POLÍTICA DE CONTINUIDADE DE NEGÓCIOS
BLP DIGITAL GESTORA DE RECURSOS LTDA.

FEVEREIRO DE 2022

SUMÁRIO

1. OBJETIVO....3
2. RISCOS POTENCIAIS....4
3. REDUNDÂNCIA DA INFRAESTRUTURA....5
3.1. *Home Office* e Escritório de Contingência....5
3.2. Treinamento Interno e Testes de Eficiência....6

1. OBJETIVO

O objetivo desta *"Política de Continuidade de Negócios*" ("Política") da BLP Digital Gestora de Recursos Ltda. ("BLP Digital" ou "Gestora") é garantir a manutenção das suas operações, provendo recursos alternativos e estratégias de continuidade em casos de ocorrências inesperadas.

Esta Política foi elaborada em conformidade com a Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21"), e o *"Código de Administração de Recursos de Terceiros* ("Código ART") da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA"), e é aplicada a todos os funcionários, estagiários, sócios, administradores e prestadores de serviços terceirizados da Gestora (quando em conjunto, "Colaboradores").

Esta Política deve ser lido em conjunto com as demais políticas, códigos e manuais da BLP Digital, os principais normativos emitidos pela CVM, os Códigos ANBIMA e demais legislações aplicáveis.

A presente Política define os riscos potenciais a que a Gestora está exposta, detalha os procedimentos para ativação da Política e estabelece alternativas e procedimentos operacionais que deverão ser seguidos em caso de incidentes.

Todos os Colaboradores devem ler esta Política e entender o seu papel diante de uma situação de contingência.

Foram estipuladas estratégias para identificação dos incidentes não usuais e planos de ação com o intuito de garantir que os serviços essenciais da BLP Digital sejam devidamente preservados após a ocorrência de situações inesperadas.

O departamento de *compliance* responsabiliza-se por assegurar a aplicabilidade e o cumprimento desta Política ("Departamento de *Compliance*"), cuja efetividade e eficácia será supervisionada pelo Diretor de *Compliance.*

Ressaltamos que o suporte de tecnologia da informação da Gestora é terceirizado, realizado por empresa prestadora de serviços de tecnologia da informação, de modo que não temos nenhum colaborador interno do setor ("Auxiliares de TI").

2. RISCOS POTENCIAIS

Riscos Potenciais			
1	Falta de energia	5	Incêndio
2	Falha de hardware, software e telecom	6	Inundação
3	Vírus / hackers	7	Furto / sabotagem
4	Greve	8	Ausência de colaborador

A lista de eventos do quadro “Riscos Potenciais” não pretende ser exaustiva e serve apenas como um guia para as situações em que a Gestora estará exposta durante o exercício de suas atividades.

Uma vez identificado um ou mais incidentes acima, o Colaborador deverá comunicar, imediatamente, ao diretor da área afetada, ou aos Auxiliares de TI, conforme aplicável, os quais serão responsáveis por analisar a situação, e decidir, juntamente com os demais diretores da instituição, pela tomada das providências cabíveis.

3. REDUNDÂNCIA DA INFRAESTRUTURA

Energia elétrica: No caso de falha no fornecimento de energia, os *nobreaks* instalados nos *desktops*, serão capazes de suportar, pontualmente, o seu funcionamento. Nos casos de interrupção prolongada de energia, o gerador do condomínio é acionado em até 05 (cinco) minutos e é capaz de suprir, de forma excepcional, o fornecimento de energia do prédio e também do escritório da BLP Digital até que o serviço seja restabelecido normalmente.

Arquivos: A BLP Digital disponibiliza em seus servidores o serviço de *backup* e *restore* dos arquivos, o objetivo é garantir a disponibilidade, integridade e confiabilidade dos dados armazenados. Os *backups* são feitos em *cloud* após cada salvamento da versão do arquivo.

***E-mail*:** O serviço de *e-mail* da BLP Digital é garantido por parceiro *Microsoft* que provê suporte 24/7 (vinte e quatro horas por dia, sete dias da semana), possui serviços de *AntiSpam*, antivírus, recuperação de informação, acesso via *webmail* e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A BLP Digital possibilita o acesso remoto de todas as mensagens pelos colaboradores.

Telefonia: O serviço de telefonia contratado pela BLP Digital prevê o encaminhamento das ligações telefônicas do escritório, para outros números indicados e aprovados por "Usuário Master" da BLP Digital, inclusive para os telefones celulares dos colaboradores, em casos de impossibilidade de receber as chamadas no escritório da Gestora.

***Internet*:** Os *links* de *internet* são contratados de diferentes provedores para dar maior segurança na disponibilidade do serviço e garantir a redundância da rede. A disponibilidade do *link* principal é monitorada constantemente, com envio de alertas em caso de falha no sinal.

Provedores de serviços de informação: Os serviços utilizados pela equipe de gestão, tais como *Bloomberg*, Valor Pró e Broadcast, podem ser acessados via mobile ou *notebooks* previamente configurados, sendo que esses serviços possuem seu próprio plano de contingência para manutenção, funcionamento e disponibilidade.

Colaboradores: As atividades prestadas pelos colaboradores no escritório da BLP Digital são compartilhadas, ou seja, mais de um colaborador executa a mesma função. O objetivo desse rodízio de atividades visa evitar que a ausência de um colaborador possa impedir as rotinas da Gestora.

3.1. *Home Office* e Escritório de Contingência

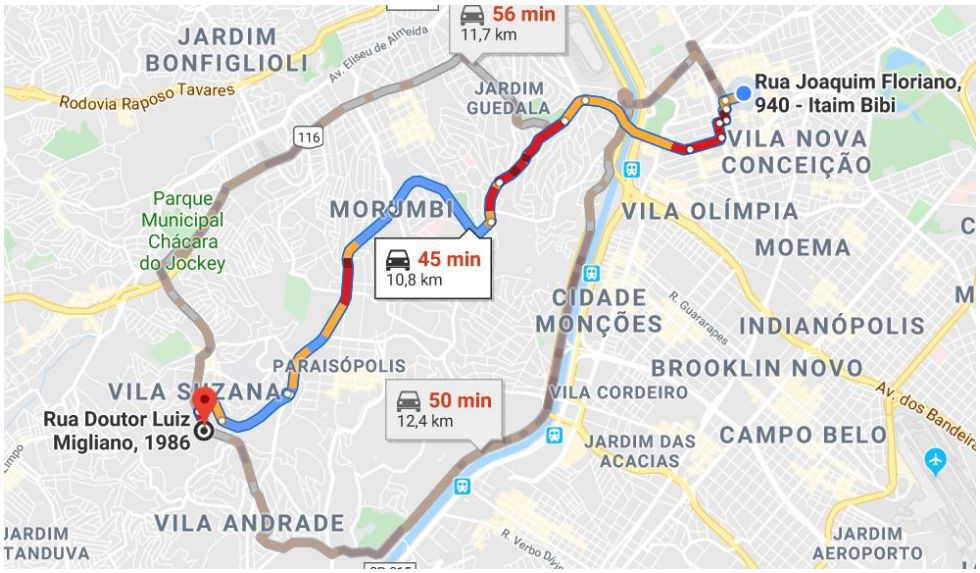
Em caso de impossibilidade de acesso às dependências do escritório da Gestora, os colaboradores poderão contar com as seguintes opções de trabalho:

a) *Home Office*: trabalhar de casa; e

b) Escritório de Contingência**:** este ambiente é mantido pelos Auxiliares de TI.

O escritório de contingência fica a cerca de 8 km (oito quilômetros) do escritório da BLP Digital, na Cidade de São Paulo, Estado de São Paulo, na Rua Doutor Luiz Migliano nº 1986, e o tempo estimado para se chegar ao endereço é de aproximadamente 40 (quarenta) minutos.

Mapa do trajeto do escritório contingência



A BLP Digital possui 03 (três) *desktops* dedicados no escritório de contingência, os quais possuem *software* padrão e aplicativos essenciais para operação dos seus sistemas.

Os aplicativos essenciais da BLP Digital estão listados abaixo bem como a disponibilidade de acesso no *site* de contingência:

Aplicativo	Home-Office	Escritório de Contingência
E-mail	✓	✓
Sophos Antivirus	✓	✓
Base de Dados	✓	✓
Bloomberg ***Broadcast*** **Valor-Pró**	✓	✓

3.2. Treinamento Interno e Testes de Eficiência

Durante o treinamento interno do Departamento de *Compliance* para novos Colaboradores, esta Política também fará parte dos temas apresentados.

Posteriormente, durante os testes de eficiência, os Colaboradores serão convidados a participar das simulações e deverão atestar que a estrutura estabelecida pela Política é capaz de suportar, de modo satisfatório, a prestação de serviços da Gestora.

Os testes de eficiência têm como objetivo avaliar os processos operacionais críticos para a manutenção dos negócios da instituição e manter a integridade, a segurança e a consistência do banco de dados da Gestora.

Esta Política será validado a cada 12 (doze) meses, ou em prazo inferior, quando exigido pela regulamentação aplicável.

Os seguintes cenários e eventos serão avaliados durante os testes de eficiência:

a) O conhecimento desta Política pelos Colaboradores;

b) Tempo para sua ativação;

c) Acesso, disponibilidade e integridade da base de dados;

d) Acesso à *softwares* e sistemas (quando aplicável); e

e) Comunicação entre os parceiros estratégicos.