

**VKN ADMINISTRAÇÃO DE RECURSOS LTDA.**

**PLANO DE CONTINGÊNCIAS  
E CONTINUIDADE DO NEGÓCIO**

**Julho / 2021**

## **DISCLOSURE**

**O presente PLANO DE CONTINGÊNCIAS E CONTINUIDADE DO NEGÓCIO é propriedade da VKN Administração de Recursos Ltda.**

**É proibida a cópia, distribuição ou uso indevido deste documento sem expressa autorização da VKN Administração de Recursos Ltda.**

## **1. Introdução e Objetivos**

Pelo presente documento, a VKN Administração de Recursos Ltda. ("VKN") tem o objetivo de definir os procedimentos aplicáveis a sua equipe em caso de contingência, de modo a impedir descontinuidade operacional por problemas que impactem no funcionamento da VKN. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da VKN sejam previamente identificados, e preservados mesmo na ocorrência de um imprevisto ou um desastre.

O modo contingencial será acionado quando for identificada qualquer ocorrência ou situação que dificulte ou impeça a rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, aos clientes da VKN e à própria VKN.

O conjunto de ações a serem tomadas quando uma situação dessas ocorre é chamado de Plano de Contingência.

O Plano de Contingência é compartilhado com todos os colaboradores da VKN e faz parte da sua cultura. Os colaboradores são preparados para exercer suas funções em situações contingenciais e dessa forma os impactos serão minimizados.

## **2. Princípios Norteadores**

A VKN, pautada pelos deveres de diligência e cuidado e pela respeitabilidade que norteiam a condução dos seus negócios, em casos de ocorrência de quaisquer eventos ou sinistros que possam inviabilizar, paralisar ou comprometer temporariamente o exercício de suas atividades seguirá os procedimentos aqui definidos ou, nos casos não previstos neste plano, os procedimentos estabelecidos pela sua diretoria.

A VKN por meio do presente Plano de Contingências buscará sempre saber de antemão quais os riscos relacionados ao seu negócio, sejam eles físicos, patrimoniais ou financeiros.

## **3. Diretrizes na Prevenção e Tratamento das Contingências**

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

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

#### 4. Estrutura

Para atendimento às necessidades mínimas de manutenção dos serviços/atividades da VKN, foi definida uma estrutura mínima física e procedimentos que devem ser adotados toda a vez em que uma situação que caracterize uma contingência às operações da VKN seja identificada.

Foram identificadas as seguintes áreas/atividades que necessitam estar contempladas no Plano de Contingência de forma a garantir o funcionamento da VKN:

- (i) **TI:** fundamental para o funcionamento da VKN, no sentido de que todas as comunicações com corretoras, administradores de fundos etc., são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios). Também é fundamental para a realização de registros de operações (compras e vendas de títulos, aplicações e resgates em fundos de investimento, clubes de investimentos ou carteiras administradas, transferência de recursos e pagamento de despesas da VKN, dentre outros);
- (ii) **Escritório:** espaço físico onde são realizadas as operações da VKN. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades; e
- (iii) **Pessoal:** pessoas responsáveis pela operação da VKN, incluindo a análise e decisão para realização ou não de investimentos, equipe responsável pelo compliance e pela gestão de risco das carteiras etc.

Tendo identificado essas 3 (três) áreas principais do ponto de vista da estrutura da VKN e dos processos sob sua responsabilidade, os riscos que podem ocasionar o acionamento do Plano de Contingência foram identificados da seguinte forma:

- **Problemas de Infraestrutura:** os problemas dessa ordem são, dentre outros, falha e/ou interrupção no fornecimento de serviços essenciais como a falta de energia elétrica, falta de água, falha nas conexões de rede, falha nos links de internet, falha nas linhas telefônicas, falhas nos sites das empresas que fornecem sistemas de uso da VKN, etc.; e
- **Problemas de acesso ao local/recursos:** os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso ao local onde se localiza o escritório. Essa impossibilidade pode ser causada por eventos como greves, por exemplo de transporte público, interdições pelas autoridades do prédio ou do entorno do escritório da VKN, etc.

Com base no levantamento da estrutura da VKN e no mapeamento de riscos, a VKN tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações.

Conforme avaliação de risco da VKN foram definidos 2 (dois) ambientes básicos que devem ser considerados nas ações a serem tomadas quando da ativação do presente Plano de Contingência. Esses ambientes são: Físico e o Tecnológico.

#### **4.1. Ambiente Físico**

O ambiente físico é definido como o espaço onde as operações diárias da VKN são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e equipamentos necessários a essa operação, como também o acesso seguro a esses recursos.

Em ocorrendo situações de problemas de acesso às suas dependências, a equipe da VKN deve continuar a desempenhar suas atividades através de Home Office, uma vez que os arquivos relativos às atividades dos Colaboradores podem ser acessados pela nuvem. Além disso, há a vinculação dos e-mails e armazenamento no Microsoft Office Business Premium 365, para que os Colaboradores sigam as instruções da equipe de contingência sobre como agir, ou seja, permanecer trabalhando através de Home Office. Adicionalmente, os Colaboradores podem ainda acessar remotamente os sistemas dos administradores fiduciários dos Veículos de Investimento.

Os equipamentos mínimos necessários para a manutenção das funcionalidades em caráter contingencial são: (i) 1 Núcleo de processador; (ii) 3.5 Gb Ram; (iii) 100 GB de espaço em disco; (iv) Windows 7, 8 ou 10; (v) Internet de 4 Mb ou superior.

#### **4.2. Ambiente Tecnológico**

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a VKN possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela empresa em seu dia a dia e garantia de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da VKN, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, softwares e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

Todos os sistemas utilizados pela VKN são acessados através de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da VKN. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência da VKN, de forma a que também estes tenham conhecimento da situação, de forma a impactar o mínimo possível a operação da VKN.

Na prestação de serviços de Tecnologia da Informação, a VKN utiliza-se dos serviços de tecnologia da informação da *Processor*, a qual é responsável pela assessoria relativa ao *software* Microsoft Office Business Premium 365, ao provedor de e-mails e ao armazenamento de dados da VKN na nuvem. Adicionalmente, a VKN também conta com os serviços de colaboradores de empresa do grupo econômico da VKN, os quais estão 100% disponíveis na hipótese de uma situação de contingência, sendo responsáveis pela assistência em quaisquer questões envolvendo os sistemas operacionais, as rotinas de backup, a rede e os servidores da VKN.

A primeira rotina de backup envolve a realização permanente de backup dos arquivos mantidos no armazenamento do OneDrive dentro do serviço da Microsoft Office Business Premium 365, onde é mantido um histórico de até 500 versões de cada arquivo, e os arquivos excluídos podem ser recuperados por até 93 (noventa e três) dias. Além disso, semanalmente os arquivos armazenados no OneDrive são copiados em um disco externo. A segunda rotina de backup é realizada no âmbito do diretório de arquivos internos da VKN, em periodicidade semanal, feita de forma remota e armazenada em local externo.

Com relação ao armazenamento de e-mail, os mesmos estão hospedados e armazenadas dentro do serviço do Microsoft Office Business Premium 365, sendo que as mensagens excluídas são recuperáveis por até 14 dias após serem excluídas.

Adicionalmente, o backup só deve ser restaurado em caso de deleção, problema de corrupção ou edição incorreta. Em caso de restauração do backup, o colaborador deve validar os dados recuperados e prosseguir com as atividades. Caso haja alguma inconsistência na recuperação dos dados, o Coordenador de Contingência (conforme definido abaixo) deve ser comunicado imediatamente para que providências sejam tomadas em relação à nova restauração de dados.

#### **4.3. E-mail**

A VKN utiliza um serviço de e-mail em cloud (nuvem) na modalidade de Software as a Service (SaaS) oferecido pela Microsoft Exchange online Office 365. O serviço de e-mail pode ser acessado diretamente pela web através de senha. O Exchange Online protege as informações das caixas de correio utilizando recursos avançados, tais como: filtros *antimalware* e *antispam*, assim como a prevenção contra perda de dados. Os servidores possuem redundância global e recursos avançados de recuperação em caso de desastres.

Além disso, para garantir o funcionamento ininterrupto do serviço de e-mail, a Microsoft oferece uma disponibilidade de 99,9%.

## **5. Equipe De Contingência**

Para coordenar todas as ações necessárias em situações de contingência bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da VKN, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance, Risco e PLD (Coordenador de Contingência); e
- Diretor de Gestão.

Essas pessoas deverão tomar as decisões necessárias para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, na ausência de um dos diretores, isoladamente e deve ser comunicada imediatamente a todos os colaboradores da VKN. O Coordenador de Contingência entrará em contato (ou pedirá para o Diretor de Gestão entre em contato) com a *Processor* e com os colaboradores da equipe da empresa do grupo econômico da VKN responsável pela assessoria aos assuntos de Tecnologia da Informação da VKN, para comunicar o modo contingencial e tratar do acesso aos dados/sistemas, bem como efetuar o desvio das ligações dos telefones do escritório para linhas alternativas.

## **5. Cenários De Contingência**

A ocorrência de eventos de contingência deverá ser avaliada pela Equipe de Contingência da VKN e, com base nas informações disponíveis, deverá ser tomada uma decisão quanto ao acionamento do Plano de Contingência.

Com base na decisão tomada pela Equipe de Contingência, a VKN deverá adotar os procedimentos a seguir listados.

### **5.1. Situação de Contingência**

Neste cenário, considera-se basicamente a impossibilidade ou dificuldade em manter o funcionamento normal da VKN devido a problemas de ordem técnica (*hardware*), física (acesso ao escritório), pessoal (ausência significativa de funcionários) e de infraestrutura (falta de energia).

Nessa situação, o Diretor de Compliance, Risco e PLD da VKN deverá acionar este plano, em caráter imediato, e iniciar também imediatamente a avaliação das causas que geraram a contingência para providenciar sua solução o mais rapidamente possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo, quais sejam:

(a) Comunicar imediatamente o ocorrido à toda a equipe interna, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição, indicando nessa oportunidade qual o procedimento a ser adotado por cada colaborador de acordo com a contingência ocorrida;

(b) Caso seja verificada a necessidade de sair do escritório da VKN, os colaboradores poderão continuar a desempenhar suas atividades através de Home Office, uma vez que todos os arquivos podem ser acessados pela nuvem. Em havendo necessidade, a equipe da VKN irá se reunir no Escritório de Contingência localizado na residência de um dos Diretores da VKN que dispõe de ambiente e infraestrutura para tanto e prosseguirá com a gestão remota dos fundos sob sua administração. A continuidade das operações da VKN deverá ser assegurada no próprio dia útil da ocorrência da contingência no escritório físico, de modo que as atividades diárias não sejam interrompidas ou gravemente impactadas.

O Diretor de Compliance, Risco e PLD da VKN deverá acompanhar todo o processo acima descrito até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela VKN e reportar eventuais alterações e atualizações da contingência aos demais colaboradores.

## **6. Aspectos Gerais**

O presente Plano de Contingência é de uso restrito dos colaboradores da VKN e não pode ser divulgado para terceiros, exceto se autorizado pela Equipe de Contingência.

É responsabilidade do Diretor de Compliance, Risco e PLD manter este Plano atualizado, bem como realizar a validação, a cada 12 (doze) meses, dos procedimentos estabelecidos neste Plano de Contingência.

Ainda, o Diretor Compliance, Risco e PLD realizará testes de contingências que possibilitem que a VKN esteja preparada para eventos desta natureza, proporcionando à VKN condições adequadas para continuar suas operações.

Sendo assim, anualmente, é realizado um teste de contingência para verificar:

- a) Acesso aos sistemas;
- b) Acesso ao e-mail corporativo;
- c) Acesso aos dados armazenados; e
- d) Qualquer outra atividade necessária para continuidade do negócio.



O resultado do teste é registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

## **7. Vigência e Atualização**

Este plano será revisado anualmente, podendo ser alterado sempre que necessário. As novas versões serão divulgadas para todos os sócios e colaboradores pelo Diretor de Compliance, Risco e PLD.

## 8. Histórico das Atualizações do Plano de Contingência.

<b>Data</b>	<b>Versão</b>	<b>Responsáveis</b>
Dezembro/2018	1.0	Diretor de Gestão e Diretor de Compliance, Risco e PLD
Julho/2019	2.0	Diretor de Gestão e Diretor de Compliance, Risco e PLD
Julho/2020	3.0	Diretor de Gestão e Diretor de Compliance, Risco e PLD
Julho/2021	4.0	Diretor de Gestão e Diretor de Compliance, Risco e PLD

\* \* \*