Plano de Contingência e Continuidade dos Negócios

Índice:

B.1 –Plano de Contingência e Continuidade dos Negócios

B.1.1 – Introdução ao BCP

O objetivo do Plano de Contingência e Continuidade dos Negócios ("BCP") é possibilitar que a MOAT Capital de Recursos Ltda ("MOAT") continue com as suas operações e serviços essenciais mesmo nos cenários de crise.

O presente documento define os procedimentos que deverão ser seguidos pela MOAT, 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 MOAT 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 MOAT dentro do contexto de seu negócio.

B.1.1.1 – Cenários de Crise

A *Alternative Investment Managment Association* (AIMA) lista em seu documento "*Business Continuity Management for Hedge Fund Managers – version June 2012*" 24 possíveis cenários de crise:

1. Explosão em uma grande área;	2. Fogo;	3. Falta localizada de energia;
4. Explosão localizada;	5. Inundação;	6. Falha de circuito / terminal;
7. Explosão na vizinhança;	8. Pandemia;	9. Falha de hardware;
10. Bomba radiológica;	11. Clima extremo;	12. Virus / hackers;
13. Guerra ou insurreição civil;	14. Interrupção de transportes;	15. Roubo / sabotagem;
16. Alerta de segurança;	17. Acidentes (dentro ou fora do escritório);	18. Falha no sinal de telecom (internet e/ou voz);
19. Vazamento de gás;	20. Eletrocução;	21. Falha no hardware de telecom e
22. Terremoto;	23. Falta geral de energia (apagão);	24. Falha na rede de celular

Uma vez que ocorra algum incidente parecido com estes 24 cenários ou algo que chame a atenção do colaborador, o líder do BCP – que é o Compliance Officer ou na ausência deste o seu back-up – deverá ser imediatamente comunicado. (Ver B.1.4 – lista de contatos de emergência)

B.1.1.2 – Desdobramentos

A lista de cenários apresentadas em B.1.1.1 não tem a pretensão de ser definitiva. Além disto, cenários de crise são por definição imprevisíveis. No entanto os cenários acima geralmente levam a combinação de um ou mais dos desdobramentos abaixo:

1. **Perda de Acesso ao Prédio:** significa que todos os colaboradores e contratados da MOAT que estiverem no prédio no momento do incidente deverão evacuá-lo e quem estiver fora não poderá entrar.

2. **Perda de Pessoal:** afeta o *staff* e prestadores de serviços da MOAT. Inclui ferimentos, doenças, morte e incapacidade de chegar no escritório (ou potencialmente trabalhar de casa).

3. **Perda de Infraestrutura de TI: i**nclui falha parcial ou completa da rede de TI, incluindo hardware e softwares essenciais. O fator-chave é envolver os prestadores de serviços assim que possível para instaurar os sistemas de *back-up*.

4. **Perda de Infraestrutura de Telecom: i**nclui falha parcial ou completa da rede de telecomunicações, incluindo equipamentos, telefones fixos, celulares e a internet).

5. **Perda de Energia Elétrica:** Falta de energia devido a apagões ou interrupção da rede elétrica devido a chuvas e/ou quedas de árvores.

B.1.2 – Gestão da Crise, Recuperação e Retomada

Uma vez que o líder do BCP foi acionado devido a uma potencial crise, caso seja possível ele convocará (pessoalmente ou via *call-tree*) os colaboradores-chave da MOAT para formar o comitê de crise e avaliar conjuntamente a situação e próximos passos.

Na impossibilidade de decisão em conjunto – devido a situação onde a pressão é extrema – o líder do BCP poderá tomar decisões sozinho sobre os próximos passos para gerenciar a crise.

Existem gerlamente três etapas a serem percorridas após a ocorrência de um evento:

1. **Gestão da Crise;**
2. **Recuperação e**
3. **Retomada**

B.1.2.1 – Gestão da Crise

1. **Etapa Inicial:** engloba vários aspectos e decisões fundamentais a serem tomados imediatamente após o incidente:
   - 1.1. Avaliação dos impactos: o foco da reunião do time de crise deve ser em
     - 1.1.1. Entender o que aconteceu;
     - 1.1.2. Quais são as consequências imediatas e gravidade da situação;
     - 1.1.3. Como manter o staff a salvo e
     - 1.1.4. O que nós devemos fazer AGORA e decidir pela formalização ou não da CRISE (Em caso afirmativo os próximos passos são seguidos)
   - 1.2. Comunicação ao restante dos colaboradores
   - 1.3. Evacuação do prédio coordenada em conjunto com a administração predial;
   - 1.4. Acionar assistência médica imediata se necessário;
   - 1.5. Notificação dos serviços de emergência (bombeiros, polícia, SAMU) se necessário;
   - 1.6. Condução de chamada para ver os membros do staff e visitantes presentes;
   - 1.7. Retomada da reunião do comitê de crise;
   - 1.8. Re-alocação do staff:

1.8.1. Quem vai para casa e quem vai para o site de contingência;
1.8.2. Combinar como serão as próximas comunicações (telefone, Whatsapp)

1.9. Notificação de parceiros-chave estratégicos: prestadores de serviços de TI e Telecom (Tecnoqualify); e administrador do fundo (INTRAG).

Tomar cuidado para manter a consistência da comunicação ao informar terceiros. Apenas os colaboradores autorizados a falar em nome da empresa deverão fazer isto (ver lista de autorizados no Manual de Compliance).

1.10. Iniciar a redundância de TI (caso seja aplicável) em conjunto com a Tecnoqualify e

1.11. Re-direcionamento das linhas de telefone para os celulares (caso seja aplicável)

2. Recuperação de Desastre – TI

Após determinar a necessidade ou não de redundância de TI, o comitê de crise deverá atuar em conjunto com a Tecnoqualify para garantir que qualquer aplicativo e hardware críticos continuem a operar via redundância/back-up. Isto inclui:

- acesso ao servidor de e-mails;
- acesso aos principais servidores (aplicativos e arquivos)
- acesso remoto aos sistemas.

3. Telecom

Caso a redundância de telecom seja necessária, o provedor deve ser instruído a desviar linhas de dados/e-mail.

4. Comunicação Externa

A gestão de relacionamentos externos durante uma interrupção das atividades normais é critica para o curto e médio prazo da MOAT. No curto prazo os prestadores de serviços críticos devem ser avisados para que eles adaptem os seus processos para a nova circunstância. No longo prazo, prover uma comunicação clara, pontual e consistente a clientes, distribuidores e contrapartes fortalece a confiança na organização

O comitê de Crise produzirá um script padrão para comunicar interna e externamente (demais prestadores de serviços, clientes, dentre outros). É muito importante que a comunicação externa seja consistente uma vez que confusão poderá resultar em perda de confiança.

Caso algum colabrador (que não esteja autorizado a falar em nome da empres) seja questionado por terceiros, o colaborador deverá direcionar o terceiro para alguém que esteja autorizado.

B.1.2.2 – Recuperação

A fase de recuperação começa após a crise inicial ter sido contornada, ou seja, o staff já foi recolocado, a redundância de TI acionada e terceiros-chave notificados.

A fase de recuperação é composta das sub-fases a seguir:

1. **Comunicação Interna**: call diário de acompanhamento do comitê de Crise e outro call com os demais membros da MOAT. Ambos devem ser minutados pelo líder do BCP e conter os action points (atividade/dono/deadline);
2. **Ações Iniciais de Recuperação**:
   2.1. Comitê de Riscos e Compliance: deverá se reunir assim que possível para avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações;

2.2. Comitê de Investimentos: o CIO e o CRO devem juntamente convocar uma reunião para verificar se todas as informações necessárias ao portfólio estão seguras. Dados faltando ou corrompidos devem ser comunicados ao comitê de crise. O time de Gestão e o CRO devem decidir se decisões de investimento são requeridas embora o trading discricionário deva ser minimizado de acordo com as novas condições operacionais da empresa.
2.3. Operações (Middle Office): este time deverá continuar a manter informados o administrador do fundo, prime brokers e outros contrapartes operacionais-chave.

3. **Cobertura de funções críticas**: todas as áreas funcionais deverão ter previamente identificado as suas atividades críticas e o seu pessoal-chave necessário. Estas funções deverão ser conduzidas com qualquer problema sendo escalado ao comite de crise.
4. **Data Management**:
   4.1. Migração dos trabalhos conduzidos externamente durante a crise para os sistemas essenciais (ou back-up)
   4.2. Back-up de dados em ambiente de Recuperação
5. **Comunicação Externa:** stakeholders-chave externos devem ser atualizados regularmente.
6. **Cenários de Retificação/ Contingência**
   6.1. Acesso ao prédio: no caso do prédio ter sido evacuado, ou o acesso a ele estar negado. é provavel que documentos ou hardware importantes estejam dentro
   6.2. Buscar acomodação alternativa: no caso do prédio ter sido gravemente danificado ou destruído e a re-ocupação não seja possível a médio prazo (ou nunca mais).

B.1.2.3 – Retomada

A terceira fase é a transição entre estar trabalhando em "modo recuperação" para voltar ao modo normal (*business as usual*). Deve ser tratada – e gerida – como um projeto incluindo atividades, check-lists e gráficos de Gantt com uma clara linha do tempo.

Os temas cobertos por esta fase são dependentes do evento ocorrido mas podem incluir:

- Como a organização volta a estar em *compliance* novamente ?
- Algum sistema necessita ser reconstruído ?
- A empresa irá mudar para um novo escritório ?

B.1.3 – Redundâncias e Contingências

Em caso de eventos de crise, a MOAT possui contingências e redundâncias de forma a permitir a continuação de suas atividades mesmo em condições adversas.

B.1.3.1 – Redundância de TI / Back-up de Arquivos

Backup Server: O servidor possui software de backup (backup Windows 2016 e Ibackup), responsável pela realização de backup predefinido pela política da MOAT.

A MOAT disponibiliza em seus servidores o serviço de backup e restore de arquivos, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

Os Backups são feitos através da ferramenta de backup do Windows 2016 Server e Arcserv Cloud e são salvos em disco externo e cloud com agenda diária das pastas de dados de toda a empresa, devendo ser usado em casos em que não é mais possível a recuperação do arquivo danificado ou perdido.

O serviço de e-mail da MOAT é garantido por parceiro *Microsoft* que provém suporte 24/7, serviço de anti spam, anti vírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A MOAT possibilita o acesso remoto de todas as mensagens pelos colaboradores.
O serviço de e-mail da MOAT é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, Antivirus (software) é ativado em cada computador individual na rede de escritório.

B.1.3.2 – Redundância de Infraestrutura (Telecom, Internet e Energia)

Telefonia
A MOAT conta com serviço VOIP de Telefone sendo 14 linhas VOIP e 2 linhas analogicas. Em caso de falhas nas linhas telefônicas VOIP, os colaboradores da MOAT ainda possuem celulares que podem substituir a telefonia fixa.

Internet
O acesso à internet é disponibilizado por 3 links de velocidade de 30 mbps no link dedicado (Algar) e 2 links ADSL de 100 mbps link VIVO e NET

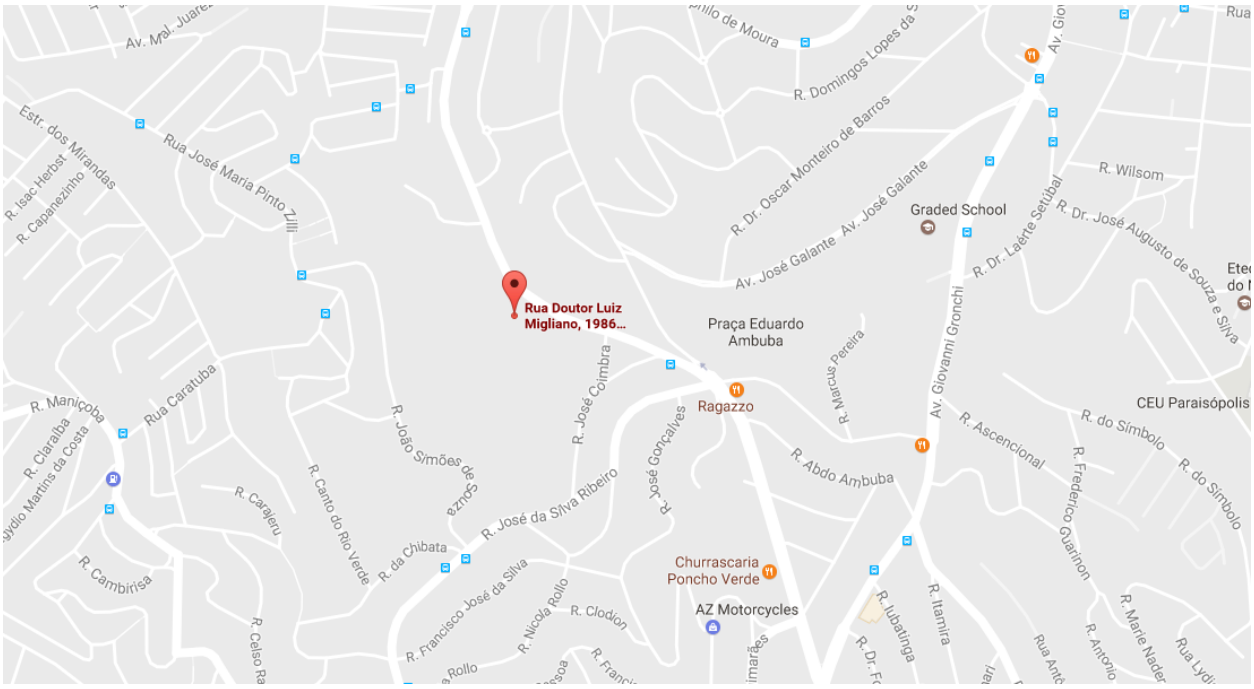
Energia
Em caso de falha de fornecimento de energia, a MOAT possui nobreak para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de 2 estações de trabalho (desktops) para a efetiva continuidade dos negócios durante 6 horas. Após 3 horas caso não retorne a energia a equipe será deslocada para o site backup.

Teste de no-break realizado duas vezes por ano.

B.1.3.3 – Site de Contingência e Home-Office

O escritório da MOAT encontra-se na Av. Brigadeiro Faria Lima, 3015, 11 andar, Itaim. Em caso da perda de acesso a este edifício, os colaboradores poderão: (a) acessar o site de contingência ou (b) trabalhar de casa com acesso VPN (*home-office*).

O site de contingência é o escritório do prestador de serviços (Tecnoqualify) cujo endereço é:
Rua Dr. Luiz Migliano, 1986 - 10 andar – São Paulo - SP
São Paulo/SP – CEP: 05711-001



O site de contingência fica a cerca de 8 km da sede da MOAT e pode ser acessado através de grandes vias como a Marginal Pinheiros. Em tráfego normal, pode-se chegar em 40 minutos.

No site de contingência, a MOAT possui posições de contingência. Estes postos possuem a "software-padrão" dos aplicativos essenciais da MOAT para operação e sistemas.

A MOAT também conta com acesso remoto via VPN à sua rede de dados e alguns aplicativos para os colaboradores que optarem pelo *home-office*. Tal acesso encontra-se disponível a todos os colaboradores autorizados pelo Compliance Officer.

Os aplicativos essenciais da MOAT estão listados abaixo bem como os a disponibilidade de acesso no site de contingência e no home-office via VPN:

Aplicativo	Site de Contingência	Home-Office (acesso VPN)
Email Outlook	✓	✓
Sophos Antivirus	✓	✓
Base de Dados	✓	✓
Feeders de cotações	✓ O software está instalado nos desktops de contingência.	✓

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

B.1.4 – Lista de Contatos de Emergência

A MOAT desenvolveu uma lista de Contatos de Emergência que inclui os nomes, telefones, endereços de e-mail dentre outras informações críticas para o negócio. Esta lista inclui colaboradores-chave, distribuidores de fundos, clientes de carteiras administradas, contrapartes prestadores de serviços essenciais dentre outros contatos. Esta lista será revista e atualizada ao menos anualmente.

nome	empresa / função	telefone	celular	e-mail
Colaboradores				
RODRIGO CARRERA	MOAT (líder BCP)	11 3181-8727	11 98301-7575	rodrigo.carrera@moat.com.br
DOUGLAS WANG	MOAT (back-up BCP)	11 3181-8726	11 97463-8477	Douglas.wang@moat.com.br
Prestadores de Serviços / Contrapartes				
Antonio Rampazzo	Itau Corretora / Clearing	11 3073-3831		middlebovespa@itaubba.com
Clayton Campos	MOAT (Suporte TI)		11 98244 7988	clayton@tecnoqualify.com.br
Luis Sposito	Safra corretora	11 35759611		Luis.sposito@safra.com.br
Waldir	CS Corretora	11 3701-6285		
LUCIANO HADDAD	Itau Coroporate	11 3072-6182		Luciano.haddad@itau-unibanco.com.br
WALTER MORAIS	CAPITAL MARKETS	3842-9977		Walter.morais@cmcapital.com.br
PEDRO JUCA	XP CORRETORA			

B.1.5 – Revisão Anual, Atualização, Treinamento e Testes

B.1.5.1 – Revisão Anual e Atualização

O BCP deverá ser revisado anualmente e atualizado sempre que for necessário. Cada revisão deverá ser aprovada pelo Diretor de Compliance (*Compliance Officer*) e as cópias do plano revisado deverão ser distribuídas a todos os colaboradores-chave da MOAT. O BCP também será revisto caso aconteça alguma das situações abaixo:

- Mudanças materiais – organizacionais – no negócio da MOAT
- Mudanças de pessoal
- Mudança de endereço do escritório da MOAT ou abertura de um escritório adicional
- Introdução de novos processos ou alteração dos existentes
- Upgrade ou alterações na infraestrutura de IT e/ou sistemas
- Mudança de prestador de serviço relevante
- Alterações de informações de contatos (p.e., números de telefone)

B.1.5.2 – Treinamento e Testes

O treinamento do staff em relação ao BCP ocorre fundamentalmente com os procedimentos de teste. O único treinamento adicional requerido é uma apresentação do BCP em uma única sessão a ser feita no momento de sua publicação. No caso de um novo colaborador a equipe de compliance fará para ele(a) a última apresentação feita.

O BCP deve ser testado para garantir que o mesmo funcione em caso de necessidade. Diferentes cenários de eventos devem ser testados ao menos anualmente. Os principais testes são elencados a seguir

Call Tree
O líder do BCP começará o teste fora do horário comercial - sem aviso prévio - transmitindo uma palavra código para os participantes do *call tree*. No dia seguinte, todos os participantes deverão reportar a palavra-código transmitida. Este teste avalia a viabilidade do call tree e se os números de telefone foram corretamente registrados.

Conectividade Remota e Site de Contingência
Todo o staff que possuir acesso remoto via VPN (*Virtual Private Network*) deverá se logar na rede da MOAT a partir de casa e checar se todos os sitemas essenciais e acessos funcionam perfeitamente. Um colaborador da equipe de Gestão e um de Middle-Office/Riscos deverão efetuar os testes através dos notebooks localizados no site de contingência.

Redundância de TI
Durante um final de semana, o provedor de serviços de TI (Technoqualify) irá acionar o sistema back-up e todo o staff tentará logar no sistema testando as aplicações essenciais. Posteriormente – no mesmo final de semana – o sistema principal/primário será acionado novamente, para testar o processo de retomada.

Redundância de Telecom
Durante um final de semana, todas as linhas fixas de telefone serão testadas e então estes serão testados através de um call tree para telefones fixos. Posteriormente – no mesmo final de semana – as linhas fixas serão reativadas e testadas como parte do processo de retomada.

Redundância de Energia (No-Breaks)

Durante um final de semana, a energia será desligada e o no-break interno entrará em funcionamento. Os acessos e os sistemas essenciais deverão ser checados. Posteriormente – no mesmo final de semana – a energia será reativada e os acessos novamente testados como parte do processo de retomada.

Teste Completo

Durante um dia útil a ser combinado, a estrutura primária de TI será desligada pela manhã e o sistema de back-up entrará em vigor; os telefones fixos serão desviados para os celulares e nenhum staff (incluindo prestadores de serviços de TI) serão permitidos no escritório. Todo o staff trabalhará de casa [OU SITE DE CONTINGENCIA] priorizando as atividades essenciais da análise de impacto no negócio. O time de Crise gerenciará ativamente o teste organizando conference calls conforme planejado. No final do dia, os sistemas primários de IT e a telefonia fixa serão restaurados. No dia seguinte, todo o staff deverá checar se os arquivos foram propriamente salvos nos servidores primários. Este teste também verificará se as atividades chaves foram corretamente identificadas dentre outros.

B.1.6 – Obrigações dos Colaboradores da MOAT em relação ao BCP

O BCP somente funcionará com o devido engajamento de todos os colaboradores-chave da MOAT. Os colaboradores da MOAT deverão obrigatoriamente:

- Manter uma versão impressa atualizada do BCP em casa e no escritório;
- Ter programado no seu celular os números dos telefones do líder do BCP, seus colegas imediatos e do seu supervisor;
- Ter o número do *conference call* do BCP programado no celular e a senha de acesso ao *conference room* facilmente acessível;
- Testar periodicamente o acesso aos sistemas primários e back-ups via VPN (aqueles que tiverem acesso e estrutura computador/internet para o *home-office*);
- Manter uma política de mesa limpa (*clean desk policy*): no caso de um roubo ou incêndio, os papéis guardados ficam muito mais seguros do que aqueles deixados soltos;
- Os colaboradores que gerenciem ou tenham relacionamentos com prestadores de serviços também devem manter programados os contatos destes no celular.

B.1.7 – Atividades e Responsabilidades relacionadas ao BCP

Os responsáveis pelas atividades relacionadas ao BCP da MOAT são listados a seguir:

Manutenção e Atualização do Plano	RODRIGO CARRERA	
Aprovação, Revisões e conduzir revisão anual	RODRIGO CARRERA	
Treinamento e Teste anual do plano	RODRIGO CARRERA	
Implementação do plano em caso de necessidade	Emergency Response Team	
Revisão Trimestral da lista de Contatos de Emergência	RODRIGO CARRERA	
Manutenção e distribuição da lista de Contatos de Emergência	RODRIGO CARRERA	
Prover informações do plano para investidores e CVM	RODRIGO CARRERA	
Revisar BCPs de prestadores de serviços essenciais • Na contratação dos serviços • Na revisão anual do BCP da MOAT	RODRIGO CARRERA	

B.1.8 – Controle do Documento

O presente documento deve ser aprovado e revisado no mínimo anualmente pelo Comitê de Riscos e Compliance (CRC) da MOAT:

Versão	Autor	Data	Comentário
1.3	RODRIGO CARRERA	Out/2018	Atualização