

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

1. INTRODUÇÃO

A política de continuidade de negócios é um conjunto de procedimentos e medidas de segurança preventivas, previamente planejadas, a serem adotados após a ocorrência de uma falha para fazer com que processos vitais do negócio voltem a funcionar plenamente ou num estado minimamente aceitável, o mais rápido possível, assim evitando uma paralisação prolongada e consequente perda de receita, sanções jurídicas, governamentais, ou até mesmo o fechamento da empresa.

A política de continuidade de negócios concentra-se nos incidentes de maior probabilidade e não nos catastróficos que, estatisticamente, são menos prováveis de acontecer. A política de continuidade de negócios foi desenvolvida com o intuito de orientar e informar os funcionários da Collab Capital Gestora de Recursos S.A. – (“GESTORA”), o sobre todos os procedimentos e atividades que deverão ser realizados por cada colaborador durante uma situação de contingência, garantindo a maior eficiência possível da execução da política de continuidade de negócios, minimizando os impactos negativos causados pelo evento. A presente política está baseada nas melhores práticas de mercado para gestão da segurança da informação, e está de acordo com as leis, regulamentações e autorregulamentação vigentes, incluindo o Código ANBIMA de Regulamentação de Melhores Práticas para a Administração e Gestão de Recursos de Terceiros (“Código ANBIMA AGRT”).

2.POTENCIAIS EVENTOS E RISCOS

Contingência é definida como “Ação ou situação imprevista, que não se consegue controlar nem prever; eventualidade, casualidade”. As principais ameaças e eventos que podem levar a interrupção ou funcionamento anormal dos negócios são:

- Interrupção de serviços essenciais: falta de energia elétrica, baixa conectividade ou interrupção dos serviços de telefonia e internet;
- Falhas nos equipamentos, redes e sistemas de informação: vírus na rede, quebra de hardwares, falhas nos servidores ou softwares.
- Impossibilidade de acesso físico: greves, enchentes, distúrbios civis etc.
- Destruição das instalações: incêndio, desmoronamento e outros.

3. PROCEDIMENTOS

Interrupção de Serviços Essenciais

O procedimento de contingência caso haja interrupção de algum serviço essencial - tal como energia, telefone etc., será feito com base nas capacidades e limitações internas existentes (exemplo: autonomia dos nobreaks e baterias), assim como em estimativas e previsões realizadas pelo provedor do serviço, administração do condomínio ou responsável e TI da GESTORA para que o serviço volte a funcionar normalmente. Caso a estimativa para solução do problema ou a GESTORA esteja operando fora da normalidade durante mais de 40 minutos será automaticamente decretada contingência e os funcionários da GESTORA deverão se reunir e preparar para o deslocamento até a CONTINGÊNCIA.

Falhas nos equipamentos, redes e sistemas de informação

O procedimento de contingência caso haja falhas nos equipamentos, redes e sistemas de informação será realizado de acordo com a gravidade do problema (exemplo: vírus na rede interna, quebra do servidor etc.) e estimativas responsável pela área e TI da GESTORA ou suporte técnico para que o serviço volte a funcionar normalmente. Em hipótese da previsão para volta da normalidade seja superior a 30 minutos e todas as estações de trabalho assim como a rede interna estejam comprometidas ou impossibilitadas de operar, será, automaticamente, decretada contingência e os funcionários da GESTORA deverão se reunir e preparar para o deslocamento até a CONTINGÊNCIA.

Caso o problema seja restrito somente a algumas estações de trabalho a contingência será realizada pelo suporte de TI da GESTORA que colocará o funcionário em um dos terminais/computadores disponíveis para contingência.

Impossibilidade de acesso físico e Destruição das instalações

Nestas duas situações de contingência há a necessidade de acionamento da CONTINGÊNCIA, cabendo aos responsáveis por declarar a contingência a comunicação com os funcionários, orientando os membros da equipe de contingência a se dirigirem

diretamente à CONTINGÊNCIA.

4. SITE DE CONTINGÊNCIA

A escolha do site foi realizada ponderando-se inúmeros fatores tais como localização, facilidade de acesso, segurança, disponibilidade de equipamentos e recursos tecnológicos, qualidade dos serviços etc. A GESTORA optou pela estruturação de sua contingência no seguinte endereço:

O endereço da contingência: Alameda Campinas, 802 - Jardim Paulista, Sala 21 - São Paulo - SP, 01404-001;

Nesta situação, a separação da área de gestão de fundos, será isolada das demais, conforme política de segregação de funções e confidencialidade de informações.

No Backup Site é possível acomodar e utilizar os seguintes recursos de sistemas necessários:

- 4 posições de contingência com especificações padrões de tecnologia;
- Internet banda larga, tanto para uso da contingência quanto para comunicação com a GESTORA
- Telefones e linhas para ligações externas.
- 2 notebooks configurados com Windows 11 PRO
- Acesso aos sistemas necessários para dar continuidade às operações

5. SISTEMA DE CONTINGÊNCIA

A GESTORA possui como contingência:

- Backups diário de dados realizado na NUVEM.
- 2 links dedicados de internet,
- Nobreaks em todos os computadores (estações de trabalho) e no servidor com possibilidade de incluir bateria externas. Cada estação de trabalho possui bateria interna com autonomia estimada acima de 1 horas.
- Acesso a armazenamento em nuvem.
- Máquinas e equipamentos reservas.

O edifício onde a GESTORA está localizada na Alameda Campinas, 802 - Jardim Paulista, Sala 21 - São Paulo - SP, 01404-001, possui gerador somente para a operação dos elevadores, contudo, o escritório da GESTORA conta com nobreaks que garantem energia por tempo suficiente para a continuidade das operações e para que todos os colaboradores possam se deslocar para o home office, garantindo a implementação do plano de contingência sem interrupções significativas.

6. DECLARAÇÃO DE CONTINGÊNCIA

Independente da situação de contingência (interrupção de serviços essenciais; falhas nos equipamentos, redes e sistemas de informação; impossibilidade de acesso físico; destruição das instalações) a declaração de contingência deverá ser feita de 2 formas:

- E-mail: O e-mail deverá ser enviado para todos os funcionários da GESTORA; no campo assunto colocar “Declaração de Contingência”.

- Telefone: Ligar para todos os sócios da GESTORA e informar sobre a contingência. Os funcionários abaixo relacionados estão autorizados a Declarar Contingência e integrarão a Equipe de Contingência da GESTORA caso seja necessário executar a política de continuidade de negócios:

    - Fabrício Oliveira — Diretor de Gestão de Investimentos;
    - Lucas Aragão — Diretor de Compliance e PLD-FT;
    - Tiago André Piccoli — Diretor de Gestão de Riscos.

7. PROCEDIMENTOS APÓS DECLARADA CONTINGÊNCIA

Reunir “Equipe em Contingência”

Os responsáveis em declarar contingência estarão encarregados de reunir e informar todos os funcionários da GESTORA escolhidos para o plano de contingência para se organizar e se prepararem para o deslocamento até o local da CONTINGÊNCIA. Caso a situação de contingência seja do tipo impossibilidade de acesso físico ou destruição das instalações e os funcionários da GESTORA estejam dispersos (em trânsito, na residência etc.) estes deverão ser contatados e informados via telefone (preferencialmente) ou e-mail.

Acesso e login

Os notebooks da contingência encontram-se em local de fácil acesso. Uma vez acomodado em sua respectiva estação de trabalho com os notebooks conectados à internet cada funcionário poderá efetuar o login e terá acesso aos recursos pré-configurados para execução normal dos trabalhos.

Acesso ao Webmail: O acesso ao e-mail de cada usuário deverá ser realizado via internet por meio de site ou celular via dados.

Banco de Dados: O servidor da GESTORA, realiza um backup diário das informações à meia-noite. Dessa forma, as informações na

NUVEM estarão atualizadas até o dia anterior (D-1).

a. Softwares e Programas: Há uma série de programas e softwares usados diariamente pelos funcionários da GESTORA que são críticos para o desenvolvimento de suas atividades.

8. SUPORTE TÉCNICO

Os serviços de suporte técnico contratados serão atendidos de acordo com o nível de severidade, impacto na condição operacional e expectativa de prazo máximo de atendimento, segundo a tabela:

Nível de Severidade Conceito de Severidade Prazo de Atendimento:

1. Software ou hardware sem condições de funcionamento: Imediato
2. Problema de conectividade que afeta a condição operacional: Até 2 horas
3. Problema de hardware e software que não afeta a condição operacional: Até 12 horas
4. Suporte técnico: Nome da Empresa de T.I / Nome do Responsável

9. AVALIAÇÃO, TESTES E REVISÃO

A GESTORA realizará um treinamento uma vez por ano que simulará uma situação de contingência real. Este treinamento será realizado na própria Contingência e seu principal objetivo é avaliar todos os procedimentos e situações buscando identificar os pontos fracos, dificuldades e questões que podem afetar a eficiência do Plano de Contingência. Cabe ao responsável pela TI, a revisão semestral de todos os equipamentos de nobreak, certificando-se que são respeitadas as autonomias mínimas definidas acima. Este procedimento contempla a avaliação e substituição de todos os equipamentos que estejam com sua autonomia afetada ou comprometida por desgaste natural, falhas etc. A revisão será formalizada através de relatório, que deverá apontar os equipamentos revisados, problemas detectados e prazo para correção das falhas. A área de Compliance deverá manter em seus arquivos cópia desse relatório.

Com relação às informações e ao servidor localizados na NUVEM, estes serão avaliados e testados pelos membros da equipe de TI.

O Plano de Contingência será revisado trimestralmente de maneira que esteja sempre adequado e atualizado a todas as necessidades e atividades desenvolvidas pelos funcionários da GESTORA.

10. CONSIDERAÇÕES FINAIS

A presente política está em constante evolução, concebida com o objetivo primordial de fortalecer o plano de continuidade de negócios a fim de mitigar as prováveis falhas operacionais da gestora. Sua importância transcende o âmbito institucional, pois está intrinsecamente ligada à salvaguarda da integridade do sistema financeiro e à contenção de atividades criminosas. Este é estabelecido sobre os pilares da conformidade estrita com as normas regulatórias vigentes e da adesão irrestrita às diretrizes estabelecidas pelos órgãos autorreguladores competentes.

CONTROLE E REVISÃO

Controle e Revisão de Informações Gerais		
Aprovado por:	**Data de Aprovação:**	**Alteração**
Diretor de Gestão de Riscos e Diretor de Compliance/PLD-FT	13/08/2026	Versão Inicial