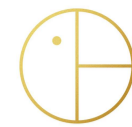
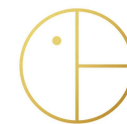


FORPUS
CAPITAL

Plano de Continuidade dos Negócios



VÁLIDO A PARTIR DE	AGOSTO DE 2025
ÁREA RESPONSÁVEL	Compliance
DESTINATÁRIOS	Público em Geral



Sumário

1. Etapas e Procedimentos para a Política de Contingência.....	4
2. Efetiva Contingência.....	5
3. Serviço de Internet.....	5
4. Evento Extraordinário.....	6
5. Testes	6
6. Ativação dos Mecanismos de Resposta.....	7
7. Responsabilidade	9
8. Documentação	9



1. Etapas e Procedimentos para a Política de Contingência

CONTINUIDADE DOS NEGÓCIOS: ESTRUTURA OPERACIONAL

Esta Política tem por objetivo, nos termos do Código ANBIMA de Administração de Recursos de Terceiros, art.16, e da Resolução 35 da Comissão de Valores Mobiliários (“CVM”), estabelecer e compartilhar (i) o Plano de Continuidade dos Negócios que a Forpus Capital Gestão de Recursos Ltda. (“Forpus Capital” ou “Gestora”) se utiliza para identificar e prevenir potenciais riscos que nos obriguem a funcionar em modo de contingência ou possam causar prejuízo na condução das atividades da Forpus Capital; e (ii) as medidas a serem tomadas para identificar e prevenir as possíveis contingências que poderão trazer um impacto negativo considerável sobre a condução das atividades da Gestora.

Visamos descrever os eventos de maior probabilidade de ocorrência dadas as características e o porte da Gestora, como quadro de funcionários, localização geográfica e rotinas diárias. Dentre estas contingências se incluem, por exemplo, crises econômicas, falhas operacionais e/ou desastres naturais.

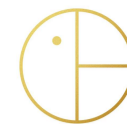
São fatores que integram a política de continuidade dos negócios da Forpus Capital:

(a) manutenção no quadro funcional da Forpus Capital de profissionais experientes no mercado financeiro com dedicação exclusiva à empresa;

(b) a existência de departamento técnico terceirizado, conferindo suporte às atividades de administração de carteiras de títulos e valores mobiliários exercidas pela Forpus Capital;

(c) a existência do *Compliance Officer*, na pessoa do Diretor de *Compliance*, PLDFT e LGPD que, dentre outras funções, concentra a responsabilidade pelo suporte a todas as áreas da Forpus Capital no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Forpus Capital com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

Tais fatores colaboram não só para melhor direcionar a aplicação de recursos pela Forpus Capital, mas também para incrementar o gerenciamento de riscos, conferir melhor fluidez ao fluxo de informações e ao processo decisório da Forpus Capital.



2. Efetiva Contingência

A Forpus Capital trabalha com o backup dos seus computadores, suportado por servidor mantido na nuvem, possibilitando o acesso às últimas 30 (trinta) versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).

Todas as informações do servidor da Forpus Capital, do banco de dados dos clientes e os modelos dos analistas são armazenados em backup em data center remoto.

Todos os executivos da Forpus Capital possuem acesso remoto aos seus *e-mails* e ao servidor de arquivos da empresa, de modo que possam acessá-los de fora do escritório, se necessário.

Os registros contábeis da Forpus Capital ficam sob guarda do contador responsável, que é vinculado à empresa contratada para este específico fim, sendo as informações sobre os fundos de investimento cujas carteiras geridas pela Forpus Capital ficando sob responsabilidade desta instituição administradora.

A equipe de gestão da Forpus Capital tem acesso a softwares que permitem a consulta do mercado financeiro em qualquer lugar do mundo.

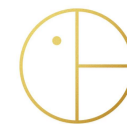
3. Serviço de Internet

A Forpus Capital utiliza 2 (dois) serviços de internet para garantir acesso, independente do evento.

A instituição Forpus Capital possui filtro de e-mail, firewall e sistemas anti-vírus, e demais sistemas oriundos dos sistemas de armazenamento em nuvem inclusive com criptografia.

Em caso de contingência, o Diretor de Compliance acionará a equipe-chave previamente definida, a qual caberá a continuidade dos negócios da Forpus Capital através do acesso às informações necessárias de qualquer equipamento de forma remota.

A Forpus Capital recomenda a utilização de filtros de e-mail, firewall e sistemas antivírus, conforme procedimentos adotados pela Forpus Capital em seus equipamentos corporativos.



4. Evento Extraordinário

Na ocorrência de um evento extraordinário que não esteja previsto neste Plano, a Forpus Capital irá aplicar as disposições deste Plano, bem como seguir as seguintes medidas:

- (a) Identificar e substituir equipamentos danificados;
- (b) Manter suas atividades durante o evento através de acessos remotos pelos Colaboradores;
- (c) Avaliar os prejuízos decorrentes da interrupção das atividades regulares e traçar uma linha de ação corretiva para normalizar o ambiente.

5. Testes

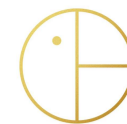
Serão realizados semestralmente, ou anteriormente se entender necessário, sendo testes efetivos de utilização do site de contingência, devendo os respectivos relatórios analíticos ser arquivados na sede da Forpus Capital.

Os testes devem contemplar, obrigatoriamente, pelo menos as seguintes características:

- a) A inacessibilidade física ao escritório, onde todos os Colaboradores trabalham remotamente;
- b) Acesso aos sistemas;
- c) Acesso ao e-mail corporativo contratado;
- d) Acesso aos dados armazenados em estrutura na nuvem; e
- e) Outros acessos necessários ao funcionamento pleno das atividades essenciais.

Os Colaboradores devem informar imediatamente sobre possíveis falhas de acesso aos sistemas, dados e arquivos na nuvem que impeçam a plena execução de suas atividades.

O resultado do teste é registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento do presente Plano de Continuidade de Negócios.



6. Ativação dos Mecanismos de Resposta

Os Colaboradores são responsáveis por comunicar ao Diretor de Compliance sobre toda e qualquer situação que possa, ainda que potencialmente, dar origem a uma situação que possa levar a ativação dos procedimentos de contingência indicados neste Plano.

A ativação do Plano de Contingência ficará a critério e será de responsabilidade do Responsável por Compliance.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

De forma a se prevenir da maneira mais adequada, a Forpus Capital adotará os seguintes mecanismos de resposta para cada contingência específica:

I. Indisponibilidade da Sede:

Caso a indisponibilidade seja superior a 04 (quatro) horas durante o normal expediente de trabalho, será contratada empresa especializada para se deslocar ao local da contingência de forma a solucionar o evento ou encontrar medida alternativa, ainda que temporária.

Os demais Colaboradores serão imediatamente notificados para que fiquem à disposição desempenhando suas funções em home office;

II. Indisponibilidade dos Servidores:

Caso a indisponibilidade seja superior a 04 (quatro) horas durante o expediente de trabalho, deverá ser contratada empresa especializada para se deslocar ao local da contingência, caso a empresa de Tecnologia da Informação contratada pela Forpus Capital não consiga solucionar a questão, ou encontrar solução temporária dentro de um prazo de 04 (quatro) horas. Os demais Colaboradores deverão permanecer na sede da Forpus Capital e desempenhar suas funções;

III. Indisponibilidade de Conexão por Internet com o Exterior

A respectiva indisponibilidade poderá ser dividida em 02 (duas) modalidades:



(i) caso a indisponibilidade seja inferior a 04 (quatro) horas, deverá ser avaliada a necessidade de substituição temporária dos fornecedores de acesso à internet, assim como deverá ocorrer o contato com os fornecedores de internet originários de modo que seja restaurada a respectiva conexão;

(ii) caso a indisponibilidade seja superior a 04 (quatro) horas, ou não haja previsão para restauração da conexão, deverá ser realizada a substituição dos fornecedores de acesso à internet e ser contratada empresa especializada a ser deslocada para local de modo a restaurar a indisponibilidade ou encontrar solução alternativa, ainda que temporária, caso a empresa contratada de Tecnologia da Informação da Forpus Capital não consiga solucionar. Os demais Colaboradores deverão permanecer na sede da Forpus Capital e desempenhar suas funções;

IV. Indisponibilidade de Informações sobre os Ativos Financeiros

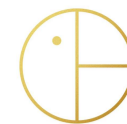
A respectiva indisponibilidade poderá ser dividida em 02 (duas) modalidades:

(i) caso a indisponibilidade seja inferior a 04 (quatro) horas, deverá ser avaliada a necessidade de substituição temporária dos fornecedores de informações, assim como deverá ocorrer o contato com os fornecedores de internet originários de modo que seja restaurada a respectiva conexão; e

(ii) caso a indisponibilidade seja superior a 04 (quatro) horas, ou não haja previsão para restauração da conexão, deverá ser realizada a substituição dos fornecedores de informações e ser contratada empresa especializada a ser deslocada para local de modo a restaurar a indisponibilidade ou encontrar solução alternativa, ainda que temporária, caso a empresa terceirizada TI da Forpus Capital não consiga solucionar. Os demais Colaboradores deverão permanecer na sede da Forpus Capital e desempenhar suas funções;

V. Redução no Quadro de Colaboradores

A Forpus Capital avaliará a possibilidade de locomoção até o local de sua sede e determinarão quais serão as funções a serem desempenhadas pelos Colaboradores disponíveis até que se encontre solução



alternativa, mesmo que temporariamente. Os Colaboradores que não conseguirem se locomover à sede da Forpus Capital deverão ficar à disposição e desempenhar suas funções em home office; e

VI. Tempos de Resposta dos Colaboradores

É de responsabilidade de cada Colaborador manter seus meios de contato atualizados e de conhecimento da Forpus Capital. Da mesma maneira, é de responsabilidade de cada Colaborador estar acessível e comunicar suas respectivas localizações tão logo tenham conhecimento da ocorrência de um evento que possa colocar em risco a continuidade de sua função, mesmo que momentaneamente, ou, dos negócios da Forpus Capital. Deverão, também, reportar a localização de outros Colaboradores caso tenham certeza da localização destes.

7. Responsabilidade

O Diretor da Forpus Capital responsável pela prevenção de perdas e implementação do presente Plano de Contingências e Continuidade dos Negócios é o Sr. Luiz Alberto Nunes Jr.

8. Documentação

É mantida no site de contingência uma lista por acesso remoto com as informações de todos os integrantes da Forpus Capital, das corretoras com as quais se realizam negócios, do histórico da conta de investimento dos clientes e dos prestadores de serviço contratados.