PLANO DE CONTINUIDADE DE NEGÓCIOS

1. OBJETIVO

1.1. Este documento estabelece o Plano de Continuidade de Negócios ("PCN" ou "Plano") da Nikos Gestão de Recursos Ltda. ("Gestora") com o objetivo de assegurar a manutenção ou o restabelecimento tempestivo das atividades críticas da instituição em cenários de crise, falhas operacionais relevantes, desastres naturais, indisponibilidade de infraestrutura ou quaisquer outros eventos que possam impactar significativamente a continuidade dos negócios. Este PCN observa as diretrizes da Comissão de Valores Mobiliários ("CVM") e a autorregulação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA").

2. ABRANGÊNCIA

2.1. Aplica-se a todos os colaboradores da Gestora. Para fins desta Plano, são entendidos como colaboradores, os diretores, funcionários estagiários e terceiros contratados para a prestação de serviços nas dependências da Gestora.

3. INTRODUÇÃO

3.1. Diversos eventos de natureza interna ou externa podem comprometer a continuidade operacional da Gestora, incluindo, mas não se limitando a: pandemias, inundações, incêndios, sabotagem, vandalismo, greves, bloqueios logísticos, ameaças de bomba, quedas de energia, furtos e roubos de ativos físicos ou informações, falhas de software crítico, indisponibilidade de sistemas, e falhas em equipamentos de telecomunicação ou componentes de rede.

3.2. A depender da gravidade e extensão desses eventos, há o risco de materialização de perdas financeiras relevantes, danos à reputação institucional e descumprimento de obrigações regulatórias, contratuais ou operacionais.

3.3. Diante disso, o PCN da Gestora estabelece um conjunto estruturado de diretrizes, responsabilidades, processos e estratégias de resposta voltados à mitigação dos impactos de interrupções, assegurando o restabelecimento das operações críticas dentro de prazos previamente definidos como aceitáveis, com foco na proteção dos interesses dos clientes, da integridade do mercado e da própria instituição.

3.4. Como um dos pilares centrais do PCN, está prevista a ativação de regime de trabalho remoto, com recursos tecnológicos e operacionais adequados, garantindo a continuidade das atividades essenciais mesmo em situações de indisponibilidade física da sede ou das unidades de apoio

3.5. Para fins de atuação rápida e eficiente, o PCN foi segmentado em dois cenários distintos: (i) ocorrências identificadas fora do horário regular de expediente (antes do início ou após o encerramento das atividades); e (ii) ocorrências durante o expediente, quando há colaboradores em atividade, exigindo protocolos específicos de resposta emergencial e comunicação.

3.6. O PCN também aborda: (a) os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem; e (b) o tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

4. INFORMAÇÕES BÁSICAS

4.1. Recursos disponibilizados. Em caso de contingência, os colaboradores da Gestora possuem acesso a notebooks corporativos já configurados para acesso remoto. Dessa maneira, todos os sistemas são acessíveis por um canal seguro de comunicação, mesmo conectados a redes particulares.

4.1.1. Cada estação de trabalho possui cliente VPN, com duas configurações, onde a primeira se conecta ao *firewall* da sede da Gestora na cidade e estado do Rio de Janeiro.

4.1.2. A Gestora utiliza sistema de computação em nuvem que realiza o armazenamento dos dados em servidores externos terceirizados. Esses dados são replicados em diferentes regiões e, em caso de falha, é possível a restauração. Além disso, existe um backup diário da base de dados, por tempo indeterminado.

4.1.3. O sistema de arquivos corporativo possui backup na nuvem. O backup é realizado de forma automática com controle de versão e mecanismo que permite a recuperação de dados.

4.1.4. Nesse sentido, no caso de contingência, o acesso aos dados e informações da Gestora será imediato, podendo ser ativado pelos colaboradores de qualquer local.

4.1.5. Todo o ambiente colaborativo da Gestora é baseado em cloud, não sendo necessárias infraestruturas onpremisses.

4.2. Responsável pela ativação do Plano. O Diretor de Compliance e Risco será o responsável pela ativação, coordenação, fiscalização e monitoramento do presente Plano, atuando, para todos os fins, como "Coordenador de Contingência".

4.2.1. O Coordenador de Contingência deverá ser procurado por qualquer Colaborador da Gestora em caso de dúvidas e/ou necessidade de maiores esclarecimentos sobre os procedimentos aqui descritos.

4.3. Colaboradores da Gestora. Os colaboradores da Gestora deverão se apresentar online por meio de conexão segura (VPN), de acordo com o seu horário de trabalho, e aguardar orientação do Coordenador de Contingência**.**

5. 5. PROCEDIMENTOS DE ACIONAMENTO DA CONTINGÊNCIA

5.1. O Coordenador de Contingência, em conjunto com o Diretor de Gestão, deverá avaliar a ameaça e decidir ou não pelo acionamento da contingência.

5.2. O PCN está dividido em dois momentos (i) ocorrências antes do início ou após o fim do expediente; e (ii) ocorrências durante o expediente, impossibilitando o acesso as dependências da Gestora, devido a, dentre os motivos:

i. inundações;

ii. pandemia;

iii. incêndio ou seu princípio;

iv. outros fatores como ameaça de bomba, roubo ou vandalismo;

v. interrupção do fornecimento de energia elétrica;

vi. Greves, ausências súbitas ou incapacidades de pessoal-chave;

vii. indisponibilidade total do ambiente de produção localizado no Data Center principal (sistemas e conexões); e

viii. indisponibilidade total do ambiente de produção do ambiente em nuvem (sistemas e conexões).

5.3. A decisão do acionamento da contingência deverá ocorrer, no máximo, até 1 (uma) hora após a evidência de ameaça.

5.4. Dependendo da situação, o Coordenador de Contingência contatará o Diretor de Gestão da Gestora para decidirem, em conjunto, sobre o acionamento ou não da contingência.

5.5. Se decidirem pelo acionamento, o Coordenador de contingência acionará os colaboradores, orientando-os para que se dirijam e/ou permaneçam em suas residências.

5.6. Dado que o todo o operacional da Gestora é realizado por meio da tecnologia, incluindo sistemas, e-mails, comunicações internas e externas etc., todos os sistemas utilizados possuirão a possibilidade de serem acessados de maneira remota, desde que possuam acesso à internet.

5.7. Os Colaboradores da Gestora podem continuar desempenhando as suas tarefas diárias através de home office, considerando que a sociedade possui sistema em nuvem para armazenamento de seus arquivos e e-mails.

5.8. No caso de interrupção do fornecimento de energia elétrica, se a previsão de restabelecimento do fornecimento ultrapassar o período de 2 (duas) horas, a decisão do acionamento da contingência poderá ser imediata. Para esses casos o Coordenador de Contingência contatará a concessionária para obter a previsão de restabelecimento do fornecimento da energia, além das tratativas mencionadas acima.

5.9. Independentemente da ameaça, o tempo de tolerância para retomada dos processos e atividades da Gestora é de até 2 (duas) horas após a tomada de decisão sobre o acionamento da contingência.

5.10. Os procedimentos para recuperação de indisponibilidade total do Data Center principal e do ambiente de nuvem deve estar no documento técnico sendo o acesso para edição restrito ao Coordenador de Contingência e ao Diretor de Gestão.

6. COMUNICAÇÃO AOS CLIENTES E ENTIDADES REGULADORAS

6.1. No que se refere às obrigações de comunicação aos clientes e entidades reguladoras, a Gestora se compromete a notificar autoridades, inclusive à CVM, à B3, à Autoridade Nacional de Proteção de Dados ("ANPD"), parceiros comerciais, titulares de dados pessoais, clientes, instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil ("BCB"), quando aplicável e desde que não sejam informações protegidas por sigilo, sobre os casos de interrupção dos processos críticos de negócio da Gestora, e sobre os incidentes que tenham potencial ou comprovado comprometimento de dados dos clientes, parceiros, colaboradores, ou quaisquer titulares de dados pessoais tratados pela Gestora, na forma da legislação vigente, ou em não mais que 48 (quarenta e oito) horas após a conclusão da investigação do evento.

7. RETORNO À NORMALIDADE

7.1. Será de responsabilidade do Coordenador de Contingência assegurar que as operações da Gestora voltem a normalidade no mesmo dia útil em que ocorrer a ativação desse Plano, buscando assim, evitar que sejam causados maiores danos aos trabalhos executados pela Gestora, devendo acompanhar todo o cenário de contingência de forma próxima.

7.2. Após o restabelecimento das instalações da sede da Gestora, o Coordenador de Contingência irá analisar, em conjunto com o Diretor de Gestão, qual o melhor momento para que os colaboradores retornem às atividades normais.

7.3. A partir da definição acima, o Coordenador de Contingência deverá instruir os colaboradores quanto aos procedimentos necessários para o retorno.

7.4. Verificado o retorno da normalidade, o Coordenador de Contingência elaborará para a Diretoria da Gestora relatório acerca do ocorrido e se houve algum prejuízo a Gestora, de forma que sejam mapeados os pontos não satisfatórios e corrigidos, visando mitigar os riscos de uma futura contingência, contendo dentre os pontos supramencionados:

i. data da ameaça;

ii. tipo da ameaça;

iii. danos causados;

iv. tempo de parada;

v. providências tomadas;

vi. horário inicial da contingência;

vii. tempo de tolerância para retomada dos processos essenciais;

viii. término da contingência; e

ix. data de retorno ao site principal, se aplicável.

8. PÁGINA PRINCIPAL DO PORTAL

8.1. Em situações em que a contingência for acionada, os canais de atendimento da Gestora permanecerão disponíveis aos cotistas dos fundos por meio dos recursos digitais implementados pela instituição.

8.2. O contato com os cotistas será realizado por meio de e-mail institucional e, quando necessário, por atendimento humano realizado pelos canais disponíveis.

8.3. Caso, em situações excepcionais, haja necessidade de restabelecimento de canal alternativo de contato, será disponibilizada, na página principal do portal da Gestora (**www.nikosgestao.com.br**), comunicação com orientações aos cotistas, incluindo, se aplicável, a indicação de canal temporário de suporte.

9. 9. TESTE DE CONTINGÊNCIA

9.1. Anualmente, o Coordenador de Contingência deverá realizar um Teste de Contingência para verificação do funcionamento do PCN em caso de situações reais de necessidade de sua utilização ("Teste de Contingência").

9.2. O Teste de Contingência envolve a simulação de uma situação de crise ou contingência para avaliar a resposta da Gestora diante do ocorrido, e seguirá os seguintes aspectos:

i. Ativação do Plano: deverá ser realizada a ativação do Plano, mediante a definição e execução de cenário previamente estabelecido;

ii. Comunicação Interna: deverá ser realizada a comunicação aos colaboradores acerca do início do Teste de Contingência, por meio dos canais internos disponíveis, incluindo, mas não se limitando a e-mail e telefone;

iii. Realocação de Pessoal: quando aplicável, deverá ser simulada a realocação de colaboradores para ambientes alternativos de trabalho, incluindo regime remoto, assegurando a continuidade das atividades;

iv. Verificação de Sistemas e Tecnologia: deverá ser testada a capacidade de funcionamento dos sistemas, plataformas e ferramentas tecnológicas da Gestora, incluindo acessos, comunicações e rotinas de backup;

v. Tomada de Decisão: o Coordenador de Contingência deverá conduzir a simulação do processo decisório, adotando as medidas necessárias à gestão do cenário simulado, inclusive quanto à priorização de atividades, alocação de recursos e eventual adoção de medidas extraordinárias;

vi. Comunicação Externa: deverá ser simulada, quando aplicável, a comunicação com partes externas relevantes, incluindo cotistas, prestadores de serviços e parceiros, com vistas a assegurar a adequada divulgação das medidas adotadas;

vii. Acompanhamento e Monitoramento: o Coordenador de Contingência deverá acompanhar e monitorar a execução do teste, promovendo os ajustes necessários e registrando as ações realizadas; e

viii. Avaliação Pós-Teste: ao término do teste, deverá ser elaborado relatório contendo, no mínimo: (i) a descrição do cenário testado; (ii) as eventuais falhas identificadas; e (iii) as medidas adotadas e recomendações de melhoria.

9.3. Toda a documentação do Teste de Contingência deverá ser consolidada pelo Coordenador de Contingência e submetida à Diretoria da Gestora para ciência e deliberação, sendo os resultados apresentados em reunião específica e registrados em ata devidamente assinada.

9.4. Os documentos e registros de que trata este Plano devem serão mantidos e conservados por no mínimo 05 (cinco) anos ou conforme legislação aplicável, caso maior.

10. VIGÊNCIA E REVISÃO

10.1. Este documento entrará em vigor na data de sua aprovação pela Diretoria da Gestora.

10.2. Este Plano deve ser revisada a cada 2 (dois) anos, ou extraordinariamente, a qualquer tempo, sempre que mudanças legais, regulamentares ou corporativas demandem alterações.

11. CONTROLE DE VERSÃO

Versão	Data	Última Alteração
1.0	02/05/2024	Não se aplica
1.1	01/10/2024	1.0
1.2	30/07/2025	1.1
1.3	21/01/2026	1.2
1.4	09/04/2026	1.3