



Plano de Contingência e Continuidade dos Negócios

Versão 1.2 – maio de 2025

Parcitas Ações Gestão de Investimentos Ltda.

Parcitas Macro Gestão de Investimentos Ltda.

ÍNDICE

1. Objetivo e Abrangência.....	3
2. Base Legal.....	3
3. Responsabilidade	5
4. Estrutura, Redundância e Monitoramento.....	5
5. Equipe de contingência e cenários.....	10
6. Documentação e Armazenamento	11
7. Revisão e Programa de Compliance	11
8. Controle de Versões	11

1. Objetivo e Abrangência

Esta política (“plano de contingência e continuidade dos negócios” ou “política”) tem por objetivo estabelecer os princípios, regras e procedimentos necessários a serem adotados pelas respectivas gestoras Parcitas Macro Gestão de Investimentos Ltda. e Parcitas Ações Gestão de Investimentos Ltda. (conjuntamente, “Parcitas”), no caso de contingência operacional, de modo a impedir descontinuidade das atividades por problemas que impactem no funcionamento da gestora, em conformidade com as leis, normativas, ofícios e orientações dos reguladores e autorreguladores que regem a atividade da Parcitas.

O Plano de Contingência será acionado quando for identificada qualquer ocorrência ou situação que dificulte ou impeça a rotina diária da operação da Gestora, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, aos investidores ou à Parcitas.

A abrangência desta política se aplica a todos aqueles Colaboradores que possuam cargo, função, posição, relação societária, empregatícia ou de estágio com a Parcitas (“Colaboradores”).

2. Base Legal

O Plano de Contingência e Continuidade dos Negócios da Parcitas é um componente importante para assegurar que os serviços essenciais da Gestora sejam preservados na ocorrência de um imprevisto ou um desastre, refletindo o compromisso da organização com a conformidade regulatória estabelecida pela Comissão de Valores Mobiliários (“CVM”) e a autorregulação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“Anbima”), bem como o cumprimento das leis aplicáveis no Brasil.

Este documento detalha as medidas tomadas antecipadamente e orienta as ações a serem seguidas por todos os Colaboradores, assegurando que as atividades da Parcitas sejam conduzidas de maneira ininterrupta em conformidade com os mais altos padrões regulatórios.

2.1. Regulamentação Relevante

A seguir, detalhamos as principais regulamentações que integram e orientam o Plano de Contingência e Continuidade dos Negócios Parcitas:

- Resolução CVM nº 21 de 25 de fevereiro de 2021: Esta resolução, conforme alterada, regulamenta o exercício profissional de administração de carteiras e valores mobiliários, estabelecendo diretrizes claras para a atuação dos gestores de fundos de investimento.

- Resolução CVM nº 175 de 3 de dezembro de 2022: Dispõe sobre a constituição, funcionamento e divulgação de informações dos fundos de investimento, bem como sobre a prestação de serviços para esses fundos. Seus anexos normativos complementam as exigências e orientações específicas.
- Código Anbima de Administração e Gestão de Recursos de Terceiros (AGRT): Define as melhores práticas para a administração e gestão de recursos de terceiros, sendo de cumprimento obrigatório para a Parcitas.
- Demais Normas e Orientações: Incluem manifestações e ciclos orientadores dos órgãos reguladores e autorreguladores que são aplicáveis à atividade da Parcitas.

2.2. Interpretação do Código

Para a interpretação dos dispositivos deste Código de Conduta, salvo disposição expressa em contrário, considera-se que:

- Termos Utilizados: Tem significado atribuído na Resolução CVM 175.
- Referências a Fundos: Incluem Classes e Subclasses, quando aplicável.
- Regulamentos e Anexos: Referências a regulamentos incluem seus anexos e apêndices, se houver, em conformidade com a Resolução CVM 175.
- Classes e Fundos: As referências às Classes abrangem também os Fundos que ainda não foram adaptados à Resolução CVM 175.

2.3. Aplicabilidade do Código

Para fins de interpretação deste Plano de Contingência e Continuidade dos Negócios, salvo disposição expressa em sentido contrário: (a) os termos utilizados terão os significados atribuídos pela Resolução CVM nº 175; (b) as menções a Fundos devem ser entendidas como abrangendo também suas Classes e Subclasses, quando existentes; (c) as referências aos regulamentos incluem seus respectivos anexos e apêndices, conforme aplicável pela Resolução CVM nº 175; e (d) as referências às Classes incluem também os Fundos que ainda não tenham sido adaptados à referida Resolução.

As disposições deste Plano de Contingência e Continuidade dos Negócios aplicam-se, conforme o caso, tanto aos Fundos constituídos a partir de 2 de outubro de 2023 (data de vigência da Resolução CVM nº 175), quanto àqueles previamente constituídos que já tenham sido adaptados à nova regulamentação. Até a adaptação integral às regras da Resolução CVM

nº 175, a Parcitas Investimentos e os Fundos sob sua gestão continuarão observando as disposições da Instrução CVM nº 555, de 17 de dezembro de 2014, e demais normas aplicáveis, especialmente no que se refere às responsabilidades e atribuições da gestora.

3. Responsabilidade

A coordenação direta das atividades relacionadas a esta política é uma atribuição do Diretor estatutário responsável pela Gestão de Riscos, Compliance, Controles Internos e de Prevenção a Lavagem de Dinheiro da Parcitas (“Diretor de Riscos e Compliance”), nos termos da Resolução CVM 21.

O Diretor de Riscos e Compliance também tem como responsabilidade monitorar e assegurar o cumprimento desta Política e caso ocorra algum evento ou necessidade de novo requisito operacional não mapeado em relação aos parâmetros estabelecidos nesta política, este deverá comunicar ao Comitê de Riscos e Compliance e tomar as medidas necessárias para que a infraestrutura mínima seja disponibilizada.

A Parcitas compartilha amplamente o Plano de Contingência com seus colaboradores e os prepara para exercer suas funções em situações contingenciais, evitando e/ou minimizando qualquer impacto no desenvolvimento de suas atividades.

Caso ocorra algum evento ou necessidade de novo requisito operacional não mapeado em relação aos parâmetros estabelecidos nesta política, o Diretor de Riscos e Compliance irá comunicar ao Comitê de Riscos e Compliance e tomará as medidas necessárias para que a infraestrutura mínima seja disponibilizada.

4. Estrutura, Redundância e Monitoramento

Esta política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da Parcitas, e, portanto, as estruturas que necessitam estar contempladas de forma a garantir o funcionamento da empresa:

1. Escritório/Espaço físico: onde são realizadas as operações da Parcitas. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades; 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 incêndios, pandemias, greves, interdições pelas autoridades do prédio ou do entorno do escritório da Parcitas etc.
2. Infraestrutura Tecnológica: são problemas dessa ordem, 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 Parcitas; e

3. Pessoal: Pessoas responsáveis pela operação da Parcitas, incluindo a análise e decisão para realização ou não de investimentos, equipe responsável pelo Compliance e Gestão de Riscos das carteiras.

Neste sentido, o plano de continuidade de negócios da Parcitas é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los no prazo previamente estabelecido.

A exemplo, avaliamos riscos de Nível 1, aqueles eventos de baixa probabilidade de impacto nas atividades e com monitoramento cotidiano para a sua prevenção. Tais eventos tem chance maior de ocorrência e frequência. Exemplos: eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas de porte leve, tais como falhas de ar-condicionado, elevadores, vazamentos e/ou abastecimento de água.

Como riscos de Nível 2, consideramos aqueles eventos de impacto potencial médio nas atividades e necessidade de maior nível de controles preventivos. Tais eventos tem chance moderada de ocorrência e frequência baixa. Exemplos: situações não diretamente relacionadas à Parcitas e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas de porte moderado, acesso lento ao espaço físico da Gestora, intermitência no fornecimento de luz, internet, telefonia, eventuais falhas de segurança/manutenção das instalações físicas, ferramentas e recursos tecnológicos da Parcitas.

Por fim, como riscos de Nível 3, temos aqueles de impacto relevante nas atividades da Parcitas, com adoção de rigorosos controles preventivos. Tais eventos tem baixa chance de ocorrência e frequência. Exemplos: falha grave de manutenção/atualização dos softwares e serviços críticos utilizados pela Parcitas no exercício de suas operações e monitoramentos periódicos que resultem em inoperância; interrupção do funcionamento de equipamentos utilizados pelos colaboradores da Parcitas que inviabilizem sua utilização nas atividades de operação e monitoramentos periódicos, desastres naturais (terremotos, alagamentos) ou conjunturas sócias/econômicas de natureza grave e incêndios.

Para fazer frente aos eventos acima previstos, nossa estrutura de proteção, redundância e monitoramento visa atender com rigor as ocorrências nestes diversos níveis de gravidade.

4.1. Energia Elétrica

A Parcitas possui, na sua sede em São Paulo, uma infraestrutura que conta com redundância de energia elétrica nos eventos de falta da distribuição pela empresa contratada.

A estrutura de contingenciamento conta um processo realizado em duas etapas, sendo:

- **No Break:** entrada instantânea e automática de energia fornecida pelo nobreak existente de 15 KvA (as baterias suportam 04 horas do escritório em plena função).
- **Gerador:** gerador próprio, acionado após 15 segundos da queda de energia. O gerador da Parcitas é à diesel, possui 100 KvA e autonomia de 180 litros de combustível (podendo ser reabastecido) suportando 12 horas de funcionamento de toda a estrutura da Gestora.

4.2. Links de Internet

A Parcitas possui, na sua sede em São Paulo, redundância de links de comunicação pela internet em sua infraestrutura operacional totalizando 1.4 Gigabyte de dados para comunicação e distribuídos por áreas e sistemas críticos a operação, sendo:

- 1 link primário corporativo full duplex de Internet de 700 MB com 5 IP fixos da Mundivox;
- 1 link ADSL de 700 MB com 1 IP fixo da empresa Vivo.

4.3. Servidores

Todos os serviços de infraestrutura de tecnologia da Parcitas são executados por servidores virtuais na nuvem da Microsoft Azure, sejam as informações de domínio, cadastro dos usuários, permissões de acessos, gestão das impressoras, políticas de grupos, aplicações internas, bem como o armazenamento e organização dos arquivos corporativos através dos serviços em nuvem do SharePoint Microsoft, bem como todas as demais aplicações online do Office 365.

Devido à natureza do serviço da Microsoft ser em nuvem, a equipe da Parcitas, tanto em São Paulo quanto em Belo Horizonte, desempenha suas atividades seja no escritório ou fora dele dentro do mesmo ambiente de infraestrutura de tecnologia.

4.4. Contingenciamento Firewall

A Parcitas possui, na sua sede em São Paulo, redundância do firewall em sua infraestrutura operacional. Existem dois firewalls trabalhando em cluster ativo-ativo. Caso um deles pare de funcionar o outro assume.

4.5. VPN

A Parcitas possui uma rede privada virtual (“VPN”) ativa que possibilita uma conexão segura e criptografada entre o usuário e a infraestrutura da Parcitas. Caso ocorra algum problema interno, onde não seja possível trabalhar localmente, todos os usuários conseguem trabalhar remotamente de computadores externos ou diretamente pela nuvem da Microsoft Azure.

4.6. Telefonia

A Parcitas conta com uma telefonia primária com o número (11) 3192 – “ramal”

O gerenciamento da telefonia é feito por um sistema dedicado de PABX que distribui o serviço internamente no escritório nas estações de trabalho dos colaboradores.

4.7. Acesso e Back de Dados

Como continuidade, todos os serviços de infraestrutura de tecnologia da Parcitas são centralizados, independentemente por localidade e executados por servidores virtuais na nuvem da Microsoft Azure, bem como o armazenamento e organização dos arquivos corporativos através dos serviços em nuvem do SharePoint Microsoft, bem como todas as demais aplicações online do Office 365.

Como os serviços são de natureza “em nuvem”, em caso de contingência, o acesso às pastas e sistemas críticos serão acessados do ambiente externo pelo acesso direto aos serviços em nuvem da Microsoft Azure ou pelo escritório da Parcitas através da VPN.

Além do backup de 90 dias instantâneo da Microsoft, todos os dados dos serviços de e-mail (Microsoft Exchange), arquivos corporativos (Microsoft OneDrive e Sharepoint) e comunicação (Microsoft Teams) possuem também um backup diário com 7 anos de dados utilizando o serviço *Cove Data Protection*, na modalidade *Cloud2Cloud* nos servidores da Amazon Cloud, conforme descrito no Manual de Controles Internos

4.8. Sistemas e Dados críticos

A Parcitas utiliza um grupo de sistemas de informação que dão suporte a sua operação, e para cada um deles há uma contingência em caso de indisponibilidade.

- Risco e Compliance: Plataforma de sistemas desenvolvido pela Lote45 Ltda são hospedados e processados em um data center externo “Hostway” (TIER nível máximo 3), provendo redundância em múltiplas regiões distintas. O contrato de prestação de serviço provê um SLA rígido para manutenção do sistema em caso de indisponibilidade. O acesso

aos sistemas da Lote45 está disponível aos profissionais da Parcitas no computador em nuvem Terminal Server ou em qualquer lugar com acesso à internet.

- Bloomberg: Desenvolvido pela Bloomberg, este sistema tem os dados e execução processados em um data center externo. O acesso a Bloomberg está disponível aos profissionais da Parcitas no computador em nuvem Terminal Server ou em qualquer lugar com acesso à internet.
- E-mail: A Parcitas utiliza um serviço de e-mail em cloud (nuvem) na modalidade de Software as a Service (SaaS) oferecido pela Microsoft (Exchange online Office 365) com armazenamento hospedados na Microsoft (Plano E3) com *Litigation Hold* ativado. 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%. Ademais as informações contidas neste serviço passam pela rotina de backup de dados diário utilizando o serviço da Microsoft e do *Cove Data Protection*, na modalidade *Cloud2Cloud* nos servidores de backup da Amazon Cloud. Os dados podem ser acessados pelos profissionais da Parcitas diretamente de qualquer lugar através do serviço em nuvem.
- Rede Corporativa: A Parcitas utiliza um serviço de armazenamento de arquivos (“Rede Corporativa”) em cloud (nuvem) na modalidade de Software as a Service (SaaS) oferecido pela Microsoft (Sharepoint e OneDrive Office 365). As informações contidas neste serviço passam pela rotina de backup de dados diário utilizando o serviço da Microsoft e do *Cove Data Protection*, na modalidade *Cloud2Cloud* nos servidores de backup da Amazon Cloud. Os dados podem ser acessados pelos profissionais da Parcitas diretamente de qualquer lugar através do serviço em nuvem.
- Sistema de Comunicação: a Parcitas utiliza o sistema Teams da Microsoft Office 365 para fazer a integração dos colaboradores, respectivas conversas, reuniões e compartilhamento de conteúdo no modelo de trabalho remoto. As informações contidas neste serviço passam pela rotina de backup de dados diário utilizando o serviço da Microsoft e do *Cove Data Protection*, na modalidade *Cloud2Cloud* nos servidores de backup da Amazon Cloud. Os dados podem ser acessados pelos profissionais da Parcitas diretamente de qualquer lugar através do serviço em nuvem.

4.9. Suporte e Monitoração

A Parcitas possui uma gestão, suporte e monitoração NOC (Network Operation Center) 24/7/365 terceirizada da infraestrutura de IT pela empresa ATUAL IT, com endereço na Rua Helena, 170, conjunto 133/134, Vila Olímpia, São Paulo – SP, Tel. (11) 3995-7777. A prestação dos serviços de Tecnologia da Informação são rede interna, Firewall, Wireless, DHCP, Links

de Internet, Hospedagem, CPUs \ Monitores \ Impressoras \ Scanners \ Fax, Antivírus, Servidores, Rotinas de Backup, Controladores de Domínio, Acesso Remoto, Servidor de Arquivos, E-mail, CPD, Criação e Desligamento de Usuários.

5. Equipe de contingência e cenários

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 Parcitas, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance e Risco (Coordenador de Contingência);
- Diretor de Investimentos;
- Diretor sem Designação específica.

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.

Em um cenário, onde for constatado basicamente a impossibilidade ou dificuldade em manter o funcionamento normal da Parcitas devido a problemas de ordem técnica (hardware), física (acesso ao escritório), pessoal (ausência significativa de funcionários) e de infraestrutura (falta de energia), o Coordenador de Contingência da Parcitas deverá acionar este plano e iniciar imediatamente a avaliação das causas que geraram a contingência e providenciar sua solução o mais rápido possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo, quais sejam:

- Comunicar o mais rápido possível (obrigatoriamente dentro do mesmo dia útil do ocorrido) o ocorrido à toda a equipe da Parcitas, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição;
- Entrar em contato com a empresa terceirizada responsável pela Tecnologia da Informação da Parcitas, 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 e para o aplicativo de telefonia remota instalado no celular dos colaboradores da equipe de contingência.
- Caso seja verificada a impossibilidade de utilização das dependências físicas do escritório da Parcitas, os colaboradores deverão continuar a desempenhar suas atividades através de *Home Office*, uma vez que todos os arquivos podem ser acessados pela nuvem ou VPN, obedecidos os critérios de acesso. Em havendo necessidade, a equipe da Parcitas, irá se reunir no Escritório de Contingência localizado na residência de um dos Diretores da

Parcitas, que dispõe de ambiente e infraestrutura para tanto e prosseguirá com a gestão remota dos fundos sob sua administração.

O Coordenador de Contingência da Parcitas deverá acompanhar todo o processo acima descrito até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela Parcitas e reportar eventuais alterações/atualizações da contingência aos demais colaboradores.

6. Documentação e Armazenamento

Todas as decisões relacionadas a presente política tomadas pelo Comitê de Riscos e Compliance, conforme o caso, devem ser formalizadas em ata ou e-mail e todos os materiais que documentam tais decisões serão mantidos arquivados por um período mínimo de 05 (cinco) anos e disponibilizados para consulta.

7. Revisão e Programa de Compliance

Esta política deve ser revista periodicamente, levando-se em consideração: (i) mudanças regulatórias; (ii) conversas com outros participantes do mercado; e (iii) eventuais deficiências encontradas, dentre outras.

A revisão desta política tem o intuito de permitir a aderência e conformidade às normas e requisitos regulatórios, e no mínimo anualmente, o Diretor de Riscos e Compliance deverá realizar testes de aderência/eficácia das métricas e procedimentos aqui previstos e/ou por si definidos.

Os controles desta política que irão compor o Programa Anual de Compliance são:

Código	Controle Interno	Executor	Frequência	Verificador
PCN_1	Atividades executadas	Atual IT	Mensal	Compliance
PCN_2	Teste de contingência	Parcitas/Atual	Semestral	Compliance
PCN_3	Teste Disaster Recovery	Parcitas/Atual	Semestral	Compliance

8. Controle de Versões

Nome do documento:	Plano de Contingência e Continuidade do Negócio
Área de emissão:	Riscos e Compliance

Data	Versão	Número de Páginas	Nome do Aprovador
10/04/2023	1.0	10	Comitê de Riscos e Compliance
25/03/2024	1.1	10	Comitê de Riscos e Compliance
26.05.2025	1.2	12	Comitê de Riscos e Compliance



parcitas
i n v e s t i m e n t o s