parcitas
investimentos

Política de Contingência e Continuidade dos Negócios

Versão 1.0 - 10.04.2023

ÍNDICE

1. Propósito e Abrangência

Este Presente documento Plano de Contingência e Continuidade de Negócios foi elaborado em conformidade com a Resolução CVM nº 175 de 28 dezembro de 2022 bem como as diretrizes do Conselho de Regulação e Melhores Práticas da Associação Brasileira dos Mercados Financeiro e de Capitais - ANBIMA, com objetivo de estabelecer os princípios, regras e procedimentos necessários a serem adotados pela Parcitas Gestão de Investimentos Ltda, no caso de contingência, de modo a impedir descontinuidade operacional por problemas que impactem no funcionamento da empresa.

Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da Gestora sejam preservados na ocorrência de um imprevisto ou um desastre.

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 clientes ou à Parcitas.

2. Responsabilidade

A coordenação direta das atividades relacionadas a este Plano é uma atribuição do Sr. Rodrigo Cefaly de Aranda Gatti, indicado como Diretor de Compliance e Risco da Parcitas em seu Contrato Social, na qualidade de diretor estatutário, e que deverá monitorar, assegurar e implementar os controles estabelecidos pelo Comitê de Riscos e Compliance.

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 Compliance e Risco irá comunicar ao Comitê de Riscos e Compliance e tomará as medidas necessárias para que a infraestrutura mínima seja disponibilizada.

3. 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: 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 Parcitas etc.; 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 àqueles 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; 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.

3.1 Energia Elétrica

A Parcitas possui na sua infraestrutura uma redundância de energia elétrica nos eventos de falta da distribuição pela empresa contratada ("ENEL"). O processo de contingenciamento é realizado em 2 etapas, sendo:

- No Break: Entrada instantânea e automática de energia fornecida pelo nobreak existente de 15 KvA (as baterias suportam 4 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 7 horas de funcionamento de toda a estrutura da gestora.

3.2 Links de Internet

A Parcitas possui redundância de *links* de comunicação pela internet em sua infraestrutura operacional totalizando 400 Megabite de dados para comunicação e distribuídos por áreas e sistemas críticos a operação, sendo:

- 1 link primário corporativo *full duplex* de Internet de 100 MB com 5 IP fixos da Mundivox;

- 1 link ADSL com 1 IP fixo da empresa Vivo

3.3 Disaster Recovery

A Parcitas possui seus servidores virtuais com replicação ativa para a nuvem da Microsoft Azure.

Caso aconteça algum desastre com o nosso servidor físico principal (onde estão todos os servidores virtuais), são acionadas as máquinas no Microsoft Azure para continuidade das atividades.

3.4 Contingenciamento Firewall

A Parcitas possui redundância do *firewall* em sua infraestrutura operacional. Existe 2 *firewalls* trabalhando em *cluster* ativo-ativo. Caso um deles pare de funcionar o outro assume.

3.5 VPN

A Parcitas possui uma VPN ativa que se conecta diretamente com o nosso Firewall. Caso ocorra algum problema interno, onde não seja possível trabalhar localmente, todos os usuários conseguem trabalhar remotamente de computadores externos ou notebooks.

3.6 Telefones

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.

3.7 Acesso e Back de Dados

Como continuidade, todos os servidores virtuais são replicados para o Microsoft Azure instantaneamente contendo as informações de domínio, cadastro dos usuários, permissões de acessos, políticas de grupos e principalmente os arquivos. Como os servidores são replicados online, em caso de contingência, o acesso às pastas e sistemas críticos serão acessados através do ("**Terminal Server**") configurado na Microsoft Azure.

Já com relação ao backup, esse 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 Diretor de Riscos e Compliance deve ser comunicado imediatamente para que providências sejam tomadas em relação à nova restauração de dados.

Diariamente, às 22:00hr, é realizado o backup dos servidores utilizando o serviço Cloud da Microsoft Azure. Esse backup é criptografado, tem a retenção dos últimos 10 dias (Duas semanas de segunda a sexta feira), do último dia útil de cada um dos 12 meses e dos últimos 5 anos.

3.8 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 a 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%.

- Rede Corporativa: O servidor de arquivos ("Rede Corporativa") é o local destinado a armazenar todos os dados e arquivos da Parcitas. As informações contidas neste servidor passam pela rotina de Backup de Dados descrita acima e seus dados

podem ser acessados pelos profissionais da Parcitas no computador em nuvem Terminal Server.

- 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.

- Conexão Remota: Remote Desktop Protocol (RDP) é um sistema da Microsoft com protocolo multicanal que permite que os colaboradores conectem sua respectiva área de trabalho remota aos computadores disponibilizados para contingência operacional (nuvem ou VPN).

3.9 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.

4. 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.

5. Documentação e armazenamento

Todas as decisões relacionadas à 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 5 (cinco) anos e disponibilizados para consulta.

6. Dúvidas

Dúvidas e qualquer comunicação relacionada com a presente Política deve ser esclarecida com o Diretor de Compliance e Risco da Parcitas, devendo ser feita através do e-mail compliance@parcitas.com.br

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 aos normas e requisitos regulatórios, e no mínimo anualmente, o Diretor de Risco e Compliance deverá realizar testes de aderência/eficácia das métricas e procedimentos aqui previstos e/ou por si definidos e os resultados deverão ser objeto de discussão entre os membros do Comitê de Riscos e Compliance, sendo que eventuais deficiências e sugestões deverão constar no relatório anual de riscos e *Compliance*.

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 dos Negócios
Área de emissão:	Riscos e Compliance
Responsável:	Rodrigo Cefaly de Aranda Gatti

Data	Versão	Número de Páginas	Nome do Aprovador
10/04/2023	1.0	10	Comitê de Riscos e Compliance

parcitas

investimentos