Política de Continuidade de Negócios

Junho 2021

parcitas
investimentos

Objetivo

Definir as bases, princípios e regras para contingências e continuidade de negócios da Parcitas Gestão de Investimentos Ltda ("Parcitas").

A quem se aplica?

Sócios, administradores, diretores, funcionários, estagiários, prestadores de serviço/terceirizados contratados alocados nas dependências da gestora (doravante denominados "Colaboradores").

Responsabilidades

Caberá ao Diretor de Risco a avaliação das ocorrências de contingência, bem como de possíveis atualizações e aprimoramentos destes procedimentos, podendo fazer uso do Comitê de Risco e *Compliance* para registro e tomada de decisões.

Revisão e Atualização

Este PCN deverá ser revisado, validado, testado e atualizado a cada 12 (doze) meses, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

Contexto Operacional e de Negócios

Esta política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da Parcitas:

- ✓ A Parcitas executa suas atividades utilizando sistemas, sendo em sua maior parte acessíveis via WEB[1];
- ✓ Os fornecedores dos sistemas utilizados pela Parcitas se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da Parcitas. Tais obrigações constam de seus contratos, bem como procedimentos próprios de segurança e contingência;
- ✓ Os colaboradores da Parcitas estabelecem tratativas, e, formalizam seus entendimentos com clientes, corretoras e parceiros de negócios primordialmente por meio de ferramentas e aplicativos de mensagens (*"chats"*) e/ou *e-mail* corporativo, ou, por sistemas com acesso via WEB;

[1] Todos os sistemas do administrador fiduciário, custodiante, distribuidores, AAI e plataforma, são de acesso via WEB. Da mesma forma são acessíveis sistemas relativos a análises, notícias, corretoras e cotações de mercado (mesmo que com funcionalidades reduzidas, mas preservando aquelas consideradas elementares). O sistema de risco e algumas ferramentas desenvolvidas internamente, de apoio às operações de gestão, são acessíveis exclusivamente via rede da Parcitas, mesmo externamente, sendo passíveis de rotina alternativa caso haja indisponibilidade total de servidores (acessos primários ou de contingência).

- ✓ A Parcitas aloca recursos sob gestão, bem como distribui seus produtos, mediante a utilização de corretoras/plataformas de investimento acessíveis pela WEB ou telefone;
- ✓ Os arquivos contendo informações dos fundos e carteiras da Parcitas são armazenados nos servidores da Parcitas, com *back-ups* periódicos;
- ✓ A rede interna é acessível, e, espelhada via acesso externo VPN, mediante o uso de *login*/senha e dispositivos adequados de proteção e segurança;
- ✓ Os dispositivos eletrônicos utilizados no exercício das atividades da Parcitas, para obterem acesso a rede, necessitam de senha e criptografia;
- ✓ A Parcitas utiliza redes sem fio para fornecer acesso à WEB para seus colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas;
- ✓ Em caso de indisponibilidade, temporária ou de prazo mais longo para acesso à WEB, os colaboradores utilizam equipamentos e/ou redes/roteadores/*links* de *internet*/redes sem fio de redundância (seja no caso de trabalho no escritório ou remoto);
- ✓ O espaço físico/escritório da Parcitas deve ser o local preferencialmente utilizado para as atividades da gestora, reuniões e comitês com colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas da Parcitas estão parametrizados para serem passíveis de desempenhado de maneira remota;
- ✓ Todos os colaboradores da Parcitas estão também conectados via grupos de comunicação, tais como, Microsoft teams, *whatsapp* e sistemas de *Video Conference*.

Princípios e Obrigações

O PCN 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.

Para identificação dos **ativos críticos**[2] (posições, áreas e sistemas considerados críticos constam do Anexo I a este PCN), devem ser considerados os riscos a seguir, de impacto no caso de interrupção dos processos relativos à gestão:

a) impacto financeiro – situações em que a descontinuidade de negócios possa atingir, em diferentes graus, as carteiras ou fundos sob gestão, ou a situação financeira e patrimonial da Parcitas;

b) impacto legal – descontinuidade de negócios passível de gerar consequências legais aos fundos e carteiras sob gestão, seus cotistas, ou mesmo à própria Parcitas;

[2] **Todo e qualquer sistema, equipamento, arquivo, a exemplo, todo ativo essencial para o mínimo funcionamento da Parcitas, atendendo a suas obrigações legais críticas.**

c) impacto de imagem – risco de a descontinuidade de negócios impactar a reputação e confiabilidade da Parcitas perante seus clientes e/ou o público investidor;

d) acidentes, casos fortuitos e força maior – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle da Parcitas, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

Classificação de Riscos

A Parcitas adota a seguinte classificação de riscos, com as respectivas providências a serem tomadas:

- ✓ **Nível 1:** baixa probabilidade de impacto nas atividades da Parcitas, com monitoramento cotidiano para a sua prevenção. **Tem chance maior de ocorrência e frequência**;
- ✓ **Nível 2:** impacto potencial médio nas atividades da Parcitas e necessidade de maior nível de controles preventivos. **Tem chance moderada de ocorrência e frequência baixa**;
- ✓ **Nível 3:** riscos que devem ser incondicionalmente evitados, com impacto relevante nas atividades da Parcitas, com adoção de rigorosos controles preventivos. **Tem baixa chance de ocorrência, são eventos raros, porém de natureza extremamente grave**.

São classificados como nível 3:

- ✓ Falha grave de segurança/manutenção/atualização dos *softwares* e serviços críticos utilizados pela Parcitas no exercício de suas operações e monitoramentos periódicos e que resultam em inoperância[3];
- ✓ Interrupção do funcionamento de equipamentos utilizados pelos colaboradores da Parcitas que inviabilizem sua utilização nas atividades de operação e monitoramentos periódicos[4];
- ✓ Situações de indisponibilidade total dos serviços e sistemas das instituições administradoras e custodiantes dos fundos geridos pela Parcitas, bem como das plataformas utilizadas para distribuição de tais fundos[5];

[3] Que têm como medidas preventivas a obtenção dos respectivos Planos de Contingência dos provedores de tais *softwares* ou serviços, bem como o acompanhamento dos resultados periódicos dos testes de contingência aplicados e dos planos de ação estabelecidos para mitigar eventuais falhas identificadas em tais testes (quer sejam nas dependências da Parcitas ou nas dos fornecedores.
[4] Cuja medida preventiva inclui a manutenção *back-up* dos arquivos necessários para o desempenho das atividades cotidianas, de modo a sempre possibilitar a continuidade normal de suas atividades, mesmo em eventos de crise, quer seja nas dependências da Parcitas ou fora delas.
[5] Que tem como medidas preventivas a verificação as ações preventivas e de contingência de tais parceiros de negócio.

- ✓ Inacessibilidade quase total do time[6] de gestão, risco e *compliance*, não apenas fisicamente, mas, sem acesso a computadores, dispositivos móveis, sistemas, telefones, etc. que impeçam sua comunicação e exercício de suas funções por motivos quaisquer;
- ✓ Situações não diretamente relacionadas à Parcitas e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle e de porte grave (falta de acesso total físico e lógico);
- ✓ Desastres naturais, ou conjunturas sócias/econômicas fora do seu estrito controle, e, de natureza grave;
- ✓ Outras interrupções totais e graves de sistemas que coloque em risco os mecanismos adequados de gerenciamento de ativos e passivos dos fundos da gestora.

São eventos de nível 2:

- ✓ Situações não diretamente relacionadas à Parcitas e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle e de porte moderado (acesso moderado ou lento ao espaço físico ou intermitência de fornecimento de luz, *internet*, telefonia, água, etc.);
- ✓ Falhas ou descontinuidades de segurança/manutenção das instalações físicas, ferramentas e recursos tecnológicos da Parcitas, que gere intermitência das atividades;
- ✓ Inacessibilidade de parte significativa do time de gestão, risco e *compliance*, não apenas fisicamente, mas, sem acesso a computadores, dispositivos móveis, sistemas, telefones, etc. que impeçam sua comunicação e exercício de suas funções por motivos quaisquer;
- ✓ Interrupções parciais dos sistemas relacionados a gestão de ativos e passivos que não chegam a impedir a totalidade das operações, mas, geram risco de falha parcial na execução das compras e vendas e ativos, e, na execução de aplicações e resgates.

São considerados eventos de nível 1:

- ✓ Situações não diretamente relacionadas à Parcitas e/ou à sua diligência, tais como eventos do condomínio, desastres naturais ou conjunturas sociais/econômicas fora de seu estrito controle e de porte leve (falhas de ar condicionado, elevadores, que gerem situação atípica, mas, sem o prejuízo do funcionamento moderado de luz, i*nternet*, telefonia, água, etc. no acesso ou nas dependências da gestora);
- ✓ Inacessibilidade de alguns membros do time de gestão, risco e *compliance,* não apenas fisicamente, mas, sem acesso a computadores, dispositivos móveis, sistemas, telefones, etc. que impeçam sua comunicação e exercício de suas funções por motivos quaisquer;

[6] Nestes casos, medidas preventivas incluem a definição de substitutos para as posições chave devidamente treinados, habilitados e capacitados para atuar no desempenho das funções requeridas. Pode incorrer inclusive em comunicação à CVM de tal situação e mesmo a convocação de uma reunião estatutária de sócios e diretores da empresa, e, no caso dos fundos, no extremo, em uma discussão de soluções alternativas com o administrador e com a assembleia de cotistas.

- ✓ Interrupções parciais dos sistemas relacionados a gestão de ativos e passivos, mas, que não geram risco de falha parcial na execução das compras e vendas e ativos, e, na execução de aplicações e resgates.

Para fazer frente aos eventos diversos, de Nível 1, 2, ou 3, a seguir listaremos nossa estrutura de proteção, que visa atender a ocorrências nestes diversos níveis de gravidade, com maior rigor dos procedimentos de acionamento em situações extremas.

Estrutura de Prevenção e de Contingência Operacional

Controles Preventivos

- ✓ Identificação, treinamento e capacitação profissional de substitutos para exercer as atividades chave da operação da Parcitas;
- ✓ Controle de acesso às dependências da Parcitas;
- ✓ Respeito às normas de acesso estipuladas pelo condomínio no qual a Parcitas está sediada;
- ✓ Manutenção de provedores para acesso remoto, via VPN, a arquivos eletrônicos, planilhas e demais documentos de forma segura e transparente ao usuário, bem como dos respectivos *backups* desses materiais;
- ✓ Manutenção de sistema antivírus e *firewall* para salvaguardar os arquivos eletrônicos utilizados pela Parcitas;
- ✓ Servidores/provedores de serviços tecnológicos, de Dados, ferramentas contratadas, etc. – controles e redundâncias dos serviços de servidores e prestadores de serviço em ambiente em nuvem, com as devidas proteções antivírus, *firewall*, *back-up*, etc.
- ✓ *Backup* armazenado diariamente em ambiente em nuvem;
- ✓ Redundância de provedores de *internet* e telefonia (fixa x móvel).

A Parcitas conta com uma estrutura de contingência preparada para atender a quaisquer situações críticas que impossibilitem as áreas de negócio de exercerem suas atividades diárias, com recursos necessários e suficientes à continuidade das suas rotinas.

A Parcitas conta, ainda, com a estrutura operacional, computacional e processos de contingência de seus administradores dos seus fundos de investimento, seus custodiantes, corretoras e distribuidores.

Backup de Dados Local

Diariamente, a partir das 22 horas, todos os arquivos localizados na rede de arquivos e sistemas da Parcitas são copiados, de maneira automática, para:

- ✓ **O disco rígido (HD);**
- ✓ **Depois do backup em disco, é feito uma cópia em nuvem (Microsoft Azure), nosso *Backup Online*;**

O *backup* em disco ocorre diariamente e a retenção é de 30 dias. Todo o procedimento operacional acima descrito é de responsabilidade da área de TI da Parcitas.

Backup de Dados na Nuvem (Microsoft Azure)

O *backup* em nuvem da Microsoft se inicia a partir da 1 hora da manhã, diariamente, também nos finais de semana e feriados, sem exceção. A retenção dele é:

- ✓ ***Backup* Diário, ocorre todos os dias da semana: Retenção de 14 dias;**
- ✓ ***Backup* Semanal, ocorre toda sexta: Retenção de 8 semanas;**
- ✓ ***Backup* Mensal, ocorre no último dia do mês: Retenção de 5 anos.**

O procedimento operacional acima descrito será testado em periodicidade máxima trimestral. Faz parte do teste a recuperação de arquivos e sistemas do ano corrente e de anos anteriores. A responsabilidade pelo procedimento de avaliação é da área de *Compliance* da Parcitas. Estão contemplados neste procedimento todos os arquivos na rede e sistemas Parcitas.

Cabe ressaltar que não estão contemplados neste procedimento os arquivos localizados nos discos rígidos dos equipamentos utilizados pelos colaboradores, funcionários ou sócios. Portanto, os colaboradores não devem realizar a guarda de informações relevantes em seus discos locais.

Contingenciamento do fornecimento de energia

A Parcitas possui na sua infraestrutura uma redundância de energia elétrica em casos de falta da distribuição pela empresa contratada. O processo de contingenciamento é feito em 2 etapas, sendo elas:

- ✓ **Entrada automática de energia fornecida nobreak existente de 15 KvA (as baterias suportam 4 horas do escritório em plena função).**
- ✓ **Entrada automática do Gerador a diesel de 100 KvA, após 15 segundos da queda de energia. O gerador da Parcitas tem autonomia no seu tanque 180 litros de combustível reabastecível para suportar 7 horas de funcionamento total a Parcitas.**

Contingenciamento de *links* de *internet*

A Parcitas possui redundância de *links* de *internet* em sua infraestrutura operacional, listados abaixo:

- ✓ ***Link* primário corporativo *Full Duplex* de *Internet* de 200 MB com 5 IPs fixos da Mundivox;**
- ✓ ***Link* ADSL de 300 MB com 1 IP Fixo da empresa Vivo.**

Disaster Recovery

A Parcitas possui seus principais 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.

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.

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*.

Sistemas de Terceiros

A Parcitas utiliza a lista de sistemas de informação que dão suporte a sua operação, e tais provedores de serviço possuem mecanismos seguros que garantem sua continuidade:

- ✓ **Sistema de Risco (Lote45):** Desenvolvido pela Lote45 Ltda., este sistema é executado no data center *Hostway* (TIER nível máximo 3), provendo redundância em múltiplos datacenter em regiões distintas. O contrato de prestação de serviço provê um SLA rígido para manutenção do sistema em caso de indisponibilidade. No caso de contingência, acesso se dá via acesso externo à na rede da Parcitas;
- ✓ **Sistema de *Compliance* (COMPLIASSET):** No caso de contingência, acessível via WEB;

- ✓ **Sistemas do administrador fiduciário e custodiante (BNY Mellon):** No caso de contingência, acessível via WEB;
- ✓ **Sistemas dos distribuidores, Agentes Autonômos de Investimentos e Plataformas Digitais:** No caso de contingência, acessível via WEB;

- ✓ **Sistemas de mercado/cotações (*Bloomberg* e Valor Pro):** No caso de contingência, acessível via terminais externos/*mobile*.

Responsabilidades

Os procedimentos definidos a seguir compõem este PCN:

Procedimentos	**Periodicidade**	**Responsável**
Orientar e preparar as pessoas críticas para que estejam capacitadas para exercer tais atividades em situação de contingência.	Revisão anual, ou quando houver novos colaboradores e novas atividades.	Diretor de *Compliance* e Diretor de Risco.
Identificar e reavaliar os sistemas críticos, e atualizar este plano, bem como as listas de comunicação (telefones, grupos de *WhatsApp* e/ou e-mails) para contingência.		
Decidir pelo início da contingência.	Na efetiva ocorrência de incidentes.	Dois sócios e/ou dois Diretores, ou um sócio e um Diretor em conjunto (Anexo II)
Acionar o plano de contingência.	Após a decisão de início da contingência.	
Informação à equipe.	Após decisão pelo início da contingência na estrutura alternativa.	Diretores e/ou sócios.

Após a contingência, verificar o que motivou o incidente/crise, realizar avaliações, e, se o motivo é passível de ações de aprimoramentos de pessoas, sistemas, treinamentos ou novos procedimentos (inclusive do PCN).	Após a contingência.	Gestores das áreas, Diretor de *Compliance,* Diretor de Risco e com reporte e registro no Comitê de Risco.
Realizar testes do Plano.	Anualmente.	Diretor de *Compliance* e Diretor de Risco coordena com os gestores das respectivas áreas na Parcitas, levando a Comitê de Risco, e, incluindo sua análise no relatório anual de conformidade.

Anexo I

Atividades e Sistemas críticos

Quadro mínimo de profissionais com acesso aos sistemas, redes, etc. em situação de contingência
1 de Gestão
1 de Risco e *Compliance*

Sistemas críticos com acesso em situação de contingência
Sistemas de apoio a gestão: *Bloomberg* e Valor Pro com acesso via terminais externos/*mobile*.
Sistemas do administrador, plataformas e corretoras com acesso via WEB (ordens de compra e venda, aplicação e resgate, movimentações, saldos, etc.).
Sistema de gerenciamento de risco **Lote 45** com acesso externo via rede da Parcitas.
Sistema de *Compliance Compliasset* com acesso via WEB.
Pacote Office e demais ferramentas de apoio com acesso externo à rede local ou em máquinas de contingência.
E-mail: acesso via rede da Parcitas, via WEB ou em celulares.
Telefonia (fixa e/ou celular)

No caso de impossibilidade temporária ou definitiva de atuação do responsável junto à CVM pela administração de carteira de valores mobiliários, a Parcitas nomeará um responsável (temporário ou definitivo), devendo a CVM ser comunicada por escrito, no prazo de 1 (um) dia útil a contar da sua ocorrência, no caso de total ausência e necessidade de substituição do titular.

Anexo II

Pessoas Autorizadas a Iniciar Plano de Contingência e Continuidade de Negócios na Estrutura Alternativa

Responsável por gestão: Sr. Marcelo Ferman
Responsável por *Compliance*: Sr. Ana Laura Verdi Piccinin
Responsável por Risco: Sr. Bruno Andrade Soares
Demais autorizados (se aplicável): Sr. Maurício Nunes

Quaisquer das pessoas acima está autorizada a ativar o PCN na eventual ausência, por qualquer razão, das demais, de forma a sempre possibilitar a preservação ininterrupta das atividades da Parcitas.

Plano de Comunicação

A Parcitas utiliza, para comunicação, preferencialmente os seguintes meios:

- ✓ **Lista de colaboradores via *Whatsapp*; ou**
- ✓ **E-mail, acessado via remota; ou**
- ✓ **Ligações telefônicas; ou**
- ✓ **Microsoft Teams; ou**
- ✓ **SMS.**

Ao menos uma das formas acima serão utilizadas para comunicação de contingência, visando principalmente à efetividade e agilidade proporcionada por tais ferramentas em contextos dessa natureza.

A comunicação é iniciada pelos indivíduos mencionados acima, e enviada a todos os membros das respectivas equipes, de maneira a assegurar a pronta e eficiente comunicação da contingência em questão, em tempo hábil e oportuno.