PLANO DE CONTINUIDADE DE NEGÓCIOS

ORRAM GESTÃO DE RECURSOS LTDA

Versão 4.0

(Março/2025)

SUMÁRIO

1. OBJETIVO 3

2. NORMAS RELACIONADAS 3

3. PÚBLICO-ALVO 3

4. PRINCÍPIOS 3

5. PROCESSOS CRÍTICOS 4

6. CENÁRIOS DE CONTINGÊNCIA 4

1. INDISPONIBILIDADE DA SEDE 4
2. INDISPONIBILIDADE DE COLABORADORES 5
3. INDISPONIBILIDADE DE INFRAESTRUTURA TECNOLÓGICA 5

7. DIRETOR RESPONSÁVEL E COMITÊ EVENTOS DE CONTINGÊNCIA 5

8. PRAZO DE RECUPERAÇÃO E INTERVALO CRÍTICO 6

9. PRÁTICAS DE CONTINGÊNCIA 6

1. MONITORAMENTO DE SISTEMAS E ESTRUTURA OPERACIONAL 6
2. BACK-UP E RECUPERAÇÃO DE DADOS 7
3. TESTES OPERACIONAIS 7
4. MÉTODOS ALTERNATIVOS DE COMUNICAÇÃO 7
5. INFRAESTRUTURA 8
6. ATAQUE CIBERNÉTICO 8
7. INDISPONIBILIDADE DE ADMINISTRADOR FIDUCIÁRIO 8
8. PRÁTICAS PARA RAPIDEZ NA RETOMADA 9
9. DIVULGAÇÃO E TREINAMENTO 9

10. TESTES 9

11. ÁREA RESPONSÁVEL 10

12. POLÍTICA DE REVISÃO E CONTROLE DE VERSIONAMENTO 10

1. CLASSIFICAÇÃO DE USO 10
2. REVISÃO 10
3. REVISÃO 10
4. MANUTENÇÃO DE ARQUIVOS 11
5. REGRAS DE INTERPRETAÇÃO 11

1. OBJETIVO

O objetivo deste Plano de Continuidade de Negócios ("PCN"), é estabelecer um conjunto de métodos e ações a serem adotados pela Orram Gestão de Recursos Ltda. ("Gestora" ou "ORRAM"), para o caso de eventos ou situações que impossibilitem a continuidade das operações e atividade empresarial da ORRAM.

Para minimizar perdas e evitar danos às atividades essenciais da empresa, a Gestora desenvolveu o presente PCN a fim de permitir que, após a ocorrência de evento de contingência, a ORRAM reassuma o processamento das operações críticas dentro de um intervalo de tempo adequado às necessidades de negócio.

2. NORMAS RELACIONADAS

São normas relacionadas a este PCN:

a) Resolução CVM nº 21, de 25 de fevereiro de 2021;
b) Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros ("Código ANBIMA");
c) Regras e Procedimentos de Deveres Básicos da ANBIMA ("RP Deveres Básicos");
d) Manual de Compliance da ORRAM; e
e) Política Corporativa de Segurança Da Informação e Segurança Cibernética da ORRAM ("PSI").

3. PÚBLICO-ALVO

Todos os sócios, estagiários, *trainees,* funcionários e prestadores de serviços da ORRAM ("Colaboradores") devem conhecer o presente PCN e suas alterações para, em caso de eventualidades, estarem preparados.

4. PRINCÍPIOS

São princípios que norteiam a atuação da ORRAM quanto à contingência de negócios:

a) análise de processos críticos da ORRAM, com definição de medida de contingência a ser adotada;
b) revisão periódica do PCN, com testes de sistema e tecnologia, bem como verificação de sua adequação;
c) minimização dos danos no período pós-contingência, seja para a Gestora em si ou investidores; e
d) normalização, o mais rápido possível, as atividades de gestão.

5. PROCESSOS CRÍTICOS

A Gestora gere fundos de investimento estruturados, em especial fundos de investimento em direitos creditórios ("FIDC") e fundos de investimento em participações ("FIP"), bem como fundos de investimento financeiro ("FIF") que, em regra, investem nas cotas dos anteriores.

Neste sentido, a ORRAM considera os seguintes processos, subprocessos e atividades como críticos ("Processos Críticos"):

a) análise de operações;
b) liquidação de operações;
c) batimento das carteiras;
d) controle do caixa;

Os Processos Críticos devem ser os primeiros a serem reestabelecidos.

6. CENÁRIOS DE CONTINGÊNCIA

São cenários de contingência:

a) indisponibilidade física da sede da Gestora;
b) indisponibilidade de Colaboradores; e
c) indisponibilidade de infraestrutura tecnológica, inclusive por ataque cibernético.

1. INDISPONIBILIDADE DA SEDE

A Gestora possui como site principal a unidade localizada na cidade de São Paulo, Estado de São Paulo, na Rua dos Pinheiros, n° 870, conjuntos 201 e 202, em que estão alocados seus recursos e operações, além da

infraestrutura tecnológica necessária para as atividades de administração e gestão das carteiras de valores mobiliários.

Não obstante, a Gestora tem plena capacidade de operar totalmente em sistema de *home office.,* com acesso remoto via VPN.

2. INDISPONIBILIDADE DE COLABORADORES

Em caso de indisponibilidade momentânea de Colaboradores – *e.g.,* mais da metade dos Colaboradores doente, sem poder desempenhar suas funções – a ORRAM atuará em contingência, com menor número.

Para cada atividade crítica da ORRAM, há mais de um profissional com acessos sistêmicos e aptidão técnica para seu desempenho.

3. INDISPONIBILIDADE DE INFRAESTRUTURA TECNOLÓGICA

Em caso de indisponibilidade de infraestrutura tecnológica – e.g., ataque cibernético ou falha técnica –, principal cenário de contingência, a ORRAM entende que, decretada a situação de contingência após a avaliação do Diretor de Tecnologia e definição do Diretor de Risco e Compliance, as práticas descritas na Seção 8 são suficientes para se enfrentar o cenário.

7. DIRETOR RESPONSÁVEL E COMITÊ EVENTOS DE CONTINGÊNCIA

Neste PCN e nas melhores práticas de continuidade de negócios, os eventos com as seguintes naturezas são considerados como possíveis causas de interrupções e necessidade de decretação de contingência:

a) **Humana**: greves, distúrbio civil, pandemias, falha de prestador de serviços/parceiro, acesso indevido às instalações e erro humano (*i.e.*, ato não intencional).
b) **Tecnológica:** falha em aplicativo (“SW”), falha em *hardware* (“HW”), falha em sistemas operacionais, vírus de computador, falha em rede interna (“LAN”), falha na entrada de dados, falha em rede externa (“WAN”), falha de Telecom - dados e falha em sistema de acesso.

c) **Infraestrutura**: falha em Telecom - voz, falha em sistema de refrigeração, interrupção de energia elétrica e falha em instalações elétricas.
d) **Natural**: alagamento interno do ambiente, queda de raios, vendaval, incêndio.
e) **Física:** Problema Estrutural ou de instalações e rompimento de tubulação Interna (água, esgoto e gás).

8. PRAZO DE RECUPERAÇÃO E INTERVALO CRÍTICO

O prazo máximo para a recuperação em caso de eventos extremos é de 1 (um) dia útil para os Processos Críticos, condizente com a atuação da Gestora.
No mais, o horário crítico para acionamento do PCN é das 9h às 18h, em dias úteis.

9. PRÁTICAS DE CONTINGÊNCIA

1. MONITORAMENTO DE SISTEMAS E ESTRUTURA OPERACIONAL

A Gestora mantém mapeamento dos sistemas e aplicativos considerados essenciais para o desempenho dos Processos Críticos ("Sistemas Críticos"), tais como o Power BI, utilizado pela Área de Gestão e a Área de Risco.
O desempenho e o acesso a estes é constantemente acompanhado, de modo preventivo.
Além dos Sistemas Críticos, os principais pontos de atenção monitorados pela Gestora são o funcionamento e a manutenção de:

a) Internet;
b) rede elétrica; e
c) equipamentos.

Tais serviços possuem monitoramento ativo, tanto por parte do fornecedor como por parte do Departamento de Tecnologia da ORRAM.
Uma vez identificada a inatividade total ou parcial de algum destes serviços, o Departamento de Tecnologia deve mensurar o tempo para restabelecimento

do pleno funcionamento.

Tais serviços possuem monitoramento ativo, tanto por parte do fornecedor como por parte de nossa equipe interna, visando antecipar o conhecimento da possível falha, uma vez identificada a inatividade total ou parcial de algum destes serviços, o departamento de Tecnologia deve mensurar o tempo para restabelecimento do pleno funcionamento, sendo que essas informações serão utilizadas pelo Gestor para tomada de decisão.

2. BACK-UP E RECUPERAÇÃO DE DADOS

A Gestora mantém cópias eletrônicas de todas as informações fundamentais relacionadas aos veículos de investimento, em um ambiente seguro na "nuvem".

Os arquivos do *data center* são copiados diariamente para uma cópia local, e duas cópias em nuvem.

Caso ocorra alguma falha que comprometa o acesso local a essas informações, os Colaboradores, usuários de tais dados, também recebem um *link* de acesso ao seu perfil na nuvem, o qual poderá ser utilizado também em caráter de contingência.

3. TESTES OPERACIONAIS

A ORRAM testa anualmente sua prontidão em caso de desastres para garantir que os Sistemas Críticos estão aptos a operar de uma localidade remota.

A Gestora também verifica se as cópias eletrônicas das informações dos fundos de investimento e respectivas operações, que são mantidas no escritório da Gestora e na "nuvem", não foram corrompidas e estão disponíveis para uso pela Gestora.

4. MÉTODOS ALTERNATIVOS DE COMUNICAÇÃO

Em cenário de contingência, além dos e-mails e sistemas de mensageria fornecidos pela Microsoft Office 365, a Gestora possui os telefones celulares pessoais dos profissionais, bem como sistemas de mensageria externos e gratuitos que garantem comunicação mínima.

Dentro do operacionalmente possível, em caso de interrupção significativa de

negócios e decretação de cenário de contingência, a Gestora envidar esforços para informar esta situação a Colaboradores administradores fiduciários, originadores, cedentes e contrapartes em geral.

5. INFRAESTRUTURA

Em caso de falha no fornecimento elétrico, os *nobreaks* são ativados para estações de trabalho e servidores, com autonomia de 30min, tempo suficiente para o gerador do condomínio entrar em atividade.

O *site* principal, possuí 3 *links* de *internet* para redundância. Em caso de falha do *link* principal, o primeiro *link* redundante é acionado, e, em caso de falha destes dois *links*, o *modem* 4G com *Wi-Fi* é ativado para suprimir as necessidades críticas.

Para telefonia, caso o *link* E1 não possa ser utilizado, 3 linhas móveis são disponibilizadas para uso da equipe.

6. ATAQUE CIBERNÉTICO

Anualmente, a Gestora deverá realizar teste de invasão externa, contratado do provedor terceirizado de serviços. Duas portas devem ser testadas por vez. Além disso, o ataque simulado deve ser anônimo, sendo que a Gestora deve receber o reporte do teste ao final do processo.

A qualquer indício de ataque cibernético, os Colaboradores devem interromper suas atividades e comunicar imediatamente a Área de Tecnologia, por telefone, que executará os procedimentos para evitar a sua propagação em todo o ambiente lógico da ORRAM.

É terminantemente proibido os esforços individuais e isolados do Colaborador, pois podem contribuir para provocar danos ainda maiores.

Mais disposições sobre o tema estão na PSI.

7. INDISPONIBILIDADE DE ADMINISTRADOR FIDUCIÁRIO

Em caso de indisponibilidade do administrador fiduciário, parte das rotinas dos veículos de investimento é comprometida.

Dentro do operacionalmente praticável e cabível – isto é, em caso de impacto em Processos Críticos –, a Gestora deve comunicar os originadores parceiros,

investidores até que a situação seja normalizada.

8. PRÁTICAS PARA RAPIDEZ NA RETOMADA

Ainda, para a retomada célere e eficaz das operações após uma contingência, a Gestora deve manter procedimentos que lhe permitam:

a) utilizar alternativas de dentro ou fora da Gestora para substituição de equipamentos danificados;
b) manter saldo financeiro e acesso a crédito para qualquer despesa de contingência ou compra de equipamentos ou serviços que se fizerem necessários;
c) manter suas atividades mesmo durante os efeitos da contingência, por meio de acesso remoto por parte de seus colaboradores;
d) disponibilizar *notebooks* para os colaboradores seguirem desempenhando suas atividades remotamente em casos de contingência;
e) retornar definitivamente a utilização das instalações de sua sede após a ocorrência da contingência; e
f) avaliar as perdas da interrupção dos negócios.

9. DIVULGAÇÃO E TREINAMENTO

A divulgação deste PCN é constante, sendo este de uso interno, disponível a todos os Colaboradores.
Devem ser realizados treinamentos periódicos para toda os Colaboradores.
Os Colaboradores devem, ainda conhecer os procedimentos de *backup*, salvaguarda de informações, em especial as classificáveis como confidenciais, planos de evacuação das instalações físicas, melhores práticas de saúde e segurança no ambiente de trabalho.

10. TESTES

Os testes de funcionamento de todos os serviços da contingência devem ser realizados anualmente pelo Departamento de Tecnologia.
Os testes e simulações devem ser formalmente documentados, para fornecer material útil a futuras tomadas de decisão relacionadas a melhorias do PCN.

11. ÁREA RESPONSÁVEL

O processo contínuo de continuidade de negócio deve ser de responsabilidade e gestão do Diretor de Tecnologia, que deve determinar as etapas que deverão ser executadas e os cenários de risco e impacto sobre o negócio, bem como quais as ações que devem ser executadas para a manutenção de um ambiente sempre protegido.

A decretação do estado de contingência cabe ao Diretor de Risco e Compliance, após análise do Diretor de Tecnologia, com comunicação imediata ao Comitê de Plano de Respostas a Incidentes.

12. POLÍTICA DE REVISÃO E CONTROLE DE VERSIONAMENTO

1. CLASSIFICAÇÃO DE USO

O PCN é um documento de uso interno, disponível a todos os Colaboradores, bem como fornecido à ANBIMA.

2. REVISÃO

O PCN deve ser submetido a revisão a cada 24 (vinte e quatro) meses ou em período inferior a este e sempre que ocorrerem alterações na legislação, na regulamentação ou na autorregulamentação vigentes, sendo dispensada sua alteração caso não haja melhorias pertinentes a escopo de plano de ação.

3. REVISÃO

Esta versão revoga todas as anteriores e passa a vigorar a partir da data de sua publicação, isto é, em 20/03/2025.

O controle de versões é:

Versão	Data	Modificações
01	Abril/2020	Original.
02	Dezembro/2021	Revisão geral, adequação de redação e nova formatação dos itens.

03	Dezembro/2022	Revisão periódica e adequação para os processos atuais.
04	Março/2025	Revisão periódica e adequação para os processos atuais.

4. MANUTENÇÃO DE ARQUIVOS

Embora a regra usual de manutenção de arquivos e evidências seja de 5 (cinco) anos no contexto da regulamentação aplicável ao mercado de capitais, a ORRAM empregará melhores esforços para manter documentos – em especial os relacionados à ativação do PCN – por, no mínimo, 10 (dez) anos, em consonância com a regra geral de prescrição prevista no Código Civil.

5. REGRAS DE INTERPRETAÇÃO

Em relação ao tema aqui tratado, o PCN é considerado norma específica e se sobrepõe a eventuais outras normas internas da ORRAM em caso de conflito direto ou dúvidas de interpretação.

Alterações supervenientes na lei, na regulamentação e na autorregulamentação aplicáveis são imediatamente aplicáveis às práticas internas da ORRAM, ainda que a revisão formal do PCN esteja em curso.