todos os centros de negócios da Regus em São Paulo encontram-se no link: https://www.regus.com.br/office-space/brazil/sao-paulo

5.3. Se a impossibilidade de se utilizar o espaço físico da Garde ocorrer quando os Colaboradores estiverem no escritório, eles irão se dirigir ao centro de negócios da Regus portando os notebooks da empresa, que estão preparados com todas as ferramentas necessárias para o processo de contingência (Bloomberg, TT, Lote 45 e Microsoft Office). Já se a impossibilidade de se utilizar o espaço físico da Garde ocorrer quando os Colaboradores não estiverem no escritório, eles irão se dirigir ao escritório da Regus escolhido, onde utilizarão os equipamentos disponibilizados pela própria Regus.

5.4. Chegando no centro de negócios da Regus escolhido, o Colaborador da área de Risco e *Middle Office* será responsável por recuperar os arquivos no back-up diário realizado na nuvem.

5.5. Além do processo de recuperação de arquivos da nuvem, o Colaborador da área de Risco e *Middle Office* irá providenciar junto à Regus o acesso à Internet, que sem fio poderá ser acessada utilizando somente o código do cartão de acesso da Regus e que com fio será providenciado um usuário e senha de acesso na recepção do centro de negócios escolhido.

5.6. A Garde realiza, periodicamente, e no mínimo a cada 12 (doze) meses, testes para validação dos prazos, processos e recursos descritos nesta Política.