PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

VERSÃO REVISADA EM 30/09/2015

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS DA GARDE ASSET MANAGEMENT GESTÃO DE RECURSOS LTDA.

Área: *Compliance* e Risco

Esse Manual contém o Plano de Contingência, e tem como objetivo definir os procedimentos que deverão ser seguidos pela Garde Asset Management Gestão de Recursos Ltda. (”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 da Garde 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.

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 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 *back-up*

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, *on-line* 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 semanalmente, 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, conforme detalhado no item 6 deste documento.

3.2. A Garde contratou junto a Regus um serviço que dá direito a 5 diárias de escritório privativo. O cartão de acesso está em nome de Marcelo Giufrida e ele está autorizado para utilizar o escritório com 2 acompanhantes.

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.

3.4. A Garde conta com linhas de telefone digitais e linhas analógicas em caso de contingencia. Em caso de falhas nas linhas telefônicas, os colaboradores da Garde ainda possuem celulares que podem substituir a telefonia fixa.

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 *back-up* 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.

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 as pessoas responsáveis pelas funções de: boletagem e conferência das operações junto ao administrador, os principais gestores das carteiras além do CIO da gestora.

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

5. Lista de Informações

5.1. Deverá ser mantida no local de contingência uma lista com as informações de todos os integrantes da Garde, das corretoras com as quais se realizam negócios, dos clientes e dos prestadores de serviço contratados.

6. Procedimentos de contingência

6.1. Na impossibilidade de se utilizar o espaço físico da Garde, os colaboradores envolvidos no processo de contingência (nomes destacados na tabela abaixo) deverão comparecer ao *meeting point* do plano de contigência.

Nome	Celular
CARLOS LUIZ MARINO CALABRESI	9 8245 0837
CAROLINA ATHANAZIO DOS SANTOS	9 6552 0230
DANIEL WEEKS	9 8969-0110
DIEGO LOMBELLO SANTOS DONADIO	9 6197-0882
FELIPE AUGUSTO DA SILVA BASTOS	9 8555-9919
HENRIQUE POLI DE SOUZA	9 7083 5919
LEONARDO MIRANDA	9 8678 6666

MARCELO FIDÊNCIO GIUFRIDA	9 8266 5868
MARCIO ALEXANDRE GEORGETTI	9 8685 7303
NATHALIA GAMEIRO CATALDO	9 9975 4493
EDUARDO MAGOZO	9 9277 5790
RODRIGO BERLOFFE PAGNANI	9 8244 2826

6.2. O *meeting point* do plano de contingência da Garde é a residência de Marcelo Giufrida (CEO), localizada na Rua Dr. Fausto de Almeida Prado Penteado, 200, Jardim Silvia, CEP 05678-040 (cerca de 1,5 km do escritório da Garde).

6.3. Se a impossibilidade de se utilizar o espaço físico da Garde ocorrer quando os colaboradores estiverem no escritório, eles irão se dirigir ao *meeting point* 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 *meeting point* portando seus notebooks pessoais, que estão preparados com todas as ferramentas necessárias para o processo de contingência (Bloomberg, TT, Lote 45 e Microsoft Office).

6.4. No *meeting point*, o Marcelo Giufrida (CEO), e na sua ausência o diretor de Compliance e Risco, deverá contatar a Regus, efetuar a reserva do centro de negócio e indicar os colaboradores que irão para a Regus. É importante avisar que serão utilizadas 3 estações no ato da reserva.

Centro de Negócios	Endereço	Telefone
São Paulo, Top Center Paulista	Avenida Paulista, 854, 10º andar - Bela Vista, São Paulo, SP – CEP 70712-900	55 (11) 2186-0200
São Paulo, Paulista Financial District	Avenida Paulista, 1079, Torre João Salém, 7º e 8º andar – Bela Vista, São Paulo, SP – CEP 01310-200	55 (11) 2787-6200
São Paulo, Paulista Haddock Lobo	Avenida Paulista, 2300, Andar Pilotis – Centro, São Paulo, SP – CEP 01310-300	55 (11) 2847-4500
São Paulo, Alameda Santos	Alameda Santos, 200, Andares Térreo, Mezanino, 1º, 2º, 5º e 6º – Bela Vista, São Paulo, SP – CEP 01418-000	55 (11) 3587-1200
São Paulo, Parque Cultural Paulista	Avenida Paulista, 37, 4º andar – Bela Vista, São Paulo, SP – CEP 01311-902	55 (11) 2246-2700
São Paulo, Dacon	Avenida Cidade Jardim, 400, 7º e 20º andar – Cidade Jardim, São Paulo, SP – CEP 01454-000	55 (11) 3818-8999
São Paulo, Seculum Faria Lima	Avenida Brigadeiro Faria Lima, 3144, 3º andar – Jardim Paulistano, São Paulo, SP – CEP 01451-001	55 (11) 3568-2503
São Paulo, New Century	Rua Leopoldo Couto de Magalhães Júnior, 758, 11º andar – Itaim Bibi, São Paulo, SP – CEP 04542-000	55 (11) 2505-9101
São Paulo, Faria Lima	Avenida Brigadeiro Faria Lima, 3729, 4º e 5º andar – Itaim Bibi, São Paulo, SP – CEP 04538-905	55 (11) 3443-6200
São Paulo, Edifício Eldorado	Avenida das Nações Unidas, 8501, 17º andar – Pinheiros, Pinheiros, São Paulo, SP – CEP 05425-070	55 (11) 3434-6400
São Paulo, Continental Square Vila Olímpia	Rua Olimpíadas, 205, 4º andar – Vila Olímpia, São Paulo, SP – CEP 04551-000	55 (11) 3728-9200
São Paulo, Millennium Vila Olímpia	Avenida Chedid Jafet, 222, Torre D, 5º andar – Vila Olímpia, São Paulo, SP – CEP 04551-065	55 (11) 2655-1704
São Paulo, E-Tower Funchal	Rua Funchal, 418, 34º e 35º andar – Vila Olímpia, São Paulo, SP – CEP 04551-060	55 (11) 3521-7000
São Paulo, Shopping Cidade Jardim	Avenida Magalhães Castro, 4800, Park Tower, 14º andar – Cidade Jardim, São Paulo, SP – CEP 05502-001	55 (11) 3199-0100
São Paulo, Plaza Centenário	Avenida das Nações Unidas, 12995, 10º andar – Brooklin Novo, São Paulo, SP – CEP 04578-000	55 (11) 5503-6600
São Paulo, World Trade Centre	Avenida das Nações Unidas, 12551, 9º e 17º andar – Brooklin Novo, São Paulo, SP – CEP 04578-000	55 (11) 3443-7400
São Paulo, Market Place I	Avenida Doutor Chucri Zaidan, 920, 9º andar – Morumbi, São Paulo, SP – CEP 04583-904	55 (11) 3048-4000
São Paulo, Morumbi Office Tower	Avenida Roque Petroni Júnior, 999, 13º andar – Morumbi, São Paulo, SP – CEP 04707-910	55 (11) 5185 2800
São Paulo, Market Place II	Avenida Doutor Chucri Zaidan, 940, 16º andar – Morumbi, São Paulo, SP – CEP 04583-906	55 (11) 5095-3400
São Paulo, Rochavera - Morumbi	Avenida das Nações Unidas, 14171, 15º andar – Morumbi, São Paulo, SP – CEP 04794-000	55 (11) 3568 2000
São Paulo, Alexandre Dumas	Rua Alexandre Dumas, 1711, 5º andar – Chácara Santo Antônio, São Paulo, SP – CEP 04717-004	55 (11) 2599-8200

6.5. Chegando no centro de negócios da Regus escolhido, o diretor de Compliance e Risco, e na sua ausência o colaborador Felipe Bastos, será responsável por recuperar os arquivos no back-up diário realizado na nuvem. Segue lista dos arquivos que necessitam de recuperação:

Nome do arquivo	Localização	Área Responsável
Risk Report.xlsm	P:\RISKIT\Production	Risco&Middle
BTG Booking Generator.xlsm	P:\RISKIT\Production	Risco&Middle
Data Contribution.xlsm	P:\RISKIT\Production	Risco&Middle
TradesHistory.xlsm	P:\RISKIT\Production	Risco&Middle
BrokerageHistoryDARTAGNAN.xlsm	P:\RISKIT\Production	Risco&Middle
Limbo.xll	P:\PUBLIC\Library\x32	Risco&Middle
Regus.xlsx	P:\RISKIT\Compliance\Manuais	Risco&Middle

6.6. Além do processo de recuperação de arquivos da nuvem, o diretor de Compliance e Risco, e na sua ausência o colaborador Felipe Bastos, irá providenciar junto a 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.