PLANO DE CONTINUIDADE DE NEGÓCIO

iVi Technologies

Versão 2

Novembro de 2023

Sumário

CONTROLE DE VERSÕES

Versão	Data Revisão	Revisor
1	Dezembro de 2021	Versão Inicial
2	Novembro de 2023	Lendel Augusto Vaz Lucas

1. Objetivo

O Presente Plano de Continuidade de Negócio tem por objetivo estabelecer as medidas a serem tomadas para identificar e prevenir as possíveis contingências que poderão trazer um impacto negativo considerável sobre a condução das atividades da iVi Capital Management. Dentre estas contingências se incluem, por exemplo, crises econômicas, falhas operacionais ou desastres naturais. O presente documento visa ainda, atender ao disposto artigo 15 do Código de Administração de Recursos de Terceiros, da Anbima.

A iVi por meio do presente Plano de Continuidade de Negócio buscará sempre identificar e prevenir os riscos relacionados ao seu negócio sejam eles físicos, patrimoniais ou financeiros.

2. Diretrizes para Prevenção e Tratamento de Contingências

Para a eficaz implementação deste Plano, a iVi buscará conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para tal finalidade tomará medidas que a permitam:

a. Conhecer e minimizar os danos no período pós-contingência;
b. Minimizar as perdas para si, seus clientes e Colaboradores advindos da interrupção de suas atividades; e
c. Normalizar o mais rápido possível as atividades de gestão.

3. Análise de Riscos Potenciais

- Risco Cibernético
- Risco de falha na rede de internet e a consequente falta de acesso por parte dos membros da Gestora, sejam eles da área de gestão de recursos ou da área de compliance e controles internos;
- Risco de problemas internos na nuvem que nos impossibilite o acesso aos diretórios no Google Drive.
- Falha no acesso aos sistemas dos administradores/distribuidores;
- Outros, não identificados até a presente data.

4. Plano de Contingência

- Com relação ao risco cibernético, deveremos seguir o disposto na Política de Cibersegurança da IVI Technologies. Além disso, nós temos uma equipe de T.I que está preparada para atuar, tanto na prevenção quanto ativamente, caso venhamos a ser alvos.
- Atualmente estamos preparados para trabalhar de forma 100% remota e todos os membros da empresa possuem um login e senha para acesso aos sistemas, diretamente de casa, ou outro local considerado seguro, de forma que, na hipótese de ocorrência dos eventos acima, especialmente o que diz respeito à falta de acesso à internet, todos os membros da Gestora podem trabalhar remotamente, até que a falha seja sanada. O acesso às pastas e documentos da Gestora é feito via Google Drive e cada membro possui seu devido acesso, com as devidas permissões.
- São feitos ainda backups de todos os dados que estão no Google Drive anualmente, de forma que na ocorrência de qualquer problema no drive, temos uma cópia salva em um drive externo, nos possibilitando a recuperação dos arquivos e informações em caso de algum problema.
- Na hipótese de não conseguirmos acesso aos sistemas dos Administradores/Distribuidores, caso os mesmos estejam com algum problema interno, os respectivos Administradores/Distribuidores ou demais prestadores de serviço relevantes para a operação da nossa Gestora deverão ser notificados da falha no acesso, **de imediato**, e os diretores da IVI Capital deverão também ser comunicados de forma imediata.
- Todos os membros da IVI Capital Management estão instruídos a informar aos demais, caso identifique qualquer dos problemas identificados acima e deverão informar especialmente aos diretores das áreas, de forma que seja identificada a melhor maneira de tratar da possível falha e seja analisado o plano de contingência adequado para o problema.

5. Tratamento das Contingências Operacionais

Um Plano de Contingência é uma ação preventiva, que visa prover a empresa de procedimentos, controles, responsabilidades e regras, permitindo a continuidade das

operações de suas áreas de negócio após eventuais ocorrências que impossibilitem a sua utilização, parcial ou total.

Caberá à Área de Compliance assegurar a implementação do plano de contingência no caso da materialização dos eventos descritos no item anterior, assegurando, também, a realização de testes (anuais) que atestem sua efetividade.

Para o tratamento das contingências diretamente relacionadas com a operação dos negócios da iVi, deverão ser mantidos sempre atualizados procedimentos que permitam:

d. Aumentar rapidamente seu contingente de pessoal técnico qualificado e/ou fornecedores caso a demanda por seus serviços aumente rapidamente sem que isso implique na queda da qualidade da prestação dos serviços;
e. Identificar novos potenciais mercados de atuação e/ou produtos caso haja queda, ou longos períodos de recessão, na demanda de seus clientes atuais;
f. Manter-se sempre competitiva e inovadora, de forma a evitar a perda de sua participação no mercado, com a exploração de seus pontos fortes e com a constante diminuição de seus pontos fracos;
g. Manter um fluxo de caixa que, à critério da diretoria, seja hábil para fazer frente à despesas imprevisíveis.
h. Na hipótese de impedimento do gestor de recursos de terceiros de continuar a exercer às suas atividades a gestora possui no seu quadro de sócios, outros gestores credenciados na CVM capazes de substituir de imediato esse diretor.
i. Em caso de impedimento de qualquer prestador de serviço, a iVi deve manter relacionamentos com outras instituições financeiras que poderão vir a substituir a atual.

Para tanto, a iVi Technologies adota as seguintes ações:

I. Backup das planilhas e bancos de dados operacionais;

II. Manutenção de uma lista em local de fácil acesso com o telefone dos fornecedores de sistemas e nomes das pessoas chave para solucionarem os problemas no menor tempo possível;

III. Plano alternativo de comunicação;

IV. Espaço operacional alternativo: Eventualmente, em havendo a impossibilidade em se utilizar o escritório sede, os diretores terão como ponto de encontro oficial a residência do Diretor de Administração de Carteira, para assim deliberarem sobre o plano de trabalho. O fato da iVi Technologies manter todos os arquivos hospedados na nuvem através do sistema GoogleDrive, permitirá com que todos os membros continuem tendo

acesso aos arquivos normalmente, podendo desempenhar plenamente suas funções de forma remota; e

V. Plano para substituição de pessoal em caso de saída: documentação de informações, redistribuição de tarefas, contratação de novo funcionário ou realocação interna.

6. Riscos Não Identificados

Em nossos processos diários, a equipe de risco e compliance, bem como a equipe de gestão de recursos, são orientados a, na hipótese de identificarem algum risco novo ou ainda não identificado, relacionado ao nosso negócio, informar aos respectivos diretores para que seja elaborado um plano de prevenção/ação e a consequente atualização desta política.

7. Disposições Finais

Conforme disposto no Código Anbima de Administração de Recursos de Terceiros, “Validações ou testes, deverão ser feitos, no mínimo a cada 12 (doze) meses, ou em prazo inferior se exigido pela Regulação em vigor”.