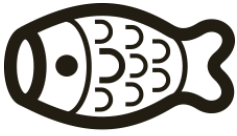


**CARPA**  
FAMILY OFFICE

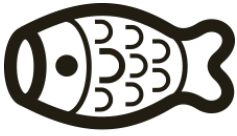
# **PLANO DE CONTINUIDADE DE NEGÓCIOS**

Propriedade da **CARPA FAMILY OFFICE**. Proibida a reprodução total ou parcial deste plano sem a devida autorização prévia.



## **CONTROLE DE VERSÕES**

| <b>VERSÃO</b> | <b>DATA</b> | <b>ELABORADOR/MODIFICADO POR</b>             | <b>DESCRIÇÃO</b> |
|---------------|-------------|--|------------------|
| 1ª            | 27/04/2016  | Felipe Rabaçal                               | Versão Original  |
| 2ª            | 02/01/2019  | Pedro Romeiro / Celso Casaro                 | 1ª Alteração     |
| 3ª            | 15/09/2020  | Pedro Romeiro / Celso Casaro                 | 2ª Alteração     |
| 4ª            | 26/03/2021  | Pedro Romeiro / Celso Casaro / Beatriz Guido | 3ª Alteração     |
| 5ª            | 27/12/2021  | Pedro Romeiro / Celso Casaro / Beatriz Guido | 4ª Alteração     |
| 6ª            | 05/04/2024  | Pedro Romeiro / Celso Casaro                 | 5ª Alteração     |



## **Sumário**

|  |    |
|--|----|
| 1. Da Introdução .....   | 4  |
| 2. Base Legal.....   | 4  |
| <i>Interpretação e Aplicação</i> .....                           | 4  |
| 3. Dos Objetivos .....   | 5  |
| 4. Das Etapas e Procedimentos para o Plano de Contingência ..... | 5  |
| 5. Das Considerações Finais.....                                 | 11 |
| 6. Da Revisão e Atualização .....                                | 11 |
| ANEXO I .....  | 12 |



## 1. Da Introdução

Este Plano de Continuidade de Negócios (“PCN”) estabelece estratégias e procedimentos a serem observados na eventualidade de incidentes ou emergências que envolvam as empresas que atuam no âmbito do mercado regulado pela CVM do grupo da Carpa Gestora de Recursos Ltda. e da Carpa Consultoria Financeira e Gestão Patrimonial Ltda (“Carpa Family Office”).

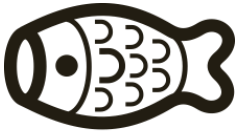
## 2. Base Legal

- (i) Resolução da Comissão de Valores Mobiliários (“CVM”) nº 21, de 25 de fevereiro de 2021, conforme alterada (“Resolução CVM 21”);
- (ii) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“Anbima”) de Administração e Gestão de Recursos de Terceiros (“Código de AGRT”); e
- (iii) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorreguladores aplicáveis às atividades da Gestora.

### Interpretação e Aplicação

Para fins de interpretação dos dispositivos previstos nesta Política, exceto se expressamente disposto de forma contrária: (a) os termos utilizados nesta Política terão o significado atribuído na Resolução CVM 175; (b) as referências a Fundos abrangem as Classes e Subclasses, se houver; (c) as referências a regulamento abrangem os anexos e apêndices, se houver, observado o disposto na Resolução CVM 175; e (d) as referências às Classes abrangem os Fundos ainda não adaptados à Resolução CVM 175.

As disposições da Política são aplicáveis aos Fundos constituídos após o início da vigência da Resolução CVM 175 e aos Fundos constituídos previamente a esta data que já tenham sido adaptados às regras da referida Resolução. Com relação aos Fundos constituídos antes da entrada em vigor da Resolução CVM 175, a Gestora e os Fundos permanecerão observando as regras da Instrução CVM nº 555, de 17 de dezembro de 2014, conforme alterada (“Instrução CVM 555”), e de outras instruções aplicáveis às diferentes categorias de Fundos sob gestão, especialmente, no que diz respeito às responsabilidades e atribuições da Gestora, enquanto gestora da carteira dos Fundos, até a data em que tais Fundos estejam adaptados às disposições da Resolução CVM 175.



### 3. Dos Objetivos

Como estratégia para atingir nosso objetivo principal, são definidos como objetivos específicos:

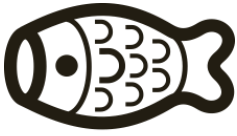
- a) Realizar *backup* diário de todo o banco de dados, envolvendo todas as operações diárias, incluindo os arquivos de programas;
- b) Assegurar a integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações;
- c) Manter os sistemas operacionais disponíveis; e
- d) Manter rede eletrônica em funcionamento e em boas condições operacionais. Para redução e controle de eventuais perdas com contingências, todos os colaboradores da Carpa Family Office 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.

### 4. Das Etapas e Procedimentos para o Plano de Contingência

#### Continuidade dos Negócios: Estrutura Operacional

São fatores que integram o Plano de Continuidade de Negócios da Carpa Family Office:

- (a) manutenção no quadro funcional da Carpa Family Office de profissionais experientes no mercado financeiro com dedicação exclusiva à empresa;
- (b) a existência do Diretor de Compliance, que, dentre outras funções, concentra a responsabilidade pelo suporte a todas as áreas da Carpa Family Office no que concerne a esclarecimentos de todos os controles e regulamentos internos (*Compliance*), bem como no acompanhamento de conformidade das operações e atividades da Carpa Family Office com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento



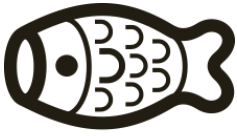
de prazos e do nível de excelência dos trabalhos efetuados, além de assegurar que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*);

- (c) a existência de equipe de um Departamento de Tecnologia, Segurança da Informação e Segurança Cibernética, sendo esta fundamental para o funcionamento da Carpa Family Office, no sentido de que todas as comunicações com corretoras (quando aplicável), administradores de fundos etc., são realizadas por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios), sendo também fundamental para a realização de registros de operações; e
- (d) a manutenção da plena capacidade operacional do escritório, sendo este o espaço físico onde são realizadas as operações da Carpa Family Office e onde encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades, sem prejuízo do acesso remoto quando necessário por 100% dos Colaboradores.

Tais fatores colaboram não só para melhor direcionar a aplicação de recursos pela Carpa Family Office, mas também para incrementar o gerenciamento de riscos, conferir melhor fluidez ao fluxo de informações e ao processo decisório da Carpa Family Office e para atendimento às necessidades mínimas de manutenção dos seus serviços/atividades.

Tendo identificado os fatores principais que integram seu Plano de Contingência do ponto de vista da estrutura da Carpa Family Office e dos processos sob sua responsabilidade, os riscos que podem ocasionar o acionamento do plano de contingência foram identificados da seguinte forma:

- (i) Problemas de Infraestrutura: 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 Carpa Family Office, etc.; e
- (ii) Problemas de acesso ao local/recursos: os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso ao local onde se localiza o escritório. Essa impossibi-



lidade pode ser causada por eventos como greves, por exemplo, de transporte público, interdições pelas autoridades do prédio ou do entorno dos escritórios da Carpa Family Office, pandemias, etc.

Com base no levantamento da estrutura da Carpa Family Office e no mapeamento de riscos, a Carpa Family Office tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações.

Neste sentido, conforme avaliação de risco da Carpa Family Office, foram definidos 2 ambientes básicos que devem ser considerados nas ações a serem tomadas quando da ativação deste Plano de Contingência. Esses ambientes são: Físico e o Tecnológico.

**(i)** Ambiente Físico

O ambiente físico é definido como o espaço onde as operações diárias da Carpa Family Office são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e equipamentos necessários a essa operação, como também o acesso seguro a esses recursos.

Em ocorrendo situações de problemas de acesso às suas dependências, a equipe da Carpa Family Office deve continuar a desempenhar suas atividades a partir do plano de contingência.

O referido plano contempla acesso remoto ao ambiente Carpa Family Office na nuvem, através do qual, os usuários-chaves para continuidade dos negócios têm, através de uma VPN e seu login único e individual de usuário, acesso a todos os sistemas e arquivos necessários para realizar suas atividades. Independentemente do acesso dos usuários-chave, a Carpa Family Office está capacitada a operar com 100% da equipe em ambiente remoto em formato de *home office*.

**(ii)** Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a Carpa Family Office possa realizar sua operação de forma normal.



Isso implica basicamente na disponibilidade de acesso aos sistemas utilizados pela empresa em seu dia a dia, e na garantia de que suas informações estejam protegidas, e possam ser acessadas e/ou utilizadas na operação da empresa, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, *softwares* e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

Todos os sistemas utilizados pela Carpa Family Office no ambiente das áreas de Gestão, Risco e Consultoria são acessados através de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da Carpa Family Office. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência, para que estes também tenham conhecimento da situação, de forma a impactar o mínimo possível a operação.

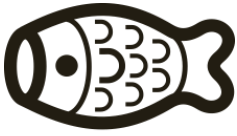
A Carpa Family Office conta com colaboradores que prestam serviços de Tecnologia, Segurança da Informação e Segurança Cibernética (a “Equipe de TI”), os quais estarão 100% disponíveis na hipótese de uma situação de contingência.

As informações relativas a *backup*, *hardware*, *firewall*, servidores, telefonia, rede, *e-mails* etc. encontram-se no Anexo I deste Plano de Contingência, e mais detalhadamente na Política de Segurança da Informação e Segurança Cibernética da Carpa Family Office, conforme disposta via intranet (Microsoft Teams / Microsoft Sharepoint) e no site da Carpa Family Office (a “Política de SI e SC”).

➤ Equipe de Contingência

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





- Diretor de Compliance (Coordenador de Contingência);
- Diretor de Gestão (Responsável pela definição de prioridades da área de gestão e operações a serem operadas em modo de contingência);
- Diretor de Consultoria (Responsável pela definição de prioridades da área de consultoria em modo de contingência); e
- Diretor de Tecnologia, Segurança de Informação e Segurança Cibernética (responsável pela coordenação dos trabalhos de contingência do âmbito tecnológico).

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 e deve ser comunicada imediatamente a todos os colaboradores da Carpa Family Office. O Coordenador de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com a Equipe de TI da Carpa Family Office, para comunicar o modo contingencial e tratar do acesso aos dados/sistemas.

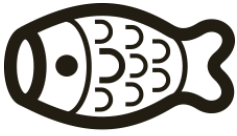
➤ Cenários de Contingência

A ocorrência de eventos de contingência deverá ser avaliada pela Equipe de Contingência da Carpa Family Office e, com base nas informações disponíveis, deverá ser tomada uma decisão quanto ao acionamento do plano de contingência.

Com base na decisão tomada pela Equipe de Contingência, a Carpa Family Office deverá adotar os procedimentos a seguir listados.

➤ Situação de Contingência

Neste cenário, considera-se basicamente a impossibilidade ou dificuldade em manter o funcionamento normal da empresa devido a problemas de ordem técnica (*hardware*), física (acesso ao escritório), pessoal (ausência significativa de funcionários) e de infraestrutura (falta de energia).



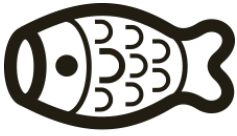
Nessa situação, o Diretor de Compliance deverá acionar este plano de contingência em caráter imediato e iniciar a avaliação das causas que geraram a contingência, para providenciar sua solução o mais rapidamente possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo, quais sejam:

- (a) Comunicar imediatamente o ocorrido a toda a equipe interna, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição, indicando nessa oportunidade qual o procedimento a ser adotado por cada colaborador de acordo com a contingência ocorrida; e
  
- (b) Caso seja verificada a necessidade de sair do escritório físico da empresa, os colaboradores poderão continuar a desempenhar suas atividades através de *Home Office*, uma vez que todos os arquivos podem ser acessados pela nuvem e há equipamentos para que 100% dos Colaboradores possam trabalhar em lugar externo. Em havendo necessidade, a equipe da Carpa Family Office irá se reunir no site de Contingência no RJ ou em escritórios compartilhados (*coworking*) que dispõe de ambiente e infraestrutura para tanto, e prosseguirá com a gestão remota dos fundos sob sua gestão e, conforme o caso, consultoria de valores mobiliários. A continuidade das operações da Carpa Family Office deverá ser assegurada no próprio dia útil da ocorrência da contingência no escritório físico, de modo que as atividades diárias não sejam interrompidas ou gravemente impactadas.

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

➤ Testes

Semestralmente são realizados testes efetivos de utilização do site de contingência, verificando se tudo está funcionando como deveria, exceto em períodos de pandemia com restrição de acesso ao escritório, em que o plano de contingência será aplicado de maneira contínua.



Ademais, é responsabilidade do Diretor de Compliance manter este plano de contingência atualizado, bem como a realização de reavaliação a cada 12 meses dos procedimentos estabelecidos como um todo neste Plano de Contingência.

Neste sentido, o Diretor de Tecnologia, Segurança de Informação e Segurança Cibernética realizará testes de contingências exigidos pelo Compliance (além do teste relativo ao site de contingência) que possibilitem que a Carpa Family Office esteja preparada para eventos desta natureza, proporcionando à Carpa Family Office condições adequadas para continuar suas operações.

Sendo assim, anualmente, é realizado um teste de contingência para verificar:

- a) Acesso aos sistemas;
- b) Acesso ao e-mail corporativo;
- c) Acesso aos dados armazenados; e
- d) Qualquer outra atividade necessária para continuidade do negócio.

O resultado do teste, se no todo ou em parte for falho, deve ser registrado em relatório por e-mail pelo referido Diretor ao Diretor de Compliance, que servirá como indicador para regularização das falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

## **5. Das Considerações Finais**

Todas as dúvidas sobre as diretrizes deste Plano podem ser esclarecidas com a área de Compliance.

## **6. Da Revisão e Atualização**

O presente Plano entra em vigor na data de sua publicação e deverá ser revisto e, se necessário, atualizado pelo Compliance, no mínimo a cada 24 meses. Para tanto, serão utilizadas como base para sua atualização as legislações, instruções normativas e regulamentações vigentes na data da sua revisão.



## **ANEXO I**

### Rede

A rede da Carpa Family Office contém um *Active Directory* (AD) que faz o gerenciamento de Diretiva de Grupo e Diretivas de Conta para todo o domínio integrado ao ambiente na nuvem. Para acessar a rede da Carpa Family Office é necessário ingressar no domínio e ter permissões registradas no *firewall*. Funcionários e dispositivos previamente autorizados devem ser cadastrados no AD/Entra, para que fiquem em conformidade com as políticas de grupo. O uso de dispositivos pessoais para acesso a rede é extremamente restrito, sendo permitido apenas após inspeção da área de tecnologia e em conformidade com a política de segurança.

A Carpa Family Office possui um sistema de *firewall* com equipamentos redundantes em cada site. Esse é um sistema moderno com diversas políticas e configurações para impedir acessos, de terceiros, as informações que trafegam na rede, bloqueio de acesso dos colaboradores a sites que violem a política de segurança da companhia e sistemas de proteção de ponto de extremidade com inspeção de pacotes, detectando e impedindo ameaças antes que elas cheguem à rede.

O *firewall* gerencia as conexões VPN entre os escritórios e a nuvem.

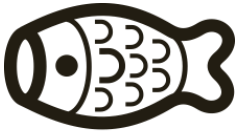
A rede pode ser acessada remotamente através de uma VPN direta com a nuvem, conectando o usuário aos sites de SP e RJ, com os devidos acessos e autorizações cadastrados na nuvem e integrados ao *firewall*, utilizando o login único e individual disponibilizado pela área de tecnologia.

### Banco de Dados

Os bancos de dados ficam localizados na nuvem, acessos diretos aos dados são permitidos apenas pelos administradores de banco de dados e sócios. Cada administrador ou sócio possui uma senha individual.

### Servidores

A Carpa Family Office possui 4 servidores em nuvem, 1 servidor físico com 2 máquinas virtuais no escritório do Rio de Janeiro e 2 servidores físicos com 4 máquinas virtuais no escritório de São Paulo.



Os servidores na nuvem são responsáveis por armazenar todos os dados, sistemas e bancos de dados da companhia, e estão divididos da seguinte forma: 1 servidor controlador de domínio, 1 servidor de aplicação e banco de dados, 1 servidor de arquivos e 1 servidor para acesso remoto as aplicações legadas ou sensíveis.

Os servidores locais são réplicas do controlador de domínio e *proxies* para monitoramento da infraestrutura, além de executar funções secundárias para o funcionamento operacional da empresa.

### Backup

O *backup* dos bancos de dados é efetuado de hora em hora e armazenados em outros servidores da nuvem

O *backup* das máquinas virtuais é executado automaticamente e armazenado na nuvem, seguindo o padrão da política de segurança e redundância da provedora (Azure – Microsoft).

Seguindo as definições da política de *backup*, o processo dá-se:

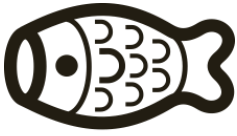
- diariamente, armazenado por 90 dias;
- semanalmente, armazenado por 52 semanas;
- mensalmente, armazenado por 60 meses; e
- anualmente, armazenado por 10 anos.

### Permissão de Acesso

O acesso aos arquivos na nuvem é controlado por níveis de acordo com a função de cada colaborador na companhia, através de um login único e individual, fornecido pelo departamento de tecnologia da informação quando solicitado pelo gestor da área em conformidade com as políticas de segurança da companhia. Apenas pessoas devidamente autorizadas têm acesso remoto aos servidores.

### Telefonia

O sistema de telefonia é composto por 3 contratos distintos com 2 provedores (OI, Net2Fone e L5), sendo entregues no Rio de Janeiro e nuvem. Os equipamentos são integrados entre si e com o aplicativo de comunicação Microsoft Teams, oferecendo um ramal para todos os colaboradores.



### Gravação Telefônica

A Carpa Family Office possui um sistema de gravação local e em nuvem das ligações internas e externas, efetuado em tempo real.

Diariamente, é executado um processo automático de transferência das gravações locais para o servidor de arquivos na nuvem, quando o disco desse servidor atinge certos limites. Em um processo manual, esses arquivos são transferidos para uma conta de armazenamento frio na nuvem.

### Internet

A disponibilidade de internet dá-se por 4 contratos distintos, sendo no Rio de Janeiro entregue pelas provedoras: Mundivox, 1 link dedicado de 200Mb, via fibra óptica; NET, 1 link ADSL de 120Mb, via cabo coaxial;

A distribuição dos serviços de internet no site de São Paulo é entregue por: Mundivox, 1 link dedicado de 300Mb via fibra óptica; Hostfiber, 1(um) link dedicado de 100Mb, via fibra óptica,;

### Eletricidade

O sistema de redundância de fornecimento de energia elétrica da Carpa Family Office conta com 1 *nobreak* em São Paulo e 3 *nobreaks* e 1 gerador no Rio de Janeiro. Em casos de falha do fornecimento pela concessionária, os *nobreaks* impedem a queda de energia e, em seguida, o gerador é acionado automaticamente.

### Manutenção

Os equipamentos são, em sua maioria, adquiridos da DELL, onde, os desktops/laptops têm 3 anos de garantia, e os servidores, 5 anos.

Manutenções preventivas são realizadas a cada 3 anos para os *nobreaks*, anualmente para os geradores e equipamentos de ar-condicionado, por empresas terceiras especializadas. Além disso, são efetuadas verificações periódicas e reparos quando necessário.