M SQUARE Brasil

# PLANO DE CONTINGÊNCIA

**M SQUARE BRASIL INVESTIMENTOS LTDA.**

**Abril de 2018**

# 1. Introdução

## 1.1. Objetivo

A M Square Brasil Investimentos Ltda. ("**Empresa**" ou "**M Square Brasil**") elaborou este plano de contingência e recuperação de desastre (o "**Plano de Contingência**") com o objetivo de estabelecer os procedimentos adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas que causem impacto nas rotinas operacionais da empresa como um todo ("**Eventos de Contingência ou Desastre**") com vistas a assegurar à M Square Brasil e seus colaboradores a plena continuidade operacional das atividades da empresa, a todo tempo e sob qualquer circunstância.

São exemplos de Eventos de Contingência ou Desastre: suspensão total ou interrupção temporária na prestação de serviços por provedores de energia, acesso à internet, serviços de telefonia, etc., catástrofes naturais que impeçam o acesso ao prédio, interdição do prédio onde funciona a sede da M Square Brasil por qualquer motivo, inclusive em cenários de greves, pane nos sistemas e softwares utilizados pelos Colaboradores da Empresa, perda de arquivos por qualquer motivo, dentre outros.

Dentre as funcionalidades críticas à M Square Brasil a que este Plano de Contingência se propõe a cobrir incluem-se (i) a contínua execução de trades (com a respectiva manutenção das regras de *compliance* aplicáveis), (ii) o desempenho das rotinas operacionais, (iii) a possibilidade de recebimento e troca regular de e-mails (sejam internos ou com contrapartes externas) e atendimento telefônico via PABX além de (iv) acesso/uso ininterrupto aos sistemas, funcionalidades e arquivos utilizados pela Empresa, conforme descritos no item 1.2 abaixo ("**Sistemas Cobertos**"), mesmo em caso de total impossibilidade de acesso ao escritório físico da Empresa.

## 1.2. Funcionalidades e Sistemas Cobertos

São funcionalidades e sistemas cobertos para fins deste Plano de Contingência:

(i) E-mails & Intranet;

(ii) Sistema de controladoria, *Drive Senior Solution*;

(iii) Sistema de *trade* e *compliance,* Order Management System - Charles River (CRD);

(iv) Sistema de carteiras – Igenesis*;* e

(v) *Bloomberg*.

## 2. Medidas Preventivas

A M Square Brasil adota as seguintes medidas preventivas visando a mitigação de eventuais riscos de ocorrências de Eventos de Contingência ou Desastre:

**A. Rota de fuga, sinalização de emergência e simulações de incêndio:** a sinalização das rotas de fuga e colocação da sinalização de emergência é feita em locais estratégicos do escritório da Empresa e facilmente identificáveis. Os colaboradores são ainda, instruídos à se portarem com um padrão de conduta adequado em caso de incidentes com fogo. Neste caso, os colaboradores são obrigados a participar das simulações periódicas de incêndio realizadas pelo condomínio de modo a se familiarizarem com os procedimentos mínimos exigidos para o caso de uma ocorrência que demande a evacuação do prédio.

**B. Identificação de visitantes / Circulação de terceiros:** com vistas a assegurar um nível de segurança mínimo nas suas premissas, os visitantes são identificados pelo condomínio, e somente permitidos a subir ao escritório da M Square Brasil mediante prévia aprovação de um dos colaboradores. Neste mesmo sentido, os visitantes e prestadores de serviços são instruídos a observar o procedimento padrão para circulação dentro do escritório, não sendo permitida sua entrada no salão principal exceto se acompanhado de um colaborador. Ademais, a entrada de colaboradores no escritório é controlada por sistema biométrico implantando na única entrada disponível em seu escritório, evitando-se, assim, o acesso por terceiros que eventualmente tomem posse de crachás de identificação pessoal dos colaboradores (os quais tão somente permitem a entrada no edifício, mas não garantem efetivo acesso ao escritório da Empresa).

**C. Monitoramento do Ambiente Corporativo:** o monitoramento do ambiente corporativo se dá através da instalação de câmeras em locais estratégicos do escritório, permitindo a identificação de quem circula nas suas áreas comuns a todo o tempo, com a respectiva retenção das gravações.

**D. Avaliação Periódica dos Circuitos Elétricos e Instalações Hidráulicas:** a Empresa, através de prestadores de serviços terceirizados, realiza anualmente a reavaliação dos circuitos elétricos e do sistema hidráulico de seu escritório com vistas a mitigar riscos de curto-circuito e rompimento e/ou defeito das instalações hidráulicas (registros, válvulas e pontos de infiltração).

**E. Telefones de Colaboradores:** a Empresa disponibiliza aos seus colaboradores - em sua intranet - o acesso à lista de telefones celulares pessoais de cada um dos demais colaboradores, inclusive para os casos de emergência, facilitando assim a comunicação em cenários de estresse ou emergenciais.

## 3. Infraestrutura Tecnológica

A M Square Brasil é detentora de uma infraestrutura tecnológica robusta. A Empresa opera com 1 *datacenter* próprio onde ficam localizados seus servidores físicos e virtuais e 3 *datacenters* externos, sendo (i) 1 responsável pelos sistemas de produção, (ii) 1 localizado em continente diverso do primeiro para back-up dos sistemas de produção e (iii) um terceiro, localizado em Cotia, para telefonia, desktops virtuais e back-up de *File Server*. Todos os sistemas de produção e arquivos rodam nos servidores e todos eles têm redundância interna completa (discos e fontes de energia).

*Sistemas:* Os servidores responsáveis pelos sistemas de produção (Order Management System - CRD, Accounting System – *Drive Senior Solution*, etc) e bancos de dados da Empresa estão localizados em datacenter externo (*Private Cloud*), com contrato que inclui 99,99% de uptime e geo-redundância – isto é, os sistemas são espelhados, online, em outro datacenter do mesmo fornecedor, localizado em outro continente. A M Square Brasil se conecta até a Private Cloud através de duas VPNs criptografadas, cada uma por um link de internet diferente, para garantir que tenhamos o mais próximo de 100% de prontidão dos sistemas e de acesso a eles.

*Arquivos:* Os servidores responsáveis pelo sistema de arquivos (*File Server*) da M Square Brasil estão localizados em datacenter próprio localizado no escritório da M Square Brasil – em um ambiente com servidores, *storage* e rede totalmente redundantes (CPD) – e todos os dados desse sistema de arquivos são sincronizados, online, a duas *Private Cloud,* uma da Microsoft em São Paulo e outra da Level3 em Cotia. Ou seja, assim que um arquivo é atualizado localmente, ele é replicado para dois datacenters externos (São Paulo e Cotia). Isso permite à Empresa recuperar arquivos sem qualquer interferência com, ou prejuízo ao, acesso destes mesmos arquivos no dia a dia. Além disso, diariamente é feito um back-up dos arquivos para retenção histórica de 1 ano (*IBackup*).

*E-mail:* O sistema de e-mail também está localizado fora do escritório (Microsoft Office 365), com retenção/armazenamento automático de todos os e-mails por 5 anos. Sendo assim, em caso de um Evento de Contingência ou Desastre, todo o histórico de e-mails estará disponível via *webmail*, o qual conta com mecanismos de Two Factor Authentication, e o fluxo de entrada e saída de e-mails não será afetado.

*Acesso à rede:* Todas as permissões de rede/login/senha são sincronizadas online com o ambiente de *Private Cloud* tendo em vista a existência de um *domain controller* da rede. Ou seja, uma alteração de senha no ambiente de produção é replicada no ambiente de *Private Cloud* em questão de segundos, viabilizando desta forma, o acesso remoto à rede com o mesmo login e senha de acesso utilizados no escritório físico. O acesso remoto aos sistemas e arquivos por parte dos funcionários é feito por uma VPN com Two Factor Authentication, para evitar que um vazamento de senha possibilite que alguém externo à empresa consiga acessar os sistemas e arquivos.

*PABX:* Nossa telefonia (PABX e troncos) está em datacenter físico externo (localizado em Cotia), com total redundância elétrica, de ar condicionado e de conectividade. Todos os ramais se conectam a este PABX por meio de uma VPN IP redundante. Em caso de contingência, um script pré-programado será ativado pelo Gerente de TI da M Square Brasil acionando o encaminhamento das chamadas feitas aos ramais originais de cada um para o seu telefone celular pessoal. Assim há garantia de acesso telefônico total e irrestrito em situações de *Disaster Recovery*. Adicionalmente, vale ressaltar que todas as ligações são gravadas e as mesmas ficam retidas por 5 anos.

*Escritório:* O escritório da M Square Brasil possui redundância no acesso à internet (4 links), backup de eletricidade (2 nobreaks com 3 horas de autonomia e 4 geradores no prédio, que entram em serviço em média 19 segundos após uma falta de luz) e redundância de firewall. Em adição, há PCs de backup disponíveis em caso de falha dos equipamentos existentes. O plano de contingência foi estruturado de forma a garantir a manutenção do maior tempo de atividade possível ao nosso escritório.

*Disaster Recovery*: A estrutura externa de *Disaster Recovery* (ver abaixo "Estrutura e Plano de *Disaster Recovery*") é sincronizada automaticamente e pode ser acessada em Eventos de Contingência ou Desastre, observados os critérios e procedimentos abaixo definidos.

Sumário da Infraestrutura:

| | |
|---|---|
| **Sistemas e Bancos de dados** | Localizados em servidores virtuais localizados em datacenter da Microsoft em São Paulo, com contingência em geo-redundância em outro continente. |
| **Arquivos** | Localizados no escritório da Empresa situado na Avenida Brigadeiro Faria Lima, com cópia online para um servidor localizado no datacenter da Microsoft em São Paulo e outro no datacenter da Level3 em Cotia, além de back-up histórico no *IBackup*. |
| **E-mails** | Armazenados e fluem através de uma solução em nuvem da Microsoft (Office365), com retenção dos últimos 5 anos. |
| **PABX/ Telefonia** | Disponível no datacenter da Level3 localizado em Cotia, sendo que há uma programação prévia para que uma vez ativado o sistema, este transfira todas as ligações feitas aos ramais da Empresa para os respectivos celulares pessoais dos colaboradores. |
| **Desktops Virtuais** | Disponíveis 7 Desktops Virtuais no datacenter da Level3 em Cotia, os quais encontram-se sempre atualizados e em total compatibilidade com os sistemas operacionais utilizados nas rotinas diárias da Empresa, permitindo a plena continuidade das funções críticas inerentes ao negócio no caso de um Evento de Contingência ou Desastre. Para acesso a tais Desktops Virtuais, é necessário tão somente que o colaborador possua um computador (Windows ou Mac) com acesso à Internet. |

## 4. Estrutura e Plano de *Disaster Recovery*

A M Square Brasil possui uma estratégia para cenários de desastre composta por (i) back-ups de seus sistemas e (ii) estrutura de acesso remoto aos seus desktops, com sincronismo diário e completamente disponíveis para uso tanto em caso de um desastre físico envolvendo seu escritório quanto em caso de contingencia envolvendo o ambiente de *Private Cloud*.

(i) Back-up de Sistemas: com relação aos sistemas, todos os sistemas de produção da Empresa estão localizados em um datacenter externo da Microsoft em São Paulo, com back-up online para outro datacenter do mesmo fornecedor em outro continente (geo-redundância). Assim, em caso de um desastre que atinja fisicamente o datacenter principal, os colaboradores poderão imediatamente acessar os sistemas de produção no datacenter de back-up. Em caso de um desastre que impossibilite o acesso a ambos datacenters da Microsoft (ou seja, um desastre atingindo ambos datacenters deste fornecedor a despeito de situados em continentes distintos) a Empresa possui ainda back-up dos servidores virtuais e banco de dados em datacenter de outro fornecedor (*IBackup*), que nos permitiria recriar todo o ambiente de produção em algum *peer* da Microsoft usando os back-up disponíveis na *IBackup*.

(ii) Acesso remoto a desktops: com relação ao acesso remoto por colaboradores da M Square Brasil a seus desktops, a M Square Brasil conta com um contrato com um datacenter externo em Cotia com telefonia, back-up de File Server e 7 desktops virtuais para cenários de contingência. Estes 7 desktops destinam-se a atender as 4 áreas críticas da Empresa, com funções que são time sensitive e não podem parar ("Desktops Virtuais"). Os Sistemas Cobertos ficam atualizados nestes 7 Desktops Virtuais, a todo o tempo, formando um ambiente de Disaster Recovery ("DR"). Sempre que instalado um novo sistema ou uma versão de sistema atualizada no ambiente de produção, o mesmo procedimento é replicado no ambiente de DR mantendo, desta forma, os desktops de uso diário e os Desktops Virtuais simultaneamente sincronizados. O acesso a estes desktops por parte dos funcionários é feito por uma VPN com Two Factor Authentication, para evitar que um vazamento de senha possibilite que alguém externo à empresa consiga acessar os sistemas e arquivos. Da mesma forma, o acesso a e-mails através do webmail, conta com a proteção do mecanismo de Two Factor Authentication. Todo o ambiente de Disaster Recovery é protegido por firewall operando em redundância, para garantir o máximo de disponibilidade.

O acesso ao ambiente de DR é feito através da utilização de mesmo usuário e senha da rede adotados no acesso ordinário de dentro da Empresa, apenas com o adicional de fechamento da VPN com Two Factor Authentication com o ambiente, similar ao que já é feito hoje para conexão remota ao escritório da Empresa.

## 5. Procedimentos

### 5.1. Procedimentos durante um Evento de Contingência ou Desastre

- **Falha de Sistemas:**

No caso de um Evento de Contingência ou Desastre que implique na descontinuidade na prestação de serviço atrelados aos sistemas operacionais considerados críticos – Sistemas Cobertos, e/ou em seus servidores e rede, o Gerente de TI atuará para reestabelecer o acesso aos referidos sistemas de forma emergencial, além de ativar imediatamente e disponibilizar na rede em modo redundante. Caso tal falha seja decorrente de um Evento de Contingência ou Desastre na qual fique inviabilizado o acesso ao escritório físico da M Square Brasil, os colaboradores devem se orientar para que o acesso seja feito remotamente e conforme guia de acesso remoto disponível na sede da Empresa.

- **Falha de Infraestrutura:**

**(a) Energia Elétrica**: caso haja falha no fornecimento de energia, a M Square Brasil conta com os seguintes recursos: (i) 2 sistemas de alimentação secundária de energia elétrica (nobreaks) com 3 horas de autonomia de bateria; e (ii) 4 geradores no prédio inicializados automaticamente que levam em média 19 segundos para ativação após a ocorrência de queda de energia e possuem autonomia de mais 36 horas até que seja necessário seu reabastecimento.

- ✓ Principais Ações e Responsáveis: Caso os back-ups de eletricidade elencados acima não funcionem ou sejam insuficientes, o Gerente de TI orientará os Key Users para que desloquem-se até suas casas e deem continuidade operacional aos trabalhos via acesso aos Desktops Virtuais localizados no datacenter externo de Cotia.

**(b) Comunicações:** a M Square Brasil conta com 4 links de acesso à internet (redundância) para a eventualidade de uma falha na prestação do serviço do provedor de internet e/ou no link de dados. Ademais, todos os ramais se conectam por meio de um PABX que é ligado por meio de uma VPN IP redundante, permitindo assim o fornecimento de link de voz ininterrupto.

- ✓ Principais Ações e Responsáveis: Caberá ao Gerente de TI a responsabilidade de ativação do script de encaminhamento de chamadas para que os colaboradores tenham acesso integral a ligações feitas aos seus ramais originais, em seus telefones celulares pessoais.

**(c) Controle Ambiental CPD:** o ambiente do CPD situado no escritório da M Square Brasil é monitorado regularmente para garantir o seu correto funcionamento e a manutenção de temperatura (aproximadamente 21° C) e umidade (aproximadamente 22%).

- ✓ Principais Ações e Responsáveis: O Gerente de TI é responsável por monitorar diariamente, inclusive via acesso remoto, as condições mínimas de funcionamento do CPD. Caso haja qualquer intercorrência no ambiente do CPD gerando falha nos mecanismos de controle e/ou alteração de tais condições, o Gerente de TI atuará para mitigação das falhas e reestabelecimento de suas funcionalidades, inclusive comunicará à Diretora de Gestão de Risco da M Square Brasil (nomeada nos termos do seu contrato social) caso verifique que um problema no CPD pode causar falhas acessórias sistêmicas. Neste sentido, o Gerente de TI e a Diretora de Gestão de Risco atuarão, conjuntamente, para desenvolver um plano imediato de ação. Dependendo do grau de complexidade da falha e por medida de segurança, caberá a Diretora de Gestão de Risco orientar os demais colaboradores a procederem à evacuação do escritório, e subsequente acesso remoto aos Desktops Virtuais. Caso isso

aconteça, o Gerente de TI solicitará à administradora do escritório que proceda à imediata comunicação dos fatos ao condomínio.

**(d) Desastres (Incêndio, inundação, assalto, etc):** Eventos de Contingência ou Desastre que impliquem na evacuação e/ou inacessibilidade do escritório físico onde está localizada a sede social da Empresa, impossibilitando o acesso aos sistemas de operação da empresa.

- ✓ Principais Ações e Responsáveis: Além dos procedimentos padrão de evacuação do edifício e atuação ativa dos brigadistas para salvaguardar a vida dos colaboradores da M Square Brasil, ficará a cargo do Gerente de TI e em sua ausência, da Diretora de Gestão de Risco da M Square Brasil, atuar para viabilizar a ativação do site de contingência, permitindo às 4 áreas críticas e aos colaboradores designados para seu acesso, nos termos acima, acesso seguro e integral à rede, aos Sistemas Cobertos, aos seus e-mails e demais recursos mínimos necessários para restabelecimento operacional, sem maiores rupturas.

  Para tanto, a orientação aos colaboradores é de procederem às suas residências ou a um local seguro em que possam, através de qualquer computador, acessar os computadores virtuais que ficam disponíveis no site de DR localizado em Cotia, seguindo os procedimentos descritos no item 4.2 abaixo.

- ✓ Tempo de Ação: Imediato - quanto antes for a atuação da Empresa e de seus colaboradores, menor será o prejuízo. O Gerente de TI da M Square Brasil ficará a inteira disposição dos Key-Users para viabilizar os acessos aos Sistemas Cobertos em Eventos de Contingência ou Desastre.

### 5.2. Acesso ao Ambiente DR

Como todos os Sistemas Cobertos encontram-se na nuvem, Eventos de Contingência ou Desastre e indisponibilidade de acesso ao escritório físico não causam um impacto direto à continuidade dos negócios. Para tanto, contamos com 7 Desktops Virtuais pré-configurados que permitem a continuidade imediata das funções mais críticas, conforme melhor detalhado abaixo.

Neste cenário, os colaboradores permanecem com acesso full aos e-mails (incluindo nos aparelhos celulares) e com as ligações para os ramais redirecionadas. Os bancos de dados, sistemas e arquivos estarão no exato estado imediatamente anterior ao Evento de Contingência ou Desastre, bastando o acesso os Desktops Virtuais. Os procedimentos para acesso aos Desktops Virtuais encontram-se detalhados abaixo:

- ➢ Acesso ao DR utilizando Windows 7 / Vista
- ➢ Acesso ao DR utilizando Mac

A Empresa disponibiliza o acesso ao ambiente DR para dois grupos segregados de colaboradores, quais sejam:

**(1) Key Users** – 4 Desktops Virtuais ficam disponíveis restritamente para atendimento às 4 áreas consideradas críticas para fins de continuidade do negócio em um Evento de Contingência ou Desastre, são elas: *Trading, Operations, Compliance* e Relações com Investidores.

Nesta linha, a Empresa designou os seguintes colaboradores, de cada uma dessas 4 áreas críticas, os quais ficam responsáveis pelo acesso aos Desktops Virtuais localizados no datacenter do DR e pelo manuseio e manutenção da continuidade dos negócios em um Evento de Contingência ou Desastre.

1. Trading: Bruno Rignel (backup Arieh Levin)
2. Operations: Rodrigo Canteli (backup Sidnei Almeida)
3. Compliance: Marta Kheirallah (backup Priscila Romanizio)
4. Relações com Investidores: Juliana Paolillo (backup: Flávia Shibata)

**(II) Demais Colaboradores**: Os demais Desktops Virtuais ficam disponíveis para a área de TI e subsidiariamente, aos demais colaboradores, os quais possuem acesso aos arquivos da rede bastando tão somente fechar a VPN e mapear o servidor de arquivos ("R:/").

A prioridade de atendimento é para os *Key Users*, seguida de restauração do ambiente de produção e posteriormente, atendimento e acesso aos demais usuários. Em caso de problemas no acesso durante um Evento de Contingência ou Desastre, os colaboradores são orientados a ligar ou contatar um dos contatos listados na lista de emergência disposta na intranet da Empresa.

### 5.3. Procedimentos após Evento de Contingência ou Desastre

Na ocorrência de um Evento de Contingência ou Desastre, será estabelecido um comitê de gerenciamento de crise ("**Comitê de Gerenciamento de Crise**"), composto essencialmente pelo Gerente de TI, Diretora de Gestão de Risco e um colaborador nomeado em conjunto por ambos, os quais ficarão responsáveis por:

(i) avaliar os impactos diretos e indiretos sofridos;

(ii) elaborar e implementar um plano de ação para recuperação dos serviços impactados, em especial com vistas a restabelecer as 4 funções críticas à Empresa, com a maior brevidade possível;

(iii) comunicar aos demais colaboradores acerca do referido plano de ação e se necessário, convoca-los para reunião presencial para esclarecimento de dúvidas e ponderações acerca das medidas que foram e serão adotadas em tal cenário; e

(iv) atuar para a reparação da estrutura afetada, incluindo, mas não se limitando, conforme o caso, ao reestabelecimento do ambiente, dos sistemas de rede e operacionais, bem como estabelecer metodologias de prevenção à ocorrência de novos eventos de contingência ou desastre com características similares (se e quando possível) mitigando, desta forma, o risco de recorrências.

O Comitê de Gerenciamento de Crise será instaurado e permanecerá atuante até que sanados todos problemas decorrentes do Evento de Contingência ou Desastre e restabelecidas, em sua integralidade, as funções e atividades da Empresa.

## 6. Registros, Treinamentos & Revisões Periódicas

### 6.1. Registros de Ocorrências

Caberá ao Comitê de Gerenciamento de Crise o registro em pauta de toda e qualquer incidência que implique na ativação dos procedimentos de contingência descritos neste plano. Constará de tal registro, no mínimo:

- Descrição dos fatos;
- Data e hora (quando aplicável) da ocorrência;
- Descrição das medidas adotadas;
- Data e hora (quando aplicável) do reestabelecimento das condições normais de trabalho;
- Informações adicionais (eventualidades, estragos e afins); e
- Assinaturas da Diretora de Gestão de Risco e do Gerente de TI.

As pautas de registro ficarão armazenadas com a Diretora de Gestão de Risco pelo prazo de cinco anos.

### 6.2. Treinamentos Periódicos

Todos os Colaboradores comparecerão a um treinamento anual sobre o presente Plano de Contingência (e quando necessário, a reuniões adicionais sobre o tema), que se dará conjuntamente com a reunião anual de treinamento de Compliance. Tal treinamento será elaborado e apresentado pelo Gerente de TI sob supervisão da Diretora de Gestão de Risco.

### 6.3. Revisões Periódicas

O presente Plano de Contingência será revisado anualmente pelo Gerente de TI ou, quando necessário, na ocorrência de alterações nos processos ou na estrutura adotados pela M Square Brasil (seja por otimização, adequações, ou introdução de novas tecnologias) e estará sujeito à validação pela Diretora de Gestão de Risco da M Square Brasil.

Todos os colaboradores receberão uma cópia do presente Plano de Contingência, além do treinamento anual mencionado acima, e poderão acessá-lo, em sua versão mais atual, a qualquer tempo, no website da Empresa.