

PLANO DE CONTINGÊNCIAS E CONTINUIDADE DO NEGÓCIO

AGOSTO/2026

SUMÁRIO

1. Apresentação	3
2. Princípios Norteadores	3
3. Diretrizes na Prevenção e Tratamento das Contingências	4
4. Disseminação do Plano	4
5. Plano de Recuperação do Negócio	5
6. Tratamento das Contingências Operacionais	6
7. Testes de Contingência.....	7
8. Ativação de Mecanismos de Resposta	7
9. Disposições Gerais	9
10. Vigência e Atualização.....	9

1. Apresentação

Este Plano de Contingências e Continuidade do Negócio (“Plano de Contingências”) se aplica à administradora de carteiras de títulos e valores mobiliários, na modalidade gestora de recursos, nos termos da Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada (“RCVM 21”), da Gestora Nilus Administradora e Gestora de Recursos Financeiros Ltda. (“Nilus” ou “Gestora”).

O detalhamento do escopo das atividades da Gestora e regras para mitigação de conflitos de interesse pode ser consultado no Código de Ética da Gestora.

O Plano de Contingências da Gestora tem por objetivo estabelecer as medidas a serem tomadas para prevenir um impacto negativo considerável sobre a condução das atividades. Dentre estas contingências se incluem, por exemplo, crises econômicas, falhas operacionais e/ ou desastres naturais.

2. Princípios Norteadores

A Gestora, pautada pelos princípios de diligência e cuidado que norteiam a condução dos seus negócios e no disposto no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros (“Código ANBIMA”) e demais normas aplicáveis, deve, em casos de ocorrência de quaisquer eventos ou sinistros que possam inviabilizar, paralisar ou comprometer temporariamente o exercício de suas atividades, seguir os procedimentos aqui definidos ou, nos casos não previstos neste Plano de Contingências, os procedimentos estabelecidos pela sua diretoria.

Desta forma, é possível conhecer e minimizar os prejuízos para a Gestora, seus clientes e Colaboradores, assim definidos no Código de Ética da Gestora, no período pós-contingência, reduzindo o tempo para a normalização de suas atividades.

Além disso, a Gestora, por meio de seu Plano de Contingências, buscará sempre entender os riscos relacionados ao seu negócio, sejam eles físicos, patrimoniais ou financeiros.

De forma a cumprir com a regulação e estar apto a implementar este Plano de Contingências, a Gestora revisará a cada dois anos os procedimentos aqui dispostos, mediante solicitação e discussão no Comitê de Riscos e *Compliance* da Gestora.

Por fim, todos os Colaboradores da Gestora devem conhecer o presente Plano de Contingências e suas alterações. Caso a Gestora entenda ser necessário ou algum Colaborador manifestar interesse sobre qualquer um dos temas pertinentes, treinamento específico poderá ser fornecido.

3. Diretrizes na Prevenção e Tratamento das Contingências

Para a eficaz implementação deste Plano de Contingências, a Gestora buscará conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para tal finalidade, a Gestora 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.

Em linhas gerais, os passos para execução deste Plano de Contingências são os seguintes:

- a. Identificação das interdependências entre as instalações, equipamentos e processos de negócios da Gestora com outras empresas e/ou com fornecedores e contratados;
- b. Listagem das diferentes atividades da Gestora e identificação daquelas com alto interesse estratégico e/ou aquelas com elevado potencial de risco financeiro, físico ou operacional;
- c. Listagem das instalações, equipamentos, fornecedores, contratados que podem representar dificuldades ou restrição à aplicação deste Plano de Contingências; e
- d. Verificação da adequação dos meios preventivos e de proteção às características da operação e de negócio.

4. Disseminação do Plano

Para redução e controle de eventuais perdas com contingências, todos os Colaboradores da Gestora deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não),

planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho.

5. Plano de Recuperação do Negócio

A Gestora mantém a identificação atualizada de seus principais processos de negócios, de forma que em caso de ocorrência de contingências seja possível retomar as operações com os menores custos de transação e perdas de tempo e de recursos humanos, físicos e materiais possíveis.

No desenvolvimento do Plano de Recuperação do Negócio, conforme descrito na Política de Segurança da Informação e Segurança Cibernética, foi levado em consideração os backups dos servidores, bancos de dados e arquivos, além da estruturação do parque tecnológico na nuvem da Microsoft. Os backups realizados pelo time de tecnologia e operações são:

- a. Backup diário do banco de dados e armazenamento das versões anteriores por 30 (trinta) dias e de fechamento de mês por 5 (cinco) anos.
- b. Backup em tempo real dos arquivos (Sharepoint) e armazenamento das versões em nuvem.
- c. Backup de imagem do servidor realizado em tempo real e *Failover* (site *recovery* Microsoft Azure).

Desta forma, a salvaguarda dos dados conforme descrita acima, forma o principal processo da Gestora para a rápida recomposição de estado operacional em caso de falha no disco rígido do equipamento.

O acesso aos arquivos backups armazenados na sede da Gestora ou em local externo à sede seguirá a Política da Segurança da Informação e de Segurança Cibernética.

A Gestora conta com provedor de internet dedicado e com um Firewall FortiGate para monitoramento da navegação e permissão de conteúdo, a ser fornecido e mantido pelo time de tecnologia e Operações.

Como resultado destes procedimentos, no caso de as equipes não terem acesso ao escritório, elas terão acesso aos dados pertinentes às suas atividades por meio da nuvem, bem como acesso ao e-mail, visto que estes se encontram na nuvem. A imagem do servidor garante a possibilidade de ser executada como máquina virtualizada em qualquer outro ambiente de nuvem no caso de o ambiente Microsoft estar

indisponível. Ressaltamos que o ambiente de acesso por meio de nuvem respeita as regras de segregação eletrônica e funcional de cada departamento da Gestora.

Ainda, para a retomada célere e eficaz das operações após um evento de contingência, a Gestora mantém procedimentos que a permitem:

- a. Manter o gerenciamento do pessoal e os procedimentos das operações administrativas mesmo durante os efeitos da contingência;
- b. Retornar definitivamente a utilização das instalações de sua sede após a ocorrência da contingência;
- c. Avaliar as perdas da interrupção dos negócios.

Ademais, como todo o ambiente de dados da Gestora fica na nuvem, a Gestora entende que, em caso de contingências, as pessoas poderão acessar a nuvem a partir dos seus computadores pessoais e manter o trabalho normalmente, de forma que não é necessário ter um escritório alternativo.

6. Tratamento das Contingências Operacionais

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

- a. 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;
- b. Substituição de algum Colaborador em caso de sua saída, no menor tempo possível;
- c. Identificar novos potenciais mercados de atuação e/ou produtos caso haja queda, ou longos períodos de recessão, na demanda de seus clientes atuais;
- d. 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;

- e. Cuidar da base de clientes, de forma que seja mantido o grau de pulverização na carteira de clientes adequado ao porte da Gestora e a manutenção da confiabilidade e qualidade dos serviços prestados; e
- f. Manter um fluxo de caixa que, a critério da Diretoria da Gestora, seja hábil para fazer frente às despesas imprevisíveis.

O Diretor responsável pela prevenção de perdas e implementação do Plano de Contingências é o Sr. Marcelo Freitas de Araujo, Diretor de *Compliance*.

7. Testes de Contingência

Os testes de contingência serão realizados, no mínimo, semestralmente, de modo a permitir que a Gestora esteja preparada para a continuação de suas atividades e deverão ser reportados ao diretor de gestão da Gestora.

Os testes serão os seguintes:

- Testes de *Failover*; e
- Outros necessários à continuidade das atividades.

Caso o resultado do teste indique falha, a Gestora atuará para corrigi-la e o processo de correção será documentado.

8. Ativação de Mecanismos de Resposta

Os Colaboradores são responsáveis por comunicar a área de *compliance* da Gestora sobre toda e qualquer situação que possa, ainda que potencialmente, dar origem a uma situação que possa levar a ativação dos procedimentos de contingência indicados neste Plano de Contingência.

A ativação do Plano de Contingência ficará a critério e será de responsabilidade da área de *compliance* da Gestora.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

De forma a se prevenir da maneira mais adequada, a Gestora adotará os seguintes mecanismos de resposta para cada contingência específica:

I. Indisponibilidade da Sede

Caso a indisponibilidade seja superior a 04 (quatro) horas durante o expediente de trabalho, os Colaboradores deverão ficar à disposição e desempenhar suas funções em home office.

II. Indisponibilidade dos Servidores (nuvem)

Uma vez constatada a indisponibilidade, a empresa terceirizada de TI da Gestora ou o time próprio da Gestora deve iniciar o processo para subir o sistema em outro ambiente da nuvem Microsoft. Essa subida deveria ser relativamente rápida, mas, em caso de demora, os Colaboradores devem permanecer trabalhando normalmente e, se for o caso, desempenhar suas funções em home office.

III. Indisponibilidade de Conexão por Internet com o Exterior

A respectiva indisponibilidade poderá ser dividida em 02 (duas) modalidades: (i) caso a indisponibilidade seja inferior a 04 (quatro) horas, deverá ser avaliada a necessidade de substituição temporária dos fornecedores de acesso à internet, assim como deverá ocorrer o contato com os fornecedores de internet originários de modo que seja restaurada a respectiva conexão; e (ii) caso a indisponibilidade seja superior a 04 (quatro) horas, ou não haja previsão para restauração da conexão, deverá ser realizada a substituição dos fornecedores de acesso à internet e ser contratada empresa especializada a ser deslocada para local de modo a restaurar a indisponibilidade ou encontrar solução alternativa, ainda que temporária, caso a empresa terceirizada TI da Gestora não consiga solucionar. Os Colaboradores deverão permanecer na sede da Gestora e desempenhar suas funções.

IV. Indisponibilidade de Informações sobre os Ativos Financeiros

A respectiva indisponibilidade poderá ser dividida em 02 (duas) modalidades: (i) caso a indisponibilidade seja inferior a 04 (quatro) horas, deverá ser avaliada a necessidade de substituição temporária dos fornecedores de informações, assim como deverá ocorrer o contato com os fornecedores de internet originários de modo que seja restaurada a

respectiva conexão; e (ii) caso a indisponibilidade seja superior a 04 (quatro) horas, ou não haja previsão para restauração da conexão, deverá ser realizada a substituição dos fornecedores de informações e ser contratada empresa especializada a ser deslocada para local de modo a restaurar a indisponibilidade ou encontrar solução alternativa, ainda que temporária, caso a empresa terceirizada TI da Gestora não consiga solucionar. Os Colaboradores deverão permanecer na sede da Gestora e desempenhar suas funções.

V. Redução no Quadro de Colaboradores

A Gestora avaliará a possibilidade de locomoção até o local de sua sede e determinará quais serão as funções a serem desempenhadas pelos Colaboradores disponíveis até que se encontre solução alternativa, mesmo que temporariamente. Os Colaboradores que não conseguirem se locomover à sede da Gestora deverão ficar à disposição e desempenhar suas funções em home office.

VI. Tempo de Resposta dos Colaboradores

É de responsabilidade de cada Colaborador manter seus meios de contato atualizados e de conhecimento da Gestora. Da mesma maneira, é de responsabilidade de cada Colaborador estar acessível e comunicar suas respectivas localizações tão logo tenham conhecimento da ocorrência de um evento que possa colocar em risco a continuidade de sua função, mesmo que momentaneamente, ou, dos negócios da Gestora. Deverão, também, reportar a localização de outros Colaboradores caso tenham certeza da localização destes.

9. Disposições Gerais

Em cumprimento à RCVM 21 e ao Código ANBIMA, o presente Plano de Contingência descreve os procedimentos adotados em caso de contingências e desastres, visando sempre cumprir o dever fiduciário da Gestora, sempre com boa fé, diligência e lealdade.

10. Vigência e Atualização

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada- pelos diretores da Gestora - a qualquer tempo em razão de circunstâncias que demandem tal providência.