



Política de Desastre e Contingência

Atualizado em: Setembro, 2022

Índice

Introdução	3
Procedimentos de <i>Backup</i>	4
Desastre e Contingência	4
Testes	5

Introdução

Esta Política de Desastre e Contingência (“Política”) tem como objetivo definir os procedimentos que todos os sócios, diretores, empregados, funcionários e estagiários (“Colaboradores” e, no singular, “Colaborador”) da **GL Asset Gestão de Ativos Ltda.** (“GL Asset”) deverão seguir, no caso de contingência, impedindo, assim, a descontinuidade operacional dos serviços por problemas técnicos.

Para apresentar os principais aspectos e conceitos que envolvem o tema, bem como facilitar e nivelar o entendimento de todos, elaboramos esta Política. Sugerimos que leia o material por inteiro e que as orientações aqui repassadas façam parte do seu cotidiano.

Atenciosamente,

Diretor de *Compliance*

GL Asset Gestão de Ativos Ltda.

Procedimentos de Backup

A GL Asset é uma gestora de recursos de terceiros, credenciada perante a Comissão de Valores Mobiliários (“CVM”), e, por essa razão, conta com uma estrutura operacional desenvolvida e preparada para eventuais emergências.

Todas as informações e documentos da GL Asset (tais como arquivos, bancos de dados e cadastros e banco de e-mails) possuem cópia de segurança, feita através de um *backup* completo com salvamento automático, armazenado em servidores da [Microsoft Corporation], e que fica disponível por até 2 (dois) anos.

Desastre e Contingência

Em caso de qualquer evento de contingência ou desastre, o Diretor de *Compliance* informará os Colaboradores de imediato e indicará as medidas a serem tomadas, de forma a mitigar ou reduzir impactos indesejáveis diretos à operação e aos negócios da GL Asset.

A continuidade de negócios está diretamente ligada aos seguintes pilares:

- **Cultura e conscientização:** O pleno conhecimento dos termos e condições desta Política e dos demais manuais de *compliance* da GL Asset facilita a implementação do plano de continuidade de negócios como um todo.
- **Ações Preventivas:** Visam mitigar os riscos para que não haja incidentes.
- **Plano de Contingência:** Conjunto de medidas e providências a serem tomadas, em função de um determinado incidente passível de impactar na continuidade das operações e dos negócios da GL Asset. Exemplos: incêndio, alagamento, pane geral nos recursos de TI e telecomunicações, etc.

O Plano de Contingência da GL Asset é dividido em duas frentes de atuação:

- **Impacto Global:** Ocorre quando a GL Asset estiver impossibilitada por qualquer motivo de continuar suas operações. Nesse caso, entra em ação o plano de contingência, o ambiente de desastre e o plano de recuperação do site afetado.
- **Impacto Específico:** Ocorre quando forem afetadas uma ou mais áreas e/ou processos, mas a GL Asset conseguir operar de forma parcial ou através de redundância.

A disponibilidade de praticamente todos os sistemas de informação da GL Asset em nuvem, tais como servidores de e-mail, servidores de arquivos, sistemas de risco e contabilidade e aplicativos como Bloomberg Anywhere, permite que os Colaboradores da GL Asset usufruam de ampla independência e facilidade de acesso a esses recursos, sem abrir mão da segurança, onde quer que estejam. Com a redundância inerente a soluções em nuvem, no caso de Contingências de Impacto Global ou Impacto Específico, os recursos tecnológicos necessários para a continuidade

da operação encontram-se disponíveis prontamente, de forma transparente, segura e ininterrupta aos Colaboradores da empresa.

Ainda no caso de Contingências de Impacto Global, as ordens do Diretor de Gestão de Carteiras serão dadas, preferencialmente, através de *chats* mantidos com as principais contrapartes através do Bloomberg Anywhere, cujo acesso se dá através de controle biométrico, ou alternativamente por telefone.

Testes

Semestralmente, testes são conduzidos preventivamente para avaliar os serviços e recursos que fazem parte da infraestrutura da GL Asset, possibilitando a identificação e resolução antecipada de problemas que possam comprometer a confiabilidade das soluções implementadas, garantindo assim uma operação segura e sem falhas.