

# *Plano de Continuidade de Negócios*

## PLANO DE CONTINUIDADE DOS NEGÓCIOS

### 1. Objetivo

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal, a Persevera possui uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada funcionário, administrador ou colaborador na execução do Plano de Continuidade de Negócio (“PCN”).

O PCN é um plano traçado para que seja possível dar continuidade à execução de atividades consideradas críticas para a prestação de serviços pela Persevera, de forma que os interesses dos clientes da Persevera não sejam prejudicados.

O PCN estabelecido neste Manual é de responsabilidade do Diretor de Risco e Compliance, a quem cumprirá garantir que o PCN esteja em concordância com as leis e normas dos órgãos reguladores cabíveis, bem como zelar por sua atualização e cumprimento do cronograma de treinamento previsto.

Na eventual ocorrência de qualquer evento que impossibilite seu acesso ou permanência nas dependências da Persevera, os Colaboradores devem imediatamente contatar o Diretor de Risco e Compliance que avaliará as atividades em andamento e orientará os Colaboradores quanto à continuidade das atividades fora das dependências da Persevera, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

### 2. Principais contingências mapeadas e respostas do PCN

Apresentamos os riscos potenciais identificados diretamente relacionados à continuidade dos negócios e as principais contingências mapeadas e respostas do PCN (os riscos associados à Infração de Segurança de Sistemas são apresentados no item “Segurança Cibernética”):

#### 1. Falha no fornecimento de energia

Todos os colaboradores possuem laptops (baterias) e em caso de falta de energia, a empresa possui um No-break para até 5 (cinco) horas. Em caso de períodos maiores que 5 (cinco) horas, o acesso dos dados e arquivos deve ser feito remotamente.

O Diretor de Risco e Compliance é o responsável em monitorar e avaliar a situação e orientar os demais colaboradores quanto à continuidade das atividades fora das dependências da Persevera, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

#### 2. Queda do link para acesso à internet

Dois links redundantes de operadoras diferentes. Caso nenhuma das contingências funcionem, é possível fazer o acesso remoto aos arquivos hospedados na nuvem, que podem ser acessados através de outros provedores.

O responsável por TI é o responsável em monitorar e avaliar a situação e buscar, dentre as contingências supracitadas, as melhores alternativas.

#### 3. Sistema do administrador inoperante

Caso o sistema do administrador esteja inoperante e não seja possível executar as atividades de importação e exportação de informações, a mensageria será feita por email e/ou telefone. Além disso, o sistema Lote45 será utilizado a fim de obtenção e uma ‘cota-espelho’ e batimento de quantidades e operações junto às corretoras.

#### 4. Impossibilidade de executar as ordens junto às corretoras

As ordens serão primariamente executadas pelos operadores junto às corretoras de forma eletrônica e/ou de forma verbal e/ou escrita (as ordens verbais deverão ser sempre realizadas através de ligações telefônicas gravadas).

Uma vez realizada a ordem e concretizada a negociação, as operações serão automaticamente atualizadas no sistema de portfólio compliance e gerenciamento de risco de mercado através do sistema ‘trades hunter’ do Lote45 e os gestores, bem como a área de risco e performance, poderão acompanhar as operações *on-line*.

#### 5. Falha de hardware Monitor e Laptop

Contingência Monitor: monitor laptop + monitor reserva

Contingência Laptop: laptop reserva

#### *6. Falha do armazenamento de dados na nuvem*

A Gestora trabalha com o backup de seus dados na nuvem, possibilitando o acesso à pelo menos as últimas 30 (trinta) versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).

Todos os dados e arquivos da Gestora, do banco de dados dos clientes e os modelos dos analistas são armazenados na nuvem.

Contingência: SLA 99,9% + Backup Nuvem-Nuvem

O responsável por TI é o responsável em monitorar e avaliar a situação e buscar, dentre as contingências supracitadas, as melhores alternativas.

#### *7. Falha de Software COMPLILLY e Falha de Software Lote45*

Contingência: Fornecedores apresentam servidores redundantes e sincronizados

#### *8. Falha de Software Bloomberg, Valor Pro e Broadcast*

Contingência: em caso de falha de 01 (ou 02 softwares simultaneamente) haverá sempre, no mínimo, um terceiro fornecedor de Market Data

#### *9. Contingências para e-mail*

Serviço de e-mail é hospedado em nuvem, com redundância e acordo de nível de serviço elevados, garantindo a continuidade do acesso remoto. Há possibilidade de comunicação nos celulares dos funcionários e via chat do Bloomberg.

#### *10. Contingências com serviço de telefonia*

Contrato de suporte com prazo de atendimento para suporte à central de telefonia. Disponibilidade de linha telefônica de backup fornecida pela provedora de internet. Há possibilidade de comunicação nos celulares dos funcionários e via chat do Bloomberg.

#### *11. Acesso Remoto*

Com o propósito de permitir o acesso remoto de seus funcionários, a Gestora disponibiliza notebooks que poderão ser utilizados por seus Colaboradores de suas próprias residências. Adicionalmente, possui infraestrutura para acesso por meio de ambiente seguro, utilizando virtual private network ("VPN")

#### *12. Instalações Indisponíveis por conta de incêndio/desastres, etc*

Na impossibilidade de se utilizar o espaço físico do escritório, os colaboradores deverão utilizar seus laptops pessoais - que serão configurados com os mesmos sistemas utilizados em produção.

O Diretor de Risco e Compliance é o responsável em monitorar e avaliar a situação e orientar os demais colaboradores quanto à continuidade das atividades fora das dependências da Persevera, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

### **3. Validação e/ou testes**

Alguns riscos potenciais supracitados poderão ser validados e testados à medida que situações específicas ocorrerem já que não são eventos extremamente raros (falha de energia e queda de link da internet, por exemplo).

De qualquer forma será criada uma rotina de testes anual onde algumas situações específicas serão simuladas a fim avaliar se as contingências desenvolvidas são capazes de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da instituição e manter a integridade, a segurança e a consistência dos bancos de dados e se os planos adotados podem ser ativados tempestivamente.

O Diretor de Risco e Compliance é responsável pela atualização e cumprimento do cronograma de testes.

### **4. Disposições Gerais**

Em cumprimento a Resolução CVM n.º 21/21, ao "Código ANBIMA de Regulação e Melhores Práticas para os Fundos de Investimento" e ao "Código ANBIMA de Melhores Práticas de Gestão de Patrimônio Financeiro no Mercado Doméstico", o presente Plano descreve os procedimentos adotados em caso de contingências e desastres, visando sempre cumprir o dever fiduciário da Gestora

## **5. Endereço Eletrônico**

A presente Política está disponível no endereço eletrônico da Gestora: <http://www.persevera.com.br>

Eventuais comunicações para a Área de Gestão de Riscos e de Compliance devem ser enviadas para [compliance@persevera.com.br](mailto:compliance@persevera.com.br)

## **6. Revisões e Atualizações**

Esta Política será revisada anualmente. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência. A Área de Gestão de Riscos e de Compliance informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Gestora na Internet

## **7. Vigência**

Esta Política revoga todas as versões anteriores e passa a vigorar na data de sua aprovação pelo Comitê de Gestão de Riscos e de Compliance.