MAUD CAPITAL GESTORA DE ATIVOS LTDA. (“Maud”)

Plano de Continuidade de Negócios - PCN

Janeiro 2025

Sumário

I. OBJETIVO

1.1. O Gerenciamento de Continuidade de Negócios consiste na definição de objetivos, estratégias e planos para identificar e gerenciar incidentes ou interrupções nos negócios, com intuito de manter as operações em níveis aceitáveis, bem como assegurar o retorno das atividades à normalidade, reduzindo possíveis perdas e mantendo a perenidade da Maud, e neste sentido visa estabelecer os critérios para o Plano de Continuidade de Negócios (PCN).

1.2. A política deve ser atualizada e mantida de forma que a Maud possa identificar preventivamente a existência de vulnerabilidades que possam expô-la a riscos de continuidade de negócios, considerados incompatíveis com os níveis de riscos aceitáveis pela Diretoria da Maud e planejar ações para reduzir essa exposição.

II. CONCEITO

2.1. O Gerenciamento de Continuidade de Negócios tem o objetivo de fortalecer a resiliência da organização e a sustentabilidade de seus produtos e serviços essenciais para o negócio, mesmo em situações adversas de crises e desastres. Ela estabelece as diretrizes e os princípios básicos necessários para uma resposta emergencial adequada ao evento, e à recuperação e restauração dos níveis de normalidade operacional.

2.2. O Plano de Continuidade de Negócios (PCN) assegura à Maud a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos. Os possíveis cenários de indisponibilidade são:

a) Perda total do acesso às dependências da sede da Maud e/ou dos recursos abrigados nela;

b) Perda total ou parcial da estrutura tecnológica (serviços e/ou comunicação);

c) Perdas temporárias ou permanentes de recursos.

2.3. Para contingência/desastre que provoquem efeitos menores, o PCN poderá ser parcialmente aplicado, conforme entendimento das equipes envolvidas no processo de ativação do plano, horário de ocorrência, processos e atividades pendentes, tempo de recuperação comparado ao tempo de ativação completa e quantidade de recursos indisponíveis.

2.4. O PCN não inclui procedimentos de recuperação para serviços terceirizados essenciais à continuidade dos negócios da Maud. Para estes casos, os contratos devem possuir acordos de níveis de serviço, os quais endereçam a responsabilidade da contraparte pela respectiva retomada operacional, em cenários de contingência/desastre, de forma a atender as necessidades de negócios da Maud.

III. ESTRUTURA

3.1. O modelo de Gerenciamento de Continuidade de Negócios visa identificar os processos mais críticos ao negócio da Maud e endereçá-los para o ambiente de continuidade de negócios visando o menor impacto possível para o negócio da Maud e para seus clientes.

3.2. Para tanto, o Gerenciamento de Continuidade de Negócios é composto por:

a) PAC - Plano de Administração da Crise – É acionado após decretada a Crise, e é voltado para todo o processo. Tem seu término quando se volta à normalidade;

b) PRD-TI - Plano de Recuperação de Desastres -TI – É acionado junto com o Planos de Continuidade Operacional (PCO), e é focado na recuperação/restauração de componentes que suportam o PCN.

3.3. O desenvolvimento do Plano de Continuidade de Negócios é baseado na avaliação dos processos críticos estabelecidos pela Administração da Maud compreendendo as suas principais etapas:

a) Análise de Impacto nos Negócios (BIA); e

b) Estratégia de recuperação;

3.4. Desta forma, simular situações de emergências, definir responsabilidade de atuação para cada colaborador na execução do PCN e acima de tudo mantê-lo atualizado são fatores crítico de sucesso.

IV. TREINAMENTOS

4.1. O programa de treinamentos objetiva a conscientização e a capacitação dos funcionários envolvidos nos planos de continuidade do negócio, orientando sobre os conceitos, planos e metodologias aplicáveis. A disseminação da cultura de gestão de continuidade de negócios se faz necessária para a eficácia dos planos em um momento de crise ou de desastre.

V. PLANO DE MONITORAÇÃO E DECLARAÇÃO DE CRISE OU DESASTRE

5.1. Definição de Crise ou Desastre

Será estabelecido um cenário de crise ou desastre quando o tempo total de recuperação dos processos e sistemas críticos for superior ao tempo máximo de 1 hora de indisponibilidade do serviço/processo.

Processos e sistemas críticos podem ser definidos como um processo de trabalho que uma vez paralisado por tempo superior ao definido pelo responsável pelo processo irá afetar sensivelmente as operações e serviços da Maud gerando impacto relevante nos clientes internos e externos da Maud.

5.2. Monitoração de Comunicação de Eventos

Qualquer funcionário da Maud, ao constatar alguma anormalidade que paralise quaisquer dos processos, deverá comunicar o fato à Diretoria da Maud, ou na sua ausência ao Diretor Presidente da Maud.

Em ocorrendo estes eventos que paralisem algum processo essencial ao negócio da Maud, o Líder de Contingência avaliará a ocorrência e, com base nas informações recebidas, e tendo avaliado o grau de impacto versus horário crítico, decidirá por declarar ou não a contingência.

Líder de Contingência	Cargo	Telefone	E-mail
Marcello Vidigal	Diretor de Risco e Compliance	(11) 992574704	mlutz@maud.capital

Este é o meio de comunicação a ser utilizado pelos colaboradores da Maud como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PCN.

5.3. Análise de Impacto nos Negócios – BIA (Business Impact Analysis)

É o processo de analisar as atividades e os efeitos que uma interrupção de negócio pode ter sobre elas. Para análise de Impacto no Negócio, deve-se avaliar de forma direta e objetiva os impactos que a Maud pode sofrer em razão de prováveis falhas e/ou interrupções nos seus processos que suportam os produtos e serviços de negócio, devendo considerar minimamente:

a) O impacto da interrupção dos produtos e serviços oferecidos; e

b) As prioridades de recuperação, o mapeamento das áreas que operacionalizam o produto ou serviço, a identificação dos serviços de TI utilizados e qualquer recurso necessário para retorno da operação.

VI. AVALIAÇÃO DE IMPACTO

A Avaliação do Impacto consiste na aplicação do questionário de avaliação de impacto em cada rotina/processo/atividade, com o objetivo de avaliar a questão sob as esferas/aspectos: financeira; de imagem; legal; e operacional.

> **DESTAQUE**: Neste momento, a Maud adota a replicação/espelhamento da totalidade dos principais processos em ambiente de nuvem, dos mais críticos aos menos críticos, incluindo os considerados essenciais e que suportam o negócio na sua execução integral e no atendimento às liquidações dos clientes, de forma que, neste momento, avaliou-se como não necessária a aplicação do BIA (Análise de Impacto de Negócios) para a escolha e definição de um número mais reduzido de processos críticos, mas que suportariam a operação sem maiores impactos ao negócio.

6.1. Levantamento de Dependências e Requisitos

Para cada rotina/processo/atividade identificada é realizado o levantamento de todos os elementos que suportam a operacionalização do negócio e outros requisitos relacionados, entre eles:

a) Janela de execução (período);

b) Período crítico;

c) Se possui procedimento de contingência;

d) Quantidade de pessoas envolvidas;

e) Registros vitais de informações;

f) Sistemas/serviços de TI envolvidos;

g) Infraestrutura física (equipamentos e materiais);

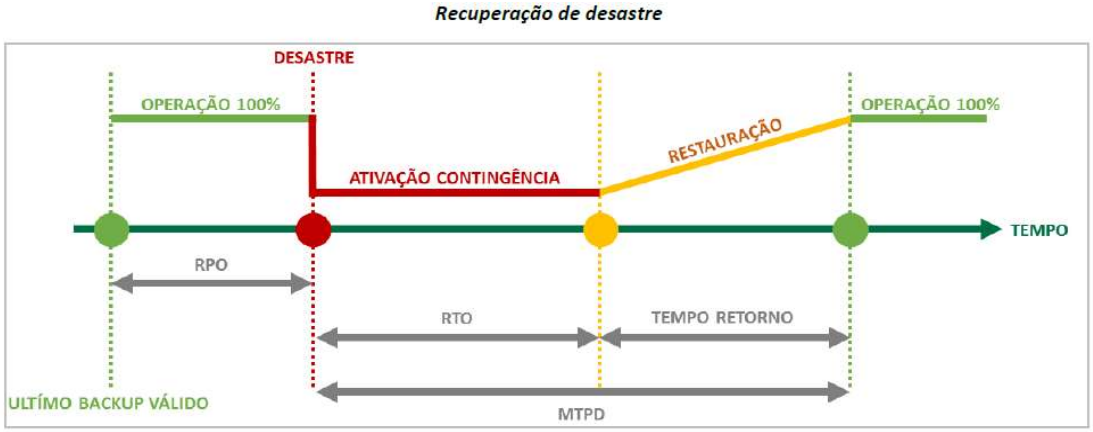
h) Terceiros relevantes (dados de fornecedores);

i) RPO - Return Point Objective – é período máximo de tempo que um processo de negócio tolera quanto à perda de seus dados, sem sofrer impactos significativos financeiros, operacionais e de imagem. É o parâmetro da informação mínima (por ex: fechamento do dia anterior) dos dados de um processo de

negócio, que o PCN precisa ser capaz de recuperar após um cenário de contingência/desastre, indicando o ponto (estado) exato de retorno para estes dados dos sistemas de informação;

j) RTO - Recovery Time Objective – é período máximo de tempo que um processo tolera em inatividade, sem sofrer impactos significativos financeiros, operacionais e de imagem. É também o parâmetro de tempo que o processo precisa estar recuperado após um desastre/contingência.

IMPORTANTE: Conceitos/premissas adotadas Maud:



- RPO - Recovery Point Objective (objetivo do ponto de recuperação) – 10/20min
- RTO - Recovery Time Objective (objetivo do tempo de recuperação) – 1 hora
- MTPD – Maximum Tolerable Period of Disruption (período máximo de interrupção tolerável) – 1 hora

1. Estratégia de Negócio em Cenário de Continuidade

VII. DEFINIÇÃO DAS ESTRUTURAS NECESSÁRIAS

7.1. Definidos os processos mais críticos para a continuidade dos negócios, bem como suas dependências e requisitos necessários, define-se então o ambiente alternativo de trabalho.

7.2. Para definição do site alternativo poderão ser considerados aspectos relacionados a:

a) **Pessoas** – logística de transporte, documentação do método de execução das atividades críticas de forma a propiciar que outras pessoas executem as rotinas;

b) **Tecnologia** – acesso remoto, distribuição geográfica da tecnologia, ou seja, manter a tecnologia em locais diferentes que não deverão ser afetados pela mesma interrupção de negócios;

c) **Informações** – as estratégias de informações devem incluir formatos físicos (impressos) e eletrônicos, sobretudo para aquelas consideradas essenciais como informações financeiras, folha de pagamento, cadastro de fornecedores e documentos legais (contratos de empréstimo, termos de adesão etc.). Cópias também devem ser guardadas em instalações alternativas, previamente estabelecidas;

d) **Instalações** – realização de trabalho em local alternativo;

e) **Gestão das partes interessadas** – identificação de responsáveis pela comunicação com as partes interessadas, autoridade e mídia, se aplicável.

VIII. PLANOS DE ADMINISTRAÇÃO DE CRISE (PAC)

O PAC compreende o conjunto de ações e medidas estratégicas que objetivam minimizar as perdas e assegurar a continuidade operacional em caso de crise ou eventos que causem a indisponibilidade prolongada dos ativos que suportam a operação da Maud. Estabelece processos e procedimentos internos para responder a eventos que possam ter impacto significativo na operação ou na reputação da Maud.

A gestão de crise deve considerar minimamente:

a) Procedimentos de identificação de eventos de alertas, ameaças e critérios de acionamento de contingência;
b) Responsáveis pelo gerenciamento de crise;
c) Mecanismos de comunicação interna, externa e com a imprensa; e
d) Procedimentos para responder a cenários de crise pré-definidos.

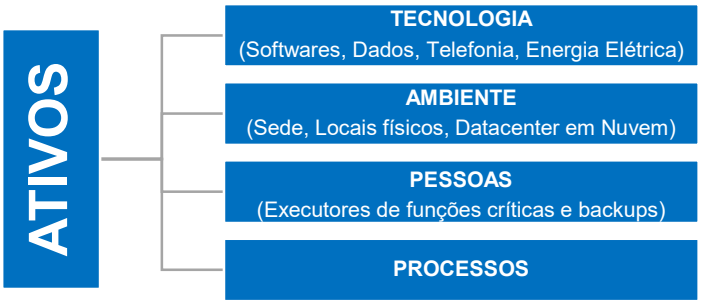
Para a definição das estratégias de mitigação de riscos operacionais relacionadas à continuidade dos negócios, a Maud poderá utilizar a Análise de Impacto nos Negócios (BIA), um insumo para a definição das áreas para as quais são elaborados Planos de Continuidade Operacional (PCO) e os sistemas críticos a serem testados nos Planos de Recuperação de Desastres de TI (PRD-TI).

8.1. PAC - Objetivo

O Plano de Administração de Crise (PAC) da Maud tem como escopo a criação de uma governança para o tratamento de situações de crise, propondo, previamente, ações e medidas a serem adotadas quando da concretização daqueles eventos.

O PAC tem como objetivo proporcionar a continuidade das atividades críticas da Maud, considerando os ativos que as suportam e os cenários de contingência/desastre, até que sejam restabelecidas as condições normais.

Tais ativos estão divididos em quatro grupos: Tecnologia, Ambiente, Pessoas e Processos:



O Plano de Administração de Crise pretende:

a) **Proteger a Maud:** assegurar a estabilidade organizacional após a ocorrência de uma crise/desastre;
b) **Atender às regulamentações vigentes**: a Maud está sujeita a diversas regulamentações de mercado;

c) **Fornecer resiliência:** desenvolver alternativas para a continuidade das operações, baseadas em estudo de impacto nos negócios, e definir equipes mínimas que suportam o trabalho de recuperação são providências fundamentais para enfrentar uma situação de contingência/desastre de forma eficiente e eficaz;

d) **Garantir confiabilidade**: o PAC atualizado e testado assegura a continuidade das operações da Maud no nível estabelecido para operações críticas; e

e) **Minimizar a tomada de decisão tempestiva:** em cenários de contingência/desastre, a tensão e estresse inerentes tornam a tomada de decisão mais complexa, podendo ocasionar erros e a tomada de decisões, muitas vezes, não eficiente ou eficaz. A comunicação também poderá ser dificultada durante um cenário de contingência/desastre. Portanto, o PAC funciona como veículo fundamental para garantir a execução de medidas acertadas, pois seu planejamento foi concluído e testado simulando situações reais de crise.

8.2. PAC - Definições

a) **Incidentes – Foco Risco Operacional**: incidentes/perdas operacionais como qualquer evento de risco operacional por meio do qual a Maud está exposta a prejuízos financeiros diretos, prejuízos indiretos e/ou oportunidades perdidas. Todas as áreas devem reportar para a Diretoria da Maud, no momento de sua ocorrência, os incidentes ou perdas operacionais ocorridas.

b) **Incidentes – Foco Gestão de Continuidade de Negócios** - incidente de continuidade de negócios como qualquer evento adverso ou anormal que torne indisponível a utilização de recursos críticos (pessoas, infraestrutura ou locais de trabalho) necessários para a operação da Maud. A resposta a estes incidentes deve ser imediata e internamente focada nos objetivos primários de conter o incidente e garantir a segurança de todos os funcionários da Maud.

c) **Crises -** definida como qualquer situação que, a partir de um evento crítico que ameace ou tenha o potencial de ameaçar a reputação da Maud, possa ocasionar graves impactos nas operações da instituição, se tornar objeto de intenso questionamento ou gerar falta de credibilidade para as partes interessadas.

d) **Administração de Crises -** definida como um processo para avaliar as eventuais situações de crise e consolidar a forma de agir para combatê-las. Para isso, estipula um método ágil de identificação e classificação dos cenários, com os possíveis impactos negativos e, a partir de suas equipes e cientes de seus papéis e responsabilidades, elabora a estruturação de uma resposta sustentável à situação apresentada para orientação de todos os funcionários da Maud.

e) **Contingência -** dependendo do cenário da crise e de suas consequências, é possível decretar o contingenciamento de recursos da Maud, visando ativar as estruturas, processos e procedimentos preparados previamente para dar continuidade aos negócios após uma crise que resulte em indisponibilização dos recursos utilizados originalmente.

f) **Partes Interessadas** - define como partes interessadas qualquer pessoa ou grupo que apresente um vínculo com as operações da Maud e que possa gerar algum impacto potencial diretamente ou indiretamente na reputação da Maud.

Este plano se concentra principalmente em proteger a reputação da Maud e, neste sentido, em oferecer diretrizes para lidar com as partes interessadas durante uma crise.

8.3. PAC - Metodologia

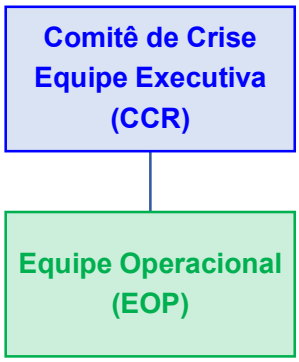
O Plano de Administração de Crise (PAC) utiliza uma abordagem de equipe para resposta às emergências e interrupções. Cada equipe possui responsabilidades específicas, que permitem a comunicação durante a interrupção do negócio. O propósito do modelo de equipe é coordenar as atividades centrais relacionadas à recuperação das funções críticas e entrega dos produtos e serviços relacionados.

O atendimento e as ações de continuidade estão determinados através dos seguintes fatores:

a) Segurança dos recursos humanos;
b) Obrigações legais, regulamentares e/ou contratuais;
c) Dependências entre as áreas, prestadores de serviços;
d) Obrigações internas e externas;
e) Acesso a informações essenciais para as rotinas operacionais.

8.4. PAC - Estrutura de Gestão de Crise

O organograma abaixo descreve a estrutura de ativação do PAC na Maud, sendo formado por duas equipes com finalidades específicas:



8.5. PAC - Funções e Responsabilidades

O Anexo I – consta a tabela que descreve os papéis e as responsabilidades de cada equipe citada no item 8.4, na operacionalização da continuidade de negócios em cenários de contingência/desastre.

8.6. PAC - Diretrizes do Plano de Gerenciamento de Crise

Para garantir desempenho, eficiência e eficácia dos objetivos do PAC, as diretrizes a serem seguidas são:

a) O PAC deve ser testado periodicamente, visando melhoria nos processos e eficácia de seus objetivos;

b) Os profissionais nomeados para as equipes do PAC devem possuir um suplente;

c) As informações produzidas/manipuladas pelas áreas/funcionários precisam ser necessariamente gravadas no diretório da rede, de forma que estejam disponíveis para a recuperação em cenário de contingência/desastre;

d) Os documentos físicos (contratos, assinaturas, documentos) devem ser mantidos nas áreas, seguindo procedimentos internos, considerando a possibilidade de incluir no sistema de gerenciamento eletrônico de documentos;

e) Os colaboradores não estão previamente autorizados a divulgar a terceiros nenhum tipo de informação sobre a interrupção dos negócios e a subsequente ativação do PAC. Tais informações serão repassadas para as partes interessadas, se a Maud julgar necessário, por um representante do Comitê de Crise (CCR);

f) Os funcionários das áreas participantes do PAC são responsáveis por enviar as observações, manutenções ou atualizações relativas ao PAC para o Comitê de Crise (CCR).

8.7. PAC – Cenários de Crise

Quanto mais rapidamente for definida uma situação de desastre, mais rapidamente se dará o início das atividades para o restabelecimento do processamento, reduzindo assim os prejuízos eventualmente causados pelo desastre. Porém, deve ser levado em conta o prazo mínimo que se deve aguardar para a decretação do desastre sem causar impactos, como por exemplo, na execução de fechamentos contábeis e outras datas críticas e as despesas que essa decisão acarretará.

Abaixo seguem alguns eventos que podem ocasionar cenários de crises:

a) Limitação de Acesso ao Prédio/Sede;
b) Problemas em Gestão de Condomínio;
c) Falha de Tecnologia;
d) Perda de Pessoas;
e) Dano à informação ou à propriedade intelectual;
f) Perda de fornecedores críticos.

IX. NÍVEIS DE SEVERIDADE DOS EVENTOS E DECISÃO DE ACIONAMENTO DO PAC

9.1. Sistêmicos

A avaliação dos eventos sistêmicos que podem gerar indisponibilidade está contemplada no processo de PRD-TI, que avalia o nível de severidade do dano, o nível de criticidade do sistema afetado, a previsão de recuperação e os planos de contingência que deverão ser acionados para assegurar as condições de restabelecimento de continuidade das atividades de negócio, limitando graves perdas decorrentes de risco operacional.

9.2. Operacionais

Devido às muitas variáveis de uma interrupção (incluindo o tempo médio de reparo de estragos, substituição de peças, componentes ou equipamentos), o Comitê de Crise (CCR) deve estar preparado para tomar a

decisão de decretar ou não a ativação do PAC, segundo critérios de severidade pré-definidos. Isto minimiza análises subjetivas e decisões precipitadas em situações de desastre.

Logicamente, é impossível prever todos os problemas, emergências ou desastres que podem desencadear uma crise. Mesmo assim, neste tópico são apresentados alguns exemplos e um critério para a tomada de decisão pelo Comitê de Crise (CCR) quando necessário.

A seguir estão definidos exemplos de eventos classificados com os níveis distintos de severidade relacionados a interrupções pequenas, médias e grandes. Cada nível corresponde a uma potencial situação:

- Nível – Incidente - normalmente são incidentes relacionados à infraestrutura ou parte dos equipamentos de TI, tais como:

a) Abastecimento de energia elétrica para os equipamentos;
b) Quadro de força;
c) Equipamentos de teleprocessamento;
d) Hardware / Software (CPU, discos, servidores, outros);
e) Operacionais em geral (erros humanos, manuseio indevido de equipamentos etc.);
f) Parada do ar-condicionado;
g) Suspeita de vazamento de gás;
h) Ameaça de bomba.

Numa situação de incidente desse tipo normalmente não é declarada contingência, pois o incidente tende a ser resolvido com ações operacionais que usualmente não ultrapassam 1 hora. Portanto, não se justifica a transferência do processamento para a Work-Area*.

- Nível – Emergência - neste nível estão englobadas situações que causem, por exemplo, uma paralisação do datacenter da Maud ou de infraestrutura predial por um período previsível que não ultrapasse 2horas hora, tais como:

a) Problemas com a rede em nuvem;
b) Problemas com a infraestrutura;
c) Problemas técnicos com parte dos equipamentos;
d) Desastre parcial (ex: inundação, parada elétrica, etc.);
e) Problemas com greve ou tumultos em geral;
f) Princípio de incêndio local ou ao redor, alagamento de algum andar;
g) Pandemias.

No caso de um evento deste nível o Comitê de Crise deverá analisar o momento, a previsão para retorno à situação normal, outros fatores relativos à situação e declarar ou não contingência.

- Nível – Desastre - enquadram-se neste nível todas as ocorrências que, pelas suas dimensões, poderão causar a paralisação total do datacenter ou eventos de grandes proporções na infraestrutura por um período maior que 2 horas e sem previsão de retorno, devido a:

a) Perda parcial ou total da Sede do datacenter;
b) Perda parcial ou total dos servidores e outros equipamentos do datacenter;
c) Problemas sérios com abastecimento de energia ou infraestrutura;

d) Incêndio local;
e) Alagamento.

No caso de um evento deste nível o Comitê de Crise deverá analisar o momento, a previsão para retorno à situação normal, outros fatores relativos à situação e declarar ou não contingência.

9.3. Avaliando os Danos

O Comitê de Crise (CCR) deve fazer uma análise da situação e avaliar os danos que ocasionaram a interrupção no processamento normal. Nessa análise, deverão ser levados em consideração os níveis de severidade citados.

Para o correto enquadramento do nível de severidade, é importante que seja feita uma acurada identificação dos danos causados e uma estimativa realista do prazo para retorno à situação normal de produção. Nessa análise, os seguintes itens devem ser considerados:

a) Momento da interrupção, tais como o horário crítico, período de pico, dia da semana ou do mês, época do ano, requisitos de contabilização, projetos críticos, etc.;
b) Tipo de evento causador e confiança no tempo estimado para solução do problema;
c) Natureza do desastre e extensão dos danos (por exemplo: explosão, fogo, ou algum evento da natureza que cause dano considerável na infraestrutura);
d) Eventos não relacionados diretamente à Sede (por exemplo: falha nos recursos de comunicação, falta de energia, greve, etc.);
e) Se há algum problema externo à Sede que esteja afetando algum componente da Sede.

9.4. Decidir pela Decretação de Contingência

Com base nos dados coletados, nos danos causados e nos prazos previstos para recuperação, o Comitê de Crise (CCR) decidirá pelo acionamento ou não do processo de contingência, utilizando como referência e apoio os tópicos apresentados neste plano.

X. ACIONAMENTO DA CONTINGÊNCIA

10.1. Convocar as equipes

A Comitê de Crise Equipe Executiva (Equipe CCR), presente no local do desastre ou no seu entorno ou distante, deverá convocar a Equipe Operacional (EOP) informando-a sobre o ocorrido para iniciar a avaliação do nível do desastre:

a) Avaliar e solicitar que se iniciem as atividades através da PRD-TI;

b) O Comitê de Crise (CCR) já poderá decidir que sua instalação será na própria Work-Area* caso o desastre afete as instalações da Sede;
c) Decidida a decretação de contingência, o Comitê de Crise (CCR) deve ser instalado e deste local serão comandadas as operações;
d) O acionamento seguirá as orientações do Anexo III deste documento.

10.2. Work-Area*

DESTAQUE: WORK-AREA - A Maud adota o modelo homeoffice como modelo principal em caso de um evento de acionamento de continuidade, e esta avaliação é continuamente monitorada e reavaliada para suportar um evento a qualquer momento.

Por ora, a Maud reconhece o sucesso efetivo deste modelo e não observa nenhum comprometimento da sua operação.

Esta decisão será definida em momento de acionamento real e de acordo com a percepção do Líder do CCR e de seus apoiadores, que diante do evento deverá definir o melhor procedimento para o momento.

10.3. Work-Area* - Localização

Conforme previsto no item 10.2 a Maud adota o modelo homeoffice para os profissionais elegíveis à Equipe EOP.

10.4. Servidor Backup - Localização

A Maud adota o modelo de datacenter principal e secundário em ambiente de nuvem e todas as instalações descritas no item 8.1 podem suportar as atividades de ambas.

XI. EXERCÍCIO DE TESTES

Os testes deverão ser executados periodicamente, sendo no mínimo anualmente, com o objetivo de garantir que o PAC está atualizado e funcional.

Para garantir o sucesso dos testes faz-se necessário:

a) Formalizar o Plano de Testes;
b) Definir o Escopo do Teste e Cenário;
c) Desenvolver Metas e Objetivos do Teste;
d) Documentar as premissas dos Testes;
e) Estabelecer data e duração do Teste;
f) Gerar o Relatório de Testes;
g) Atuar na gestão dos problemas identificados.

As atualizações deste plano deverão ser homologadas e validadas pelos membros do Comitê de Crise (CCR).

XII. PLANOS DE RECUPERAÇÃO DE DESASTRES DE TI (PRD-TI)

Os PRD-TIs devem conter os procedimentos técnicos e operacionais para a recuperação dos serviços de TI, devendo minimamente:

a) Ser implementados para os serviços de TI considerados críticos;
b) Ser revisados anualmente e em mudanças significativas no ambiente de tecnologia do serviço que houver impacto na documentação e em seus procedimentos;

c) Ser testados, no mínimo, anualmente. Cada teste deve ser documentado e seu resultado formalizado.

DESTAQUE: Neste momento, a Maud adota a replicação/espelhamento da totalidade dos principais processos em ambiente de nuvem, dos mais críticos aos menos críticos, incluindo os considerados essenciais e que suportam o negócio na sua execução integral e no atendimento às liquidações dos clientes. A viabilidade de acesso ao ambiente de tecnologia se dá por acesso VPN aos funcionários das Equipes CCR e EOP, quando necessário.

XIV. ESTRATÉGIA DE RECUPERAÇÃO - TI

A Maud adota estratégia de recuperação para situações de desastres que venham paralisar as operações do Data Center Microsoft Azure ou do prédio onde são executadas as atividades por parte da Maud. Importante mencionar que caso algum desastre ocorra nas instalações da matriz em São Paulo, teremos disponibilidade de acesso via Home Office com o uso de VPN Site to Client.

XV. REVISÃO DO DOCUMENTO

A periódicidade de revisão deste documento é, no mínimo, anual.

XVI. APROVAÇÃO DESTA POLÍTICA

A presente política foi aprovada pelo Comitê de Riscos e Compliance da Maud.

HISTÓRICO DAS ATUALIZAÇÕES			
DATA	**VERSÃO**	**AUTOR**	**REVISOR**
Janeiro 2025	1.1	Victor Obara	Marcello Vidigal

Anexo I - Procedimentos de Operação da Contingência

EQUIPES	RESPONSABILIDADES
Comitê de Crise (CCR) Formado pelos Diretores com poder de tomada de decisão. Composição conforme Anexo II	Aspectos Estratégicos: - Avaliar o evento e a potencial situação de crise e quando necessário, decretar situação de crise e ativar os planos; - Decidir sobre a necessidade de comunicações ao mercado, a órgãos reguladores e mídia, e avaliar e decidir aspectos com impacto de natureza legal e trabalhista; - Por intermédio da Equipe Operacional (EOP), colher informações sobre a natureza da contingência, desastre, local e potencial danos, assim como as medidas operacionais que estão sendo tomadas; - Conduzir a estratégia de negócios para atuação em ambiente/cenário de Continuidade. Aspectos Financeiros: - Decidir sobre escolhas de manutenção ou interrupção de negócios e de operações; - Aprovar recursos financeiros para a operacionalização do PAC, quando julgar necessário; - Negociar linhas de crédito adicionais, quando necessário; - Avaliar e aprovar ordem de compras emergenciais ou despesas extraordinárias. Aspectos Operacionais: - Comunicar-se e coordenar a Equipe Operacional (EOP); - Ativar a *Work-Area**; - Executar a ativação do plano; - Solicitar decretação da situação de desastre (ativação do plano); - Tomar decisões operacionais; - Coordenar e executar testes de validação periódicos e treinamentos; - Manter o PAC atualizado e realizar treinamentos periódicos.
Equipe Operacional (EOP) Formada por funcionários das áreas participantes do PAC para executar os processos críticos e vitais diários da Maud após a ativação e estabelecimento da *Work-Area** Composição conforme Anexo II	Aspectos Operacionais: - Execução dos testes periódicos de continuidade de negócios, além da atualização dos processos operacionais; - Execução de testes periódicos de PRD-TI, validação de processos recuperados, e formalização e apresentação dos resultados; - Avaliar e recuperar danos nos ambientes de tecnologia (Sites Principal e *Work-Area**) os quais suportam os processos/áreas críticos de negócio da Maud, prestando informações vitais para que seja tomada a decisão de ativar ou não o PCN; - Quando convocado, operacionalizar a atividade, segundo a estratégia definida e coordenada pelo CCR, em ambiente/cenário de Continuidade.

Obs:. As equipes poderão convidar pontualmente membros, internos ou externos, para a sua composição para tratamento dos eventos quando julgarem necessário.

Anexo II - Composição de Equipes e Demais Envolvidos

Identificação das equipes e áreas de atuação. A tabela abaixo demonstra as áreas, os participantes e suplentes:

Equipes	Área	Titular	Suplente
CCR - COMITE DE CRISE	CEO	Roberto Vidigal	Roberto Alem
	Risco	Marcello Vidigal	Anderson Machado
	Jurídico	Marcello Vidigal	Rafael Anthero
EOP - EQUIPE OPERACIONAL	Cadastro	Catherine Demori	Victor Lima
	Middle	Catherine Demori	Felipe Linhares
	Compliance	Marcello Vidigal	Pedro Lazzarini

Terceiros Relevantes

Outros contatos de Apoio	Front office	RB Capital DTVM S.A.
	Consultor Jurídico	Cepeda Advogados

Anexo III – Orientação para Avaliação e Acionamento da Contingência

1	Atividades de Qualificação do Incidente / Desastre
O Líder do CCR após a ocorrência de um incidente / desastre deverá avaliar os impactos, propor alternativas de continuidade dos serviços de TI e dos processos e dar todo suporte necessário que o CCR necessitar.	
1.1	Avaliar o ambiente operacional sinistrado e verificar o comprometimento da sua funcionalidade e possibilidades de recuperar e continuar, ou não, a operação no próprio local sinistrado;
1.2	Interagir com as áreas de infraestrutura predial e outras áreas da Maud visando buscar alternativas de continuidade do processamento, evitando a declaração de contingência;
1.3	Interagir com o CCR, discutindo alternativas reais de continuidade.

2	Atividades de Acionamento da Contingência
Após ser informada da declaração de contingência, o Líder do CCR deve executar a preparação para o início das atividades de restauração dos serviços de TI e/ou Work-Area*.	
2.1	Convocar os demais membros da EOP para início da restauração dos serviços de TI e sistemas, no Data Center Alternativo e/ou Work-Area*;
2.2	Participar de reunião, caso necessário, para alinhamento das ações entre as equipes e definição das próximas atividades;
2.3	Interagir com o CCR, discutindo alternativas reais de continuidade.

3	Atividades de Comunicação
O Líder do CCR deve manter comunicação diretamente com o CCR no processo de avaliação do incidente / desastre, durante a restauração dos ambientes operacionais e durante o todo período de contingência.	
3.1	Comunicar ao CCR o andamento das atividades de recuperação, as previsões de retorno e alternativas técnicas para atender a situação de contingência;
3.2	Comunicar para o CCR possíveis itens ou ações necessárias para o processo de restauração dos serviços e sistemas ou Work-Area*;
3.3	Comunicar o andamento dos serviços de restauração, testes e processamento da produção para o CCR.

4	Atividades de Execução e Acompanhamento da Contingência
O Líder do CCR deve dar suporte aos membros da EOP - executores das atividades necessárias para a recuperação das operações de TI e de negócios em contingência - e se reportar diretamente para a CCR.	
4.1	Dar suporte para as atividades de restauração;
4.2	Interagir com os membros da EOP visando garantir a execução do processo de contingência coordenado e completo;
4.3	Executar testes de funcionalidades dos ambientes operacionais, sempre que necessário, ou via Work-Area*;
4.4	Acompanhar os testes realizados pelas áreas usuárias na homologação e validação de seus processos de TI e de negócios, em contingência;
4.5	Após a validação do ambiente operacional de TI, no Data Center Alternativo e/ou Work-Area*, o Líder do CCR deve acompanhar a execução das rotinas de produção e dar suporte técnico, durante todo o período de contingência.

5	Atividades de Retorno
Após a recuperação do Data Center sinistrado, as equipes Técnicas participarão diretamente nas atividades de retorno para o Data Center Principal e Site Principal recuperado.	
5.1	Participar do processo de testes para homologação do Data Center Principal e Site Principal recuperado;
5.2	Participar no planejamento do retorno dos serviços de TI;
5.3	Executar as atividades planejadas que permitirão o retorno dos serviços de TI para o Data Center Principal e Site Principal recuperado;
5.4	Informar para as Equipes de CCR e EOP e para o Regulador, quando do término das atividades técnicas executadas, o retorno dos serviços de TI ao Data Center Principal e Site Principal recuperado.