



PLANO DE CONTINUIDADE DE NEGÓCIOS
CVPAR INVESTIMENTOS LTDA.

Agosto de 2023.

1.	INTRODUÇÃO.....	3
2.	OBJETIVO DO PCN	4
3.	CENÁRIOS E ABRANGÊNCIAS.....	4
4.	AMEAÇAS RELACIONADAS	4
4.1.	HUMANAS	4
4.2.	TECNOLÓGICAS.....	4
4.3.	NATURAIS.....	5
5.	ABRANGÊNCIAS.....	5
6.	SITE PRINCIPAL E SITE DE CONTINGÊNCIA.....	6
7.	EQUIPE DE CONTINGÊNCIA	6
8.	PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE.....	7
8.1.	DEFINIÇÃO DE DESASTRE:.....	7
8.2.	MONITORAÇÃO E COMUNICAÇÃO DE EVENTOS	7
8.3.	DECLARAÇÃO DE DESASTRE /CONTINGÊNCIA:	7
9.	AÇÕES E PROCEDIMENTOS EM SITUAÇÕES DE CONTINGÊNCIA	9
9.1.	DESLOCAMENTO DO PESSOAL	9
9.2.	ACIONAMENTO DO SERVIDOR DE CONTINGÊNCIA E SISTEMAS.....	9
9.3.	ACIONAMENTO DE TELEFONIA DE CONTINGÊNCIA	9
10.	PROCESSOS CRÍTICOS	9
10.1.	PROCESSOS X ATIVIDADES CRÍTICAS.....	10
10.2.	PROCESSOS X SISTEMAS CRÍTICOS	11
10.3.	PROCESSOS X RECURSOS HUMANOS (MÍNIMO PARA CONTINGÊNCIA).	12
11.	A ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIOS.....	13
12.	PROCEDIMENTOS DE RETORNO À NORMALIDADE - SITE PRINCIPAL	14
13.	ADMINISTRAÇÃO DO PLANO	15
13.1.	DIVULGAÇÃO E TREINAMENTO	15
13.2.	REALIZAÇÃO DE TESTES.....	16
14.	GLOSSÁRIO.....	17

1. INTRODUÇÃO

O Plano de Contingência e Continuidade de Negócios (“PCN”) é um processo proativo de planejamento que assegura que uma organização possa sobreviver a uma crise organizacional, com identificação das funções críticas e das possíveis ameaças a essas funções e da continuação das mesmas, o qual é elaborado em conformidade com os termos dos Códigos aplicáveis da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA (“ANBIMA”) e com a regulamentação expedida pela Diretoria da ANBIMA.

É um conjunto de procedimentos a serem executados para restaurar os sistemas de processamento de dados e ambientes operacionais com a máxima rapidez e o mínimo impacto à **CVPAR INVESTIMENTOS LTDA.** (“CVPAR”).

A maioria das interrupções é temporária, com as condições retornando ao normal dentro de um período considerado como não crítico para o ambiente de negócios.

Outras interrupções podem rapidamente se desenvolver em períodos mais longos os quais podem prejudicar severamente a capacidade de uma organização em fornecer serviços.

Se a capacidade em fornecer serviços estiver prejudicada, a base do cliente decai e a participação no mercado é impactada, principalmente a imagem. Para minimizar o impacto, as equipes de contingência definidas devem ser treinadas nas suas respectivas responsabilidades para garantir que todos os recursos conhecidos e disponíveis sejam utilizados para evitar que uma emergência se torne um desastre.

O desenvolvimento do PCN é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo as suas principais etapas:

- Análise de riscos de TI;
- Análise de Impacto nos Negócios (BIA); e
- Estratégia de recuperação.



Desta forma, simular emergências, definir responsabilidades de atuação para cada colaborador na execução do PCN, e, acima de tudo, mantê-lo atualizado, são fatores críticos de sucesso.

2. OBJETIVO DO PCN

O objetivo do presente PCN é estabelecer parâmetros pelos quais as atividades das áreas definidas como críticas, relacionadas às prestações de serviços e de negociação nos segmentos de Bolsa em que a CVPAR atua, serão atendidas com o menor impacto aos nossos clientes internos e externos.

3. CENÁRIOS E ABRANGÊNCIAS

Neste PCN os cenários foram divididos em dois grandes eventos:

- a) Impossibilidade de acesso ao prédio; e
- b) Falha na infraestrutura Tecnológica (envolvendo TI/Telefonia).

4. AMEAÇAS RELACIONADAS

No entendimento dos gestores das áreas avaliadas, baseado no resultado da Análise de Impacto nos Negócios (BIA), as ameaças com grau de vulnerabilidade significativa estão divididas em:

4.1. HUMANAS

Manipulação Indevida de Dados e Sistemas, Distúrbio Civil, Vírus de Computador, Falha de Prestador de Serviços/Parceiro, Roubo e/ou Furto de Recursos, Sequestro de Dados e informações, Acesso Indevido às Instalações e Erro Humano (não intencional).

4.2. TECNOLÓGICAS

Falha em Aplicativo (SW), Falha em Hardware (HW), Falha em sistemas Operacionais, Falha em Rede Interna, Falha em Telecom - Voz, Falha em Rede Externa, interrupção



de Energia Elétrica, Falha em Instalações Elétricas, Falha de Telecom - Dados, e Falha em Sistema Aplicativos.

4.3. NATURAIS

Queda de Raios, Vendaval e incêndio.

Cabe ressaltar que, paradas não programadas resultam também em perdas intangíveis aos negócios da CVPAR, as quais impactam de forma negativa na confiança da CVPAR em seus Colaboradores. Desta forma, os potenciais impactos numa eventual interrupção no negócio são:

- Interrupção de prestação de serviços a clientes;
- Multas e sanções;
- Perda da capacidade de gestão e controle;
- Comprometimento da imagem da CVPAR; e
- Exposição negativa na mídia e perda de vantagem competitiva.

5. ABRANGÊNCIAS

O PCN foi construído para minimizar o impacto de um evento, estabelecer a operação mínima após a interrupção até o retorno à normalidade, bem como para identificar os sistemas que dão suporte aos processos de negócios e de TI (sistemas, aplicativos, banco de dados, links de comunicação e de dados). Assim, este PCN abrange as seguintes áreas:

- Cadastro;
- Backoffice – Fundos;
- Backoffice – B3 S.A. - Brasil, Bolsa, Balcão (“B3”);
- Contabilidade;
- Risco;
- TI; e



- Gestão.

6. SITE PRINCIPAL E SITE DE CONTINGÊNCIA

A unidade de São Paulo, Localizada Av. Brigadeiro Faria Lima, 3477, Conjunto 83A – Torre A, Itaim Bibi, CEP 04.538-133. O Site de Contingência está localizado na Rua Luis Dib Zogaib, número 197, Jd. Guedala – São Paulo – SP, CEP 05613-020 e está dimensionado para atender os processos de negócio críticos.

Ainda, hipótese em que Site de Contingência também esteja indisponível, será viabilizado aos Colaboradores que executem Atividades Críticas o acesso remoto às informações, sistemas e ferramentas necessárias à continuidade de suas funções.

7. EQUIPE DE CONTINGÊNCIA DO PCN

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

- Diretor de Compliance e Risco (Líder de Contingência); e
- Diretor de Investimentos.

Essas pessoas deverão tomar as decisões necessárias para acionar este PCN 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 CVPAR. O Líder de Contingência entrará em contato (ou pedirá para que algum dos outros Diretores entre em contato) com a empresa terceirizada responsável pela Tecnologia da Informação da CVPAR, 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.



8. PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

8.1. DEFINIÇÃO DE DESASTRE:

Será desastre quando o tempo de recuperação do negócio for maior do que o tempo máximo suportado pela CVPAR sem os recursos que suportam a operação ou em decorrência da impossibilidade de acesso à instalação. Os tempos estão descritos no item - **Estratégia de Continuidade de Negócios**.

8.2. MONITORAÇÃO E COMUNICAÇÃO DE EVENTOS

Num evento de crise somente serão divulgadas informações das quais se tenha 100% de certeza, mesmo que isto prejudique a agilidade. Informações contraditórias contribuem para agravar a situação de crise.

Qualquer colaborador da CVPAR ao constatar uma anormalidade que impacte sua atividade operacional deverá comunicar ao seu superior imediato, e esse informará ao Líder de Contingência.

Este é o meio de comunicação a ser utilizado pelos colaboradores da CVPAR como ponto central de contato para solicitar ajuda ou relatar alguma situação que demanda o acionamento ou não da contingência.

8.3. DECLARAÇÃO DE DESASTRE /CONTINGÊNCIA:

Ocorrido algum evento que paralise alguma operação essencial ao negócio, o Líder de Contingência avalia o impacto da ocorrência nas atividades da CVPAR. Com base nas



informações recebidas e avaliando o grau de impacto, horário crítico e outros fatores, compete ao Líder de Contingência declarar ou não a contingência

9. AÇÕES E PROCEDIMENTOS EM SITUAÇÕES DE CONTINGÊNCIA

O Líder de Contingência irá comunicar o fato à Equipe de Contingência para que em conjunto possam avaliar o impacto do evento. Compete ao gestor de cada processo executar os procedimentos para continuidade das atividades relativas à sua área.

9.1. DESLOCAMENTO DA EQUIPE DE CONTINGÊNCIA.

Caso a contingência seja acionada, o deslocamento da Equipe de Contingência será realizado por meio de Taxi ou Metrô, sempre buscando a melhor alternativa e redução de tempo para chegada ao Site de Contingência.

9.2. ACIONAMENTO DO SERVIDOR DE CONTINGÊNCIA E SISTEMAS

Ao chegar ao Site de Contingência, é acionado o servidor *cloud standby*, de forma que o acesso aos arquivos seja idêntico ao servidor principal. O acesso aos sistemas de controle e e-mails será feito via web. O servidor e-mail mantém um histórico de 10 dias no webmail.

9.3. ACIONAMENTO DE TELEFONIA DE CONTINGÊNCIA

Na impossibilidade de acesso ao Site Principal, as linhas principais são transferidas a distância pelo servidor de telefonia para o Site de Contingência, ou seja, as chamadas são transferidas para o tronco de Contingência.

Na impossibilidade de acesso ao Site de Contingência, as linhas principais serão transferidas para o celular dos colaboradores que executem Atividades.

10. PROCESSOS CRÍTICOS



Processos, atividades e sistemas críticos podem ser definidos como um processo de trabalho que uma vez paralisado por tempo superior ao definido pela CVPAR irá afetar sensivelmente as operações e serviços gerando maior impacto aos clientes internos e externos.

O resultado dessa etapa é resultante da Análise de Impacto nos Negócios (BIA) realizada com os principais gestores dos processos, indicando os recursos humanos e tecnológicos mínimos para atendimento.

10.1. PROCESSOS X ATIVIDADES CRÍTICAS

Área	Processo	Atividade crítica
BackOffice Fundos	Cálculo de quotas de Fundos. Zeragem de Caixa — Fundos. Envio de Movimentações do dia para o Administrador. Aprovação de Operação no sistema do Custodiante.	Enviar informações aos Órgãos Reguladores e Administrador dos Fundos. Verificar CAIXA (aplicações, resgates e Movimentações gerais dos cotistas) para não estourar nenhum limite.
Contabilidade	Impostos. Contabilização. Contas a Pagar e Receber.	Recolhimento de impostos no devido prazo. Pagamentos e Recebimentos.
BackOffice – B3	Liquidação Diária com a B3. Coberturas de Margem e Movimentação de Garantia.	Verificar o atendimento da necessidade de Cobertura de Margem e Movimentação de garantia. Retirada ou depósitos de ativos. Vinculação de ativos.

		<p>Comunicação com Bolsas ou Bancos.</p> <p>Confirmar Ordens.</p> <p>Alinhamento de conta corrente e cadastro para liberação das Transferências.</p> <p>Liquidação das operações com o Custodiante.</p>
Risco	<p>Sistema de Risco.</p> <p>Monitoramento de Limite Intradiário.</p> <p>VaR.</p>	<p>Importação diária dos arquivos para sistema.</p> <p>Gerenciamento diário para verificar possíveis estouros de limite.</p>
Gestão	<p>Tomada de decisão para Composição de Carteiras.</p> <p>Manutenção de Estratégias.</p>	<p>Obter relatórios de <i>sell side</i> para a apoio a tomada de decisão.</p> <p>Relatório interno de Risco para limites.</p> <p>Enviar movimentações para Backoffice.</p>

10.2. PROCESSOS X SISTEMAS CRÍTICOS

Área	Processo	Sistema
BACKOFFICE FUNDOS	<p>Cálculo de quotas de Fundos.</p> <p>Zeragem de Caixa — Fundos.</p>	<p>Sistema Gerencial de Cotas.</p> <p>Sistema de Liquidação do Administrador.</p>

	Envio de Movimentações do dia para o Administrador. Aprovação de Operação no sistema do Custodiante.	Portal FIDC.
CONTABILIDADE	Impostos. Contabilização. Contas a Pagar e Receber.	Sistema de <i>Cash Flow</i> .
BACKOFFICE B3	Liquidação Diária com a B3. Coberturas de Margem e Movimentação de Garantia.	Sistema de Liquidação do Administrador. Comunicação com a Corretora.
RISCO	Sistema de Risco. Monitoramento de Limite Intradiário. VaR.	Sistema de Risco.

10.3. PROCESSOS X RECURSOS HUMANOS (MÍNIMO PARA CONTINGÊNCIA).

Área	Processo	Número de colaboradores necessários
BACKOFFICE FUNDOS	Cálculo de quotas de Fundos. Zeragem de Caixa — Fundos. Envio de Movimentações do dia para o	1

	Administrador. Aprovação de Operação no sistema do Custodiante.	
CONTABILIDADE	Impostos. Contabilização. Contas a Pagar e Receber.	1
BACKOFFICE B3	Liquidação Diária com a B3. Coberturas de Margem e Movimentação de Garantia.	1
RISCO	Sistema de Risco. Monitoramento de Limite Intradiário. VaR.	1
GESTÃO	Tomada de decisão para Composição de Carteiras. Manutenção de Estratégias.	1

11. A ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIOS.

A Estratégia de Continuidade de Negócios para as áreas de negócio, aprovada pelo Comitê de Compliance e Risco, se baseia no resultado da análise de impacto dos negócios dos processos críticos dessas áreas e na localização do site. No quadro a seguir, destacam-se os processos críticos que foram identificados com base em cenários.

Foram identificados os processos críticos sob a ótica que mais afetam a receita, ativos, clientes internos e externos da CVPAR (mercados B3 e Fundos de investimentos), conforme quadro a seguir:

Área	Atividade Crítica	Horário Crítico
BACKOFFICE FUNDO	Cálculo de quotas de Fundos Zeragem de Caixa — Fundos Envio de Movimentações do dia para o Administrador	Até 16:00 para FIDC Até 18:00 para 555
CONTABILIDADE	Impostos Contabilização Contas a Pagar e Receber	Até 18:00h
BACKOFFICE B3		Horário de pregão
RISCO	Sistema de Risco Monitoramento de Limite Intradário VaR	Horário de pregão VaR até 19:00h

12. PROCEDIMENTOS DE RETORNO À NORMALIDADE - SITE PRINCIPAL

O banco de dados do servidor de produção está configurado para gerar *backup* das alterações a cada 1 minuto, sendo esses arquivos transmitidos via web para um servidor *cloud* de *standby* por meio de link de 10Mb do site Principal para o Site de Contingência, para sincronismo dos bancos de dados de aplicações críticas da CVPAR. No servidor *cloud* de *standby*, os bancos de dados ficam on-line, recebendo as sincronizações e, em caso de necessidade de acionamento, deve-se acessar o servidor



cloud. Em caso de acionamento do *standby cloud*, este servidor atenderá a produção pelo tempo necessário para a restauração do servidor principal.

Quando o servidor principal for restaurado, é acionada a sincronização com o servidor *cloud*. Os arquivos alterados no *cloud* serão copiados ao servidor principal.

Quanto à telefonia, a transferência de chamadas é revertida para o Site Principal.

13. ADMINISTRAÇÃO DO PCN

A continuidade de negócios de uma empresa, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias, definido neste PCN como o Processo de Continuidade de Negócios.

Anualmente, ou quando houver atualização em processo de negócio crítico, ou em razão do resultado dos testes realizados, ou após algum evento de descontinuidade, o Líder de Contingência deverá atualizar o PCN e validá-lo com a Equipe de Contingência, para que o PCN espelhe a situação de negócio atual da CVPAR.

13.1. DIVULGAÇÃO E TREINAMENTO

Um dos fatores de primordial importância para o funcionamento deste PCN é o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do PCN, conferindo-lhe credibilidade, a CVPAR definiu que serão realizadas sessões de divulgação a todos os colaboradores e envolvidos na continuidade de negócios.

A divulgação será organizada pelo Líder de Contingência, visando manter os colaboradores da Equipe de Contingência atualizados sobre os conceitos de

continuidade, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação dos negócios vigente.

13.2. REALIZAÇÃO DE TESTES

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade anual a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é do Líder de Contingência em conjunto com a Equipe de Contingência.

Os cenários deverão ser definidos e o resultado dos testes registrados em um documento formal que deverá ser aprovado pela alta administração e mantido guardado como documento de validação das estratégias para atendimento dos órgãos reguladores.

Tais testes devem ser realizados **anualmente** com o objetivo de verificar as condições para:

1. Acesso aos sistemas;
2. Acesso ao e-mail corporativo;
3. Acesso aos dados armazenados em procedimento de *backup*; e
4. Outros necessários à continuidade das atividades.

Os testes não provocam quaisquer tipos de indisponibilidade ou parada nos ambientes originais de negócios da CVPAR e são conduzidos pela Equipe de Contingência em total conformidade com o PCN. As simulações são realizadas sobre cenários e ameaças contemplados no PCN, e cobrem os riscos e ameaças com maior probabilidade de ocorrência em ambiente de continuidade de negócios.

13.3. Vigência e Atualização

É responsabilidade do Líder de Contingência manter este PCN, bem como a realização de validação anualmente e alteração quando necessário, sem a necessidade de aviso prévio. As alterações serão divulgadas a todos os Colaboradores pelo Líder de Contingência ou o profissional por ele indicado.

Histórico das atualizações		
Data	Versão	Responsável
Janeiro de 2019	2ª	Diretor de Investimentos e Diretor de Compliance, Risco e PLD
Julho de 2021	3ª	Diretor de Investimentos e Diretor de Compliance, Risco e PLD
Agosto de 2023	4ª e Atual	Diretor de Investimentos e Diretor de Compliance, Risco e PLD

14. GLOSSÁRIO

ALERTA: Notificação do acontecimento de uma situação de desastre — aguarda a possível ativação do PCN.

AMEAÇA: Toda e qualquer condição adversa capaz de vir a causar alguma perda para a empresa. Ameaça é uma condição latente e potencial. Ela não irá causar necessariamente um dano.

ANÁLISE DE IMPACTO NOS NEGÓCIOS: Análise de todas as funções de negócios e o efeito que um desastre específico pode causar na organização.

COMITE DE PCN: Estrutura de organização alternativa que será ocupada durante recuperação de um desastre. Estrutura provisória que irá distribuir ações de forma dinâmica e com autonomia de decisão.

DESASTRE: É o impacto de uma força externa, agressiva, ocasionando perda ou prejuízo significativo. Trata-se de qualquer evento que gere inabilidade em toda ou parte da organização, em suas atividades de negócios, sem predeterminação de

tempo. Um desastre não precisa ser necessariamente, destruidor. Em alguns casos ele é apenas uma condição que impede a operação de uma atividade crítica, necessária para a geração de um serviço ou produto.

EQUIPE DE CONTINGÊNCIA: Grupo de pessoas habilitadas, prontas para realizar o controle das operações de recuperação de uma empresa se um desastre vir a acontecer.

ESTRATEGIA DA CONTINUIDADE DE NEGÓCIOS: Estruturar a forma mais adequada da Gestão da Continuidade de Negócios numa organização, contemplando as necessidades dos processos e as restrições técnicas, organizacionais, culturais e financeiras.

ESTRATÉGIAS DE BACKUP: Alternativa operacional (Plataforma, Localização etc.) para instalações e operações dos sistemas em caso de desastre.

EVENTO: Ocorrência de um fenômeno que impeça a operação de uma ou várias atividades necessárias para geração de serviços ou produtos.

FUNÇÕES CRÍTICAS: Atividades de negócios que não podem ser interrompidas ou ficar indisponíveis, sob o risco de prejudicar significativamente a operação da organização.

GRAU DE EXPOSIÇÃO: É o resultado da análise de impacto nos negócios de cada ameaça, contra as medidas de prevenção efetivas existentes. O objetivo é alcançar o equilíbrio entre risco e prevenção de forma a se obter um baixo grau de exposição a desastres em qualquer situação.

IMPACTO: Efeito negativo, produzido pelo acontecimento de um evento, em processos de negócios.

INTERRUPÇÃO: Parada causada por falha de um ou mais links de comunicações com entidades externas.

INTERRUPÇÃO EMPRESARIAL: Qualquer evento, antecipado (Greve no Serviço Público) ou inesperado (blecaute) que rompe o curso normal de operações empresariais em determinadas localizações da organização.



LIDER DA EQUIPE DE CONTINGÊNCIA: Responsável por administrar as operações necessárias para a condução do PCN em qualquer fase.

PERIODO DE RECUPERAÇÃO DE DESASTRE: É o período entre a ocorrência de um evento e o retorno da empresa para funções normais, durante o qual é acionado o PCN.

PLANO DE TESTE: São os planos e procedimentos de recuperação utilizados em um sistema de testes para assegurar sua viabilidade. Um plano de teste é projetado para exercitar ações de tarefas e procedimentos que poderão ser encontrados em uma situação real.

PROCESSO DE NEGÓCIO: Qualquer atividade executada pelas Unidades de Negócio da empresa, visando atingir a realização da sua atividade-fim.

RISCO: É uma medida numérica ou relativa que qualifica ou quantifica a probabilidade de ocorrência de um desastre. Embora possa ser considerado que um risco deva ser uma medida quantitativa, consideramos que a obtenção deste número nem sempre seja viável ou factível. A utilização de conceitos tais como “pequeno”, “alto” ou “médio” por vezes são mais adequados que a utilização de uma medida numérica com baixa precisão.

SITE ALTERNATIVO: Local, diferente do originalmente utilizado, usado para processar dados e/ou prover o funcionamento de negócios críticos em situações de desastre.

TESTE DE SIMULAÇÃO DO PCN: Teste de procedimentos de recuperação sob condições aproximadas de um cenário de desastre específico. Isto pode ocasionar que unidades designadas da organização cessem de fato operações normais, enquanto no exercício de procedimentos.