PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Última atualização: 15/09/2017

Produzido pelo Comitê de Contingência.

ÍNDICE

I. INTRODUÇÃO

O Plano de Contingência e de Continuidade de Negócios pode ser entendido como o conjunto de medidas preventivas e procedimentos de recuperação, no caso de qualquer interrupção de negócios. Estas medidas, vão muito além da simples adoção de um plano de seguro e, devem garantir a capacidade do grupo MODAL em operar em bases contínuas. Para tanto, esse plano deve assegurar que todos os processos críticos têm seus riscos identificados, avaliados, monitorados e controlados.

O presente plano envolve basicamente quatro grupos, a saber:

CONTINGÊNCIAS DE INFRAESTRUTURAS FÍSICAS: assim compreendidas as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos e etc. que impeçam o acesso e/ou utilização das instalações do grupo MODAL, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não e ainda falhas no fornecimento de energia elétrica.

CONTINGÊNCIAS DE PESSOAL: aquelas onde os associados-chave não estão presentes por motivos de greves, doença, licenças e etc.

CONTINGÊNCIAS DE INFRAESTRUTURAS TECNOLÓGICAS: compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como *hardware*, *software*, *telecom*, rede e segurança.

CONTINGÊNCIA DE SERVIÇOS EXTERNOS: compreendidas as situações de não prestação de serviço contratado considerado crítico / essencial aos processos do MODAL.
O presente Plano de Contingência e de Continuidade de Negócios é de uso do MODAL, sendo sua manutenção e atualização de responsabilidade do COMITÊ de CONTINGÊNCIA, a fim de mantê-lo consistente com as operações e estratégias correntes. Além disso, este plano deve ser testado periodicamente para assegurar que o MODAL possa executá-lo num evento de descontinuidade dos negócios.

EQUIPE

O Plano de Contingência e de Continuidade de Negócios deve ser de pleno conhecimento do COMITÊ de CONTINGÊNCIA, cuja responsabilidade é gerenciar todo o *staff* MODAL em quaisquer das situações de contingência previstas nesse manual. Esse grupo é soberano em qualquer decisão em situações de contingência e é formado pelo responsável da área de TI Infra, pelo responsável da área de TI Desenvolvimento, pelo diretor responsável por Risco Operacional e pelo diretor da Administração e tem a responsabilidade de eleger seus substitutos em caso de suas ausências.

Cabe ao COMITÊ de CONTINGÊNCIA:

- Identificar e analisar impactos nos negócios e perdas potenciais;
- Garantir a continuidade dos negócios, operações e serviços;
- Priorizar os processos críticos definidos corporativamente, incluindo todas as atividades da linha de frente às áreas de suporte;

- Estabelecer detalhadamente todas as atividades, procedimentos, responsabilidades e necessidades de recursos no momento de uma eventual interrupção no Plano de Contingência e Continuidade de Negócios;
- Garantir que as informações sobre o plano de contingência e de continuidade de negócios estejam sempre atualizadas e acessíveis (física e eletronicamente);
- Informar novos funcionários sobre a política existente na instituição e, incentivar a participação no treinamento do plano de contingência e de continuidade de negócios;
- Definir responsabilidade de atuação para cada funcionário, na execução do plano de contingência e de continuidade de negócios;
- Manter equipes treinadas nas suas respectivas responsabilidades para agilizarem o processo de recuperação e continuidade de qualquer negócio;
- Analisar periodicamente a documentação existente para suportar a restauração do ambiente em situação de contingência;
- Manter uma lista de contatos atualizada, inclusive de principais fornecedores e clientes;
- Testar as ações para restauração do ambiente;
- Simular situações emergenciais;
- Preparar ações necessárias à recuperação do funcionamento regular do MODAL.

SITES DE CONTINGÊNCIA

O Banco Modal S.A. dispõe da filial de São Paulo como *site* de contingência, , cuja estrutura dispõe de gerador de energia, sistemas de refrigeração e controles ambientais contra incêndio. Nesses casos será possível também que colaboradores acessem o ambiente de forma remota através de acesso seguro (VPN), podendo trabalhar de suas residências ou de qualquer computador disponível.

Sede Rio de Janeiro, que poderá ser utilizada como contingência de ocorrências no escritório de São Paulo. Nesse ambiente, poderão ser deslocados colaboradores, podendo, todos os demais acessarem o ambiente através de acesso remoto de suas residências (VPN).

O MODAL conta ainda com opções de *sites* remotos (residências e/ou, escritórios alugados) utilizando ferramentas como *webmail*, celulares com serviço de e-mail e acesso remoto à rede que permitem que os associados possam realizar tarefas fora do ambiente do escritório, utilizando criptografia forte.

III. CONTINGÊNCIAS DE INFRAESTRUTURAS FÍSICAS

ESTRUTURA DISPONIBILIZADA

Instalações Corporativas do MODAL

As instalações do MODAL encontram-se em dois prédios (Rio de Janeiro e São Paulo) providos de equipes técnicas treinadas periodicamente e preparados em engenharia, escape de incêndio, defesa civil e etc., com 24h x 7h de funcionamento. Periodicamente, as equipes técnicas efetuam treinamentos de escape anuais no Rio de Janeiro e São Paulo com equipe interna especialmente designada para essas situações.

Acesso ao MODAL

Os prédios onde se encontram as instalações do MODAL também contam com equipes de segurança 24 horas. O acesso de visitantes às salas do MODAL é dado somente com identificação por foto e documento na recepção do condomínio, mediante prévia autorização da recepção do MODAL, que recebem um crachá eletrônico que permite acesso somente às catracas para os elevadores.

O acesso às áreas comuns do MODAL é efetuado somente pela recepção do MODAL, mediante a presença de um Associado que os acompanhará por todo o tempo de permanência. Aos Associados, o acesso às áreas comuns do MODAL é controlado através de sistema de controle de acesso eletrônico por leitoras de crachá e dispositivo eletromagnético, ficando o acesso aos equipamentos críticos do MODAL permitido somente aos Associados das áreas de TI também via crachá eletrônico.

As salas relativas às atividades que mantém conflito de interesse com outras áreas são acessadas somente pelos associados da área em questão, ao Compliance, à Auditoria e para as atividades não conflitantes, como serviços de TI e Limpeza.

Serviços críticos para as atividades do MODAL

O MODAL considera o fornecimento de energia elétrica como serviço crítico para suas atividades. Na matriz Rio de Janeiro, o MODAL dispõe de equipamentos de *nobreak* para os servidores e para os usuários e um Gerador . Todos acionados automaticamente em caso de falha no fornecimento de energia. Na filial São Paulo, existe um *nobreak* acionado automaticamente e um Gerador.

SITUAÇÕES DE CONTINGÊNCIA PREVISTAS

Desastres e Catástrofes Naturais ou não

Abrangência:
Compreendem as situações de incêndios, inundações, desabamentos que exijam a imediata saída dos Associados das instalações do MODAL sem que os servidores tenham sido afetados.

Contingências existentes:

O Piloto de reservas de SPB acessará o ambiente de sua residência ou seguirá para São Paulo. Os demais associados, caso não seja possível breve retorno às dependências do MODAL, serão divididos em grupos e serão encaminhados para alguns dos *sites* de contingência, a saber:

- No Rio de Janeiro, serão dirigidos para a filial São Paulo ou retornarem para suas residências e/ou escritórios alugados, através de acesso remoto a rede, das ferramentas de webmail e celulares com serviço de e-mail;
- Em São Paulo, para a matriz Rio de Janeiro, podendo ainda ser dirigidos para suas residências, utilizando-se das mesmas ferramentas.

Procedimentos:

Responsável:

No Rio de Janeiro, a equipe interna é formada pelos brigadistas treinados do Modal, estes estão elencados, junto com os brigadistas back up.

Ativação da contingência:

No Rio de Janeiro, a ativação ocorre por alarme e pelo sistema interno de som. Quando do acionamento, a equipe interna se dirige à caixa de identificação de emergência obtendo o capacete, o colete e a bandeira, que os identificam como tal. Em seguida, divide-se para auxiliar o *staff* do banco para a saída imediata. O abridor de fila se dirige à escada de emergência especialmente designada para o MODAL seguido por todos os associados, indicando a saída. O fechador de fila verifica se não permaneceu alguém em sala de servidores, salas de reunião ou lavatórios, sendo o último a deixar o escritório. Ao chegar ao andar térreo, o abridor de fila conduz todo o *staff* para local especialmente designado para o MODAL, na praça em frente ao prédio.

Na filial de São Paulo, a ativação ocorre por alarme sonoro e visual. Quando do acionamento a equipe de brigadistas de cada andar veste o respectivo colete e inicia o procedimento de abandono predial. Para facilitar a organização os membros têm funções definidas que podem ser reconhecidos pelas cores dos coletes. O coordenador do abandono veste o colete vermelho, este é o líder de brigada do andar, determina a liberação das portas, auxilia as pessoas na saída de emergência e aguarda o bombeiro no andar para informar o número total de pessoas e se possuem alguma vitima. O encarregado do abandono nos andares veste o colete laranja, faz a varredura e percorre o andar a para auxiliar o líder e os demais funcionários no que for necessário. O socorrista veste colete verde, percorre o andar apoiando as pessoas com dificuldades, encaminhando-as para o elevador de emergência e solicitando a central de segurança ou bombeiro caso tenha que prestar algum socorro.

O COMITÊ de CONTINGÊNCIA deverá avaliar o tempo de retorno às instalações e, se necessário, dividirá o *staff* do MODAL nos *sites* de contingência acima detalhados, atentando que para a filial de São Paulo deverão ser encaminhados minimamente os associados chave descritos o item de CONTINGÊNCIA de PESSOAS – Aspectos Gerais.

Retorno à normalidade:

Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos Associados o retorno às instalações do MODAL.

Danos físicos relevantes a instalações ou equipamentos críticos intencionais ou não

Abrangência:
Compreendem as situações de danos a instalações ou equipamentos do MODAL de tal forma que impeçam a utilização de suas dependências ou de algum equipamento relevante para suas atividades.

Contingências existentes:

- Todos os equipamentos críticos possuem contrato de manutenção com o fabricante com "tempo de solução", tempo esse que varia conforme a criticidade do equipamento em questão.

O Piloto de reservas de SPB seguirá imediatamente para filial de São Paulo. Os demais associados, caso não seja possível breve retorno às dependências do MODAL, serão divididos em grupos e serão encaminhados para alguns dos *sites* de contingência, a saber:

- No Rio de Janeiro, serão dirigidos para a filial São Paulo ou retornarem para suas residências e/ou escritórios alugados, através das ferramentas de acesso remoto à rede, webmail e celulares com serviço de e-mail;
- Em São Paulo, para a matriz Rio de Janeiro, podendo ainda ser dirigidos para suas residências, utilizando-se das mesmas ferramentas.

Procedimentos:
Responsável:
COMITÊ de CONTINGÊNCIA

Ativação da contingência:
Tanto no Rio de Janeiro quanto em São Paulo, o COMITÊ de CONTINGÊNCIA avaliará o tempo de retorno às instalações ou de conserto / substituição de equipamentos e, se necessário, dividirá o *staff* do MODAL nos *site*s de contingência acima detalhados e para residências e/ou escritórios alugados com acesso remoto, atentando deverão ser encaminhados minimamente os associados chave descritos o item de CONTINGÊNCIA de PESSOAS.

Retorno à normalidade:
Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos Associados o retorno às instalações do MODAL.

Falhas no fornecimento de energia elétrica

Abrangência:
Compreendem as situações de problemas no fornecimento de energia elétrica por parte das concessionárias de serviços públicos, por "apagões", por falhas na rede elétrica das dependências internas do MODAL e etc., que acarretem na interrupção das atividades do MODAL.

Contingências existentes:
As contingências existentes são:

- Gerador no Rio de Janeiro;
- Gerador em São Paulo;
- Equipamentos de nobreak nas dependências Rio de Janeiro e São Paulo.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência:
No caso de falha no fornecimento de energia elétrica no Rio de Janeiro ou em São Paulo, o Gerador é acionado automaticamente, em caso de manutenção da situação, o Gerador deverá ser reabastecido quando necessário. Em caso de necessidade o *nobreak* será acionado automaticamente. A equipe de TI INFRA verificará imediatamente a extensão da falha no serviço e gerenciará a autonomia do *gerador*.
Caso ocorra falha no gerador e a energia seja mantida apenas pelo nobreak, como solução alternativa, a equipe de TI INFRA juntamente com o COMITÊ de CONTINGÊNCIA poderá determinar a necessidade de uso da contingência, podendo deslocar os colaboradores para a filial de São Paulo ou para suas residências/salas de escritório alugadas com acesso remoto a rede do Banco Modal S.A.

Retorno à normalidade:
A retomada será feita mediante eliminação dos efeitos motivadores da contingência. Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos associados o retorno às instalações do MODAL ou às suas estações de trabalho no caso de falha no gerador. Caso contrário nenhum movimento se faz necessário, pois a energia será estabelecida automaticamente.

IV. CONTINGÊNCIAS DE PESSOAL

ASPECTOS GERAIS

Política de "substitutos" para funções chave

Para cada associado que executar cargo considerado "função chave" haverá outro associado devidamente treinado e com senha de acesso aos mesmos sistemas, para substituição em situações de contingência.

SITUAÇÕES DE CONTINGÊNCIAS PREVISTAS

Ausência de Associados Chave por greves

Abrangência:
Compreende as situações de greves de caráter trabalhista, de transportes públicos e etc.

Contingências existentes:
No caso de greve dos transportes, o MODAL instruiu seus associados a utilizar os serviços das cooperativas de táxi ou outros meios de transporte privado, como táxis ou carros de aluguel, com reembolso garantido para suprir a despesa.
Alternativamente, aqueles que não obtiverem sucesso na locomoção até o site principal, poderá acionar a contingência remotamente.

Procedimentos:
Responsável:
Associado chave ou substituto ou COMITÊ de CONTINGÊNCIA.

Ativação da contingência:
Em caso de greve de transportes públicos em Rio de Janeiro ou São Paulo, os Associados-chave e substitutos devem procurar as meios de transporte privados a fim de chegar às dependências o mais rápido possível.
Em caso de ausência de funcionário chave, o respectivo substituto deverá realizar todas as tarefas necessárias para conclusão do processo de liquidação financeira das operações realizadas.
Em situações que obriguem o deslocamento para a filial de São Paulo ou o acesso remoto, os associados-chave e seus substitutos são deslocados até que todas as operações passem a ser realizadas através da contingência *off-site*.
Em caso de impedimento total de entrada na filial Rio de Janeiro, o COMITÊ de CONTINGÊNCIA dividirá o *staff* do MODAL na filial de São Paulo e por acesso remoto, atentando que para São Paulo deverão ser encaminhados minimamente os associados chave.
Em caso de impedimento total de entrada na filial São Paulo, os associados chave serão deslocados para filial do Rio de Janeiro ou terão acesso remoto. Dessa forma, o COMITÊ de CONTINGÊNCIA dividirá o *staff*, estabelecendo que alguns associados se dirijam para a matriz Rio de Janeiro e alguns retornem para suas residências, utilizando as ferramentas de *webmail*, celulares com serviço de *e-mail* e acesso remoto à rede (este último recurso ainda em uso muito restrito) que permitem que os associados possam realizar tarefas fora do ambiente do escritório.

Retorno à normalidade:

No caso de necessidade de deslocamento físico, a retomada será feita mediante eliminação dos efeitos motivadores da contingência. Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos Associados o retorno às instalações do MODAL.

Ausência de Associados Chave por Licença Médica ou Maternidade / Paternidade

Abrangência:
Compreende as situações de ausências de associados em virtude de doenças ou licenças maternidade ou paternidade.

Contingências existentes:
Os casos de ausência por licenças serão analisados caso a caso, podendo o sócio ou diretor responsável pela área optar pelas seguintes providências:

- Deslocamento de um associado para treinamento das funções exercidas pelo (a) associado (a) licenciado (a);
- Contratação de um funcionário temporário em substituição.

Procedimentos:
Responsável:
Sócio ou Diretor da área do Associado

Ativação da contingência:
Licença maternidade
Durante o período gestacional, será definida a pessoa chave que assumirá as responsabilidades e tarefas da funcionária em licença maternidade. O sócio ou diretor da área decidirá se haverá a necessidade de novas contratações para suprir a ausência da associada. Durante o período de licença é ativada uma mensagem de "*Out of Office*" do Outlook para que *e-mails* importantes não fiquem sem resposta. Na referida mensagem são descritos os períodos de ausência e quem contatar durante o mesmo.
Os acessos aos sistemas integrados à autenticação de rede serão bloqueados a partir da data de entrada em licença maternidade quando o *login* ficará ativo. Este controle é feito através de um *check list* de licença do Gente e Gestão.
Em caso de procurador, o restante do quadro de procuradores é suficiente para suprir a demanda.

Licença paternidade
Durante os dias de licença paternidade as funções do funcionário serão assumidas pela equipe da área. Em caso de procurador, o restante do quadro de procuradores é suficiente para suprir a demanda.

Licença médica
O sócio da área definirá como será a substituição da pessoa chave de licença médica, que dependerá do período de ausência do associado chave e da gravidade do motivo da licença. O sócio ou diretor da área decidirá se haverá a necessidade de novas contratações para suprir a ausência do associado.
Os acessos aos sistemas integrados à autenticação de rede serão bloqueados a partir da data de entrada em licença médica quando o *login* ficará ativo. Este controle é feito através de um *check list* de licença do Gente e Gestão.
Em caso de procurador, o restante do quadro de procuradores é suficiente para suprir a demanda.

V. CONTINGÊNCIAS DE INFRAESTRUTURAS TECNOLÓGICAS

ESTRUTURA DISPONIBILIZADA

Software de gerenciamento e controle de ativos de todo o Grupo Modal. Suas características são:

Gerenciamento de Servidores - Falhas, desempenho, serviços e auditoria da operação da gerência.

- Gerenciamento da operação baseado em serviços;
- Visualização gráfica do impacto que os eventos causam nos negócios;
- Detecção da causa raiz através da modelagem de serviços;
- Gerenciamento de performance e disponibilidade integradas;
- Gerenciamento do ambiente heterogêneo;
- Solução distribuída que monitora, controla e reporta a saúde do ambiente de TI;
- Visão única do ambiente gerenciado;
- Interface única.

Gerenciamento de Falhas de Redes:

- Gerenciamento de ambientes;
- Interface web com uma visão dinâmica;
- Possibilidade de gerenciamento de eventos facilitando o conhecimento da causa raiz;
- Coleta de informações sobre a rede ajudando na identificação de problemas;
- Gerenciamento pró-ativo;
- Acesso remoto via Web;
- Monitoração dos tempos de resposta dos caminhos da rede;
- Análise dos caminhos da rede baseado nas aplicações e protocolos;
- Diagnóstico e latência dos caminhos estáticos e dinâmicos da rede;
- Relatórios atuais e históricos com as informações dos caminhos da rede;
- Visualização gráfica dos caminhos da rede.

Gerenciamento de Performance de Redes:

- Relatórios com informações para garantir a disponibilidade e máxima utilização dos recursos de rede;
- Relatórios técnicos / gerenciais com informações atuais;
- Identificações de como os elementos da rede afetam o desempenho;
- Geração de relatórios do status do desempenho da rede.

Storage

O Grupo MODAL conta com dois equipamentos de *storage*. Suas características são:

- Alta disponibilidade;
- Desempenho;
- Alta escalabilidade;
- Tecnologia de armazenamento via rede utilizando fibra ótica;
- Centralização das informações;
- Servidor de gerenciamento próprio e independente.

***Backup* Lógico**
O Grupo Modal utiliza *software* e possui agentes de *backup* para o servidor de e-mail e sistemas operacionais A política de *backup* define periodicidade, horário e método.

SITUAÇÕES DE CONTINGÊNCIA PREVISTAS

1 – Falha no Servidor de *Home Broker*

Abrangência:
Abriga o sistema de negociação por *Home Broker*

Contingências Existentes:
- Um servidor na matriz do Rio de Janeiro;
- A filial de São Paulo tem um servidor em *stand by* que entrará em funcionamento apenas caso os dois servidores da matriz estejam indisponíveis;
- Estão localizados na filial de São Paulo operadores, certificados pelos órgãos competentes, que no caso de falha no Home Broker poderão executar as ordens de clientes.

Procedimento:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
Os servidores são balanceados, estão sempre em funcionamento, em caso de indisponibilidade de um dos servidores o outro permanecerá funcionando normalmente.

Retorno ao ambiente de produção:
A equipe de TI INFRA colocará no ar o servidor que apresentou falha, realizando todos os testes necessários no ambiente de produção.

2 – Falha no Sistema de Telecom

Abrangência:
Operadora de telefonia fixa Rio de Janeiro / São Paulo, operadora de celular, central Rio de Janeiro, central São Paulo, central do *Trading, link* de *Internet* e *links* diversos

Contingências existentes:
- Para as centrais telefônicas: linhas fixas diretas, fora das referidas centrais, disponíveis para os usuários do MODAL, inclusive para fax, aparelhos celulares disponíveis com associados ou extras disponíveis no apoio, além dos aparelhos celulares pessoais dos usuários;
- Para operadoras de telefonia fixa e centrais telefônicas: como contingência de *link* utilizam duas operadoras de telefonia fixa. Caso a infra-estrutura de uma das operadoras esteja indisponível, as ligações dos usuários serão roteadas automaticamente pelo *link* da operadora que estiver disponível. Ainda para as centrais telefônicas, temos a utilização de aparelhos celulares disponíveis com associados ou extras disponíveis no Apoio, além dos aparelhos celulares pessoais dos usuários;

Para *links* mais relevantes utilizamos dois *links*, um principal e um em *stand by*.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
A equipe de TI Infra deverá informar aos usuários da queda dos sistemas de telefonia para que os mesmos passem a utilizar as linhas diretas existentes e/ou os celulares.

Retorno ao ambiente de produção
A equipe de TI Infra deverá informar aos usuários que o serviço retornou e/ou que o *link* foi restabelecido.

3 – Falha no Servidor de Aplicação da Mensageria

Abrangência:
Abriga o *software* de Mensageria

Contingências existentes:
- Contingência do Banco Central via *Internet* com utilização de arquivo de chaves manual, disponibilizado em rede com acesso restrito à Área de TI INFRA;
- Lap top exclusivo da área de Tesouraria, com acesso a *Internet* via *wireless*, contendo o arquivo de chaves criptografia manual;
- *Backup* em fita do dia anterior.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
Verificado problema no serviço pelo Piloto de Reservas, a área de TI INFRA será acionada imediatamente, avaliando a extensão da falha e o prazo de retorno do serviço.

Durante a Contingência Parcial
1. As liquidações são efetuadas por telefone, onde um dos Pilotos de Reservas poderá solicitar a inserção, pelo Banco Central do Brasil;
2. Para cada mensagem, o Piloto de Reservas informa ao TI Infra se a mesma possui financeiro ou não, e o ISPB do destinatário, para o cálculo da posição e chave.

Durante a Contingência Total
1. Em caso de Contingência Total, após o bloqueio da RSFN, o aplicativo (BACEN) via *browser* é liberado para registro e envio de mensagens.;
2. Os operadores autorizados a utilizar o sistema de contingência devem estar cadastrados previamente na transações necessárias;
3. As mensagens recebidas anteriormente à entrada em contingência e que, no momento da entrada em contingência, estiverem, eventualmente, em fila de espera, serão processadas normalmente;
4. As mensagens devem ser enviadas respeitando-se a sequência dos números constantes da tabela RDLIST, isto é a primeira mensagem enviada deve conter na formação de sua chave o primeiro número da tabela, a segunda mensagem, o segundo número da tabela RDLIST, e assim sucessivamente.

Retorno ao ambiente de produção em caso de Contingência Parcial

1. O Piloto de Reservas, após ter terminado a liquidação das operações, solicita ao TI, posição e chave randômica informando que será para a saída de contingência Parcial;
2. Comunica ao DEBAN as informações acima, e o mesmo efetua a conferência. Nesse momento é efetivada a saída de contingência;
3. Paralelamente, a equipe de TI INFRA disponibilizará o serviço de mensageria para produção.

Retorno ao ambiente de produção em caso de Contingência Total

1. O Piloto de Reserva efetuará o contato telefônico com o DEBAN, solicitando a saída de contingência, e, para verificação da autenticidade, fornecerá a chave de segurança e a posição relativa usada no cálculo dessa chave;
2. O sistema efetuará a conferência da chave de segurança e, se estiver correta, será bloqueado o acesso ao endereço http://www.bcb.gov.br/spb-contingencia e será restabelecido o acesso regular ao MQ do BACEN;
3. Uma vez encerrada a contingência, o Piloto de Reserva deverá solicitar o extrato de sua conta;
4. Paralelamente, a equipe de TI INFRA disponibilizará o serviço de mensageria para produção.

4 – Falha no Servidor SPB

Abrangência:
Abriga o *software* de fila de mensagens de SPB

Contingências existentes:
- Servidor está em ambiente virtual com balanceamento de carga e alta disponibilidade;
- A contingência dos servidores de canais do SPB está baseada na utilização de redundância de máquina e sistema operacional aumentando a alta disponibilidade da aplicação. No caso mais crítico de desastre, com um *backup* temos a aplicação disponível novamente;
- Contingência do Banco Central via *Internet* com utilização de arquivo de criptografia manual, disponibilizado em rede com acesso restrito à Área de TI INFRA;
- *Lap top* exclusivo da área de Tesouraria, com acesso a *Internet* via *wireless*, contendo o arquivo de chaves manual.

Procedimentos:
Responsável:
TI INFRA

Ativação/retorno da contingência em caso de falha de *hardware* e/ou *software*:
Serão observados os mesmos procedimentos do item anterior em relação à contingência BACEN

5 – Falha nos Servidores de *Firewall*

Abrangência:
Abriga o *software* de segurança

Contingências existentes:

- Equipamentos configurados com alta disponibilidade com ativação automática em caso de falhas;
- Colaboradores da área de Tesouraria tem acesso remoto para casos de contingência.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
No caso de uma falha em um dos servidores de *firewall*.

Dispomos de dois servidores para contingência de *hardware* e *software* através de solução de alta disponibilidade. Qualquer política de segurança nova aplicada é automaticamente registrada em ambas as máquinas. Utiliza-se o conceito de ativo e *stand by* nesta solução para que no momento de falha no servidor ativo, o *stand by* assuma de maneira automática e com todas as políticas de segurança já definidas.

Retorno ao ambiente de produção em caso de falha de *hardware* e/ou *software*:
Após o fechamento dos sistemas, a equipe fará os procedimentos inversos, realizando todos os testes necessários no ambiente de produção.

6 – Falha no Banco de Dadosde *hardware* ou *software*

Abrangência:
O Banco de Dados de ***hardware* ou *software*** abriga as bases de sistemas, em sua maioria de terceiros, que são desenvolvidos nesta plataforma:

Contingências existentes:

- Servidor de contingência com replicação *on line* (Rio de Janeiro e São Paulo);
- Backup em rede do dia anterior;
- Contingência para SPB.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
A área de TI INFRA será acionada imediatamente, avaliando a extensão da falha e o prazo de retorno do serviço.

Retorno ao ambiente de produção em caso de falha de *hardware* e/ou *software*:
O retorno do ambiente de contingência para a produção deverá ocorrer após realização de *backup* do banco de dados da contingência e replicação manual do mesmo para a produção. O procedimento de retorno será disparado manualmente, através da execução de *scripts* de recuperação e ativação da produção.
Depois de restabelecido o ambiente de produção, serão reativados os processos de replicação e *standby*, restabelecendo-se o ambiente de contingência e as rotinas de *backup* serão alteradas novamente para o servidor de produção restabelecido.

7 – Falha no Banco de Dados

Abrangência:
O Banco de Dados abriga as bases de sistemas, em sua maioria de terceiros, que são desenvolvidos nesta plataforma.

Contingências existentes:
- Servidor de contingência com replicação *on line* (Rio de Janeiro e São Paulo);
- Backup em rede do dia anterior;
- Servidor replicado.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware e/ou software*:
A área de TI INFRA será acionada imediatamente, avaliando a extensão da falha e o prazo de retorno do serviço.

Retorno ao ambiente de produção em caso de falha de *hardware e/ou software*:
O retorno do ambiente de contingência para a produção deverá ocorrer após realização de *backup* do banco de dados da contingência e replicação manual do mesmo para a produção. O procedimento de retorno será disparado manualmente, através da execução de *scripts* de recuperação e ativação da produção.
Depois de restabelecido o ambiente de produção, serão reativados os processos de replicação e *standby*, restabelecendo-se o ambiente de contingência e as rotinas de *backup* serão alteradas novamente para o servidor de produção restabelecido.

8 – Falha na Rede

Abrangência:
*Switch*es

Contingências existentes:
- A estrutura atual conta com uma contingência de barramento duplo, onde cada *switch* possui dois caminhos distintos para o *switch* de borda (principal). Em caso de queda de uma das conexões, a segunda entra em atividade automaticamente, evitando assim a perda de pacotes.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
A equipe de TI será notificada e verificará o motivo da falha e deverá tomar as devidas providências para correção que dependerão do problema ocorrido.

Retorno ao ambiente de produção
A equipe de TI INFRA retornará com o equipamento após a manutenção, restabelecendo todas as conexões após o fechamento dos sistemas.

9 – Falha no Servidor de Arquivos

Abrangência:
O Servidor de arquivos abrange todos os diretórios da rede , além de sistemas de terceiros e os programas.

Contingências existentes:
- Replicação de todos os dados o site de contingência São Paulo;
- *Backup* em fita.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware*:
A área de TI INFRA será acionada imediatamente, avaliando a extensão da falha e o prazo de retorno do serviço.

Retorno ao ambiente de produção em caso de falha de *hardware*:
O retorno do ambiente de contingência para a produção deverá ocorrer na próxima noite em que este ambiente se encontrar disponível. Será necessário efetuar uma replicação do site de São Paulo para o Rio de Janeiro. Após o término da replicação precisará efetuar a alteração do script de logon dos usuários apontando novamente para o Rio de Janeiro.

10 – Falha no Sistema de Refrigeração da Sala dos Servidores

Abrangência:
A sala dos servidores abrange todos os servidores e serviços de telecom.

Contingências existentes:
- Dois equipamentos de ar condicionado que ficam ligados 24 horas.

Procedimentos:
Responsável:
TI INFRA

Ativação da contingência em caso de falha de *hardware* e/ou *software*:
O segundo equipamento de ar permanecerá ligado, devendo a equipe de TI INFRA providenciar a manutenção do equipamento com a qual possuímos um contrato de manutenção e prevenção para a solução do problema.

Retorno ao ambiente de produção
A equipe de TI INFRA ativará o equipamento envolvido assim que o mesmo estiver consertado.

VI. CONTINGÊNCIAS DE SERVIÇOS EXTERNOS

CLASSIFICAÇÃO DOS SERVIÇOS

Serviços críticos
O MODAL identificou os serviços críticos, levando em conta dois aspectos: relevância do serviço prestado e/ou prestadores de serviços com excessiva concentração no mercado.

SITUAÇÕES DE CONTINGÊNCIA PREVISTAS

Serviços críticos

1 – Liquidação de operações com a Bolsa

Contingências existentes:

- Ver capítulo de contingência de "Falha no Sistema de Telecom";
- Ver capítulo de contingência de "Falha do Servidor de *Home Broker*";
- Todos os serviços estão descritos e amparados por contratos;
- Colaboradores podem ser deslocados para a filial de São Paulo ou utilizar os sistemas por acesso remoto de qualquer computador através do *token*;
- Falar com a BM&FBovespa para confirmar o valor que será liquidado no dia da contingência.

Procedimentos:
Responsável:
Sales & Trading
Mesa de Operações
Custódia
Middle Office

2 – Manutenção de posições de clientes

Contingências existentes:

- Geração de relatório em sistema internocomparando com relatório de Custódia do dia anterior;
- Colaboradores da área de custódia deveram acessar o site de São Paulo onde o servidor de VPN está com os sistemas necessários cadastrados e poderão fazer suas rotinas de manutenção de posição normalmente.

Procedimentos:
Responsável:
Controle de Fundos
Custódia

3 – Liquidação de operações com clientes

Contingências existentes:

- Colabores podem acessar o ambiente de contingência através de *token*;
- Colabores podem se deslocar para o ambiente de contingência (São Paulo);
- Ver capítulo de contingência de "Falha no Sistema de Telecom";
- Ver capítulo de contingência de "Falha do Servidor de *Home Broker*";
- Todos os serviços estão descritos e amparados por contratos.

Procedimentos:
Responsável:
Custódia
Middle Office

4 – Serviços de administração de fundos – fundos abertos
Contingências existentes:

- Disponibilização de um outro *link* pelo administrador dos fundos;
- Planilhas de contingência formatadas pelo administrador dos fundos e individualizadas por tipo de operação com envio por e-mail;
- Planilha interna de dupla checagem para as operações da carteira;
- Para operações de cotistas o administrador dos fundosdisponibiliza um *link* de um módulo de contingência;
- Planilhas de contingência de movimentação de cotistas da Distribuição.

Procedimentos:
Responsável:
Controle de Fundos
Áreas Comerciais

5 – Serviços de administração de fundos – fundos especiais

Contingências existentes:

- Controle em planilha paralela para a carteira e apuração da cota;
- Para cotistas existe a impressão diária de relatório de fechamento de posição dos cotistas. Em caso de aplicação, aguarda-se o retorno do sistema dentro do dia, mas considera-se a entrada de financeiro na planilha de caixa (controle paralelo);
- Em caso de resgate, atualiza-se a cota em uma planilha com a posição dos clientes, e então calcula-se o resgate que será pago assim como o imposto da operação.

Procedimentos:
Responsável:
Controle de FundosFundos Especiais e Corporate

6 – Folha de Pagamento

Abrangência:

- Registros referentes à folha de pagamento no sistema. O acesso ao *software* se dá por comunicação de acesso remoto ao *datacenter*. Este processo é todo concentrado no final de todos os meses;
- Hospedagem da base de dados da folha de pagamento;
- Portal de RH disponibilizada na *Intranet.*

Contingências existentes:

- Para atualização e enquadramento do sistema em cumprimento à legislação trabalhista - Equipe especializada em matéria trabalhista para atualização legal e fiscal de todo o sistema de folha, com acompanhamento por parte do Modal das mudanças da legislação.
- Para o serviço do registro dos dados e processamento da folha – não possuímos contingência interna. Em caso de falha do sistema e indisponibilização do mesmo, a movimentação da folha de pagamento será enviada para empresa externa e a mesma será autorizada a processar a folha diretamente em suas instalações.
- Para os serviços de hospedagem da folha de pagamento e portal de RH – Não há contingência para o caso do serviço não estar disponível para o Gente e Gestão. Nesse caso a folha de pagamento está hospedada nas instalações de empresa externa hospedagem e gerenciamento do sistema com acesso controlado pela web, disponibilizando o sistema para uso dos diversos níveis de usuários.

Procedimentos:

Responsável:

Gente e Gestão

TI INFRA

Em caso de falha acionar a empresa prestadora do Serviço

7 – Compensação

Abrangência

Representação dos bancos junto às Câmaras Regionais e processamento integral dos documentos da compensação de cheques, bem como de bloquetos de cobrança e DOC's

Contingências existentes:

- O serviço é prestado pela ABBC – Associação Brasileira de Bancos que realiza tais serviços, observando os padrões de segurança, contingência e qualidade exigidos pelos órgãos reguladores (Banco Central, Banco do Brasil e CIP);
- O serviço está regulamentado pela relação de associado do Modal com a ABBC através de contrato formal entre as partes.

Procedimentos:

Responsável:

Tesouraria

Em caso de falha acionar a empresa prestadora do Serviço – ABBC

8 – Difusores de Informação

Contingências existentes:

- Ver capítulo de contingência de "Falha no Sistema de Telecom";
- Todos os serviços estão descritos e amparados por contratos.

Procedimentos:
Responsável:
TI Infra

Em caso de falha acionar a empresa prestadora do serviço

9 – Informações Creditícias e Cadastrais

Contingências existentes:

- Para Serasa informações creditícias – consultas aos Cartórios e contratação de outro serviço de consultas de crédito disponíveis no mercado;
- Ativar contato por e-mail solicitando consultas;
- Todos os serviços estão descritos e amparados por contratos.

Procedimentos:
Responsável:
Cadastro / TI Infra

Em caso de falha acionar a empresa prestadora do serviço

10 – Gerenciamento de Documento
Abrangência:

- Custódia da documentação física contábil, fiscal e contratual;
- Gestão de arquivo ativo documentação cadastral de clientes contrato assinado, porém os documentos físicos irão para armazenamento somente na finalização da digitalização no sistema;
- Custódia de mídias em fitoteca de segurança - armazenamento e transporte diário de fitas de backup, bem como outras mídias eletrônicas.

Contingências existentes:

- Empresa de gerenciamento de documentos , altos padrões de segurança, conservação e manutenção e gerenciamento de risco e procedimentos de *disaster recovery*;
- Os serviços estão formalmente regidos por contratos entre as partes.

Procedimentos:
Responsável:
CEDOC / TI Infra

Em caso de falha acionar a empresa prestadora do Serviço.