POLÍTICA DE CONTINGÊNCIA

São Paulo, 5º de março de 2026

SUMÁRIO

POLÍTICA DE CONTINGÊNCIA

1 Objetivo

A Política de Contingência tem como objetivo definir o Plano de Contingência e Recuperação de Desastres ("Plano de Contingência") a ser seguido pela DOMO, de modo a impedir a descontinuidade operacional da Gestora, considerando o acontecimento dos Eventos/Ameaças Previstos no item 2 abaixo, determinando os procedimentos que deverão ser seguidos visando proteger os interesses dos Investidores e a continuidade das atividades.

2 Eventos/Ameaças Previstos

O Plano de Contingência da DOMO traz como principais eventos/ameaças aos negócios da Gestora, incluindo, mas não se limitando a:

- Baixa conectividade ou perda de conectividade com a internet;
- Invasão sistêmica que prejudique dados internos;
- Falha nas linhas telefônicas;
- Inacessibilidade temporária do escritório;
- Inacessibilidade permanente do escritório;
- Inacessibilidade dos Diretores responsáveis por tomada de decisão por mais de 24 (vinte e quatro) horas; e
- Qualquer outra situação que ameace, física, estrutural ou virtualmente, o ambiente da Gestora, mesmo que não descrita acima.

3 Classificação dos Eventos/Incidentes

Os eventos de contingência poderão ser classificados conforme sua severidade e impacto potencial (baixo, médio, alto ou crítico), considerando indisponibilidade de sistemas, impacto aos Fundos, exposição regulatória e risco reputacional, cabendo às Pessoas Chave priorizar as ações de resposta e comunicação conforme o nível identificado.

4 Procedimento Interno (Pessoas-Chave)

Em caso de efetiva necessidade de implantação do Plano de Contingência, deverão ser encaminhadas para o Local Alternativo as "Pessoas Chave", previamente identificadas desta forma pela área de Compliance.

As Pessoas Chave avaliarão o evento ou ameaça e determinarão os deveres e responsabilidades dos demais Colaboradores.

Dentre as Pessoas Chave deverão estar responsáveis pelas funções prioritárias :

- *Trigger* do Uso do Local Alternativo: Diretor de Gestão
- Contato com Colaboradores: Diretor de Compliance
- Contato com Investidores e Contra-partes: Diretor de Compliance / Diretor de Risco / Diretor de PLDFT / Diretor de Gestão
- Confiabilidade dos Dados Armazenados / Recuperados: Diretor de Risco

5 Local de Trabalho Alternativo

Nos casos de inacessibilidade temporária ou permanente, o Plano de Contingência contempla a utilização de local de trabalho alternativo, podendo autorizar os Colaboradores da DOMO a trabalharem de suas casas ou a dirigirem-se a um local específico que será definido pela área de Compliance.

Em caso de emergência, a DOMO conta com instalação de "Sala de Emergencia" no Rio de Janeiro, em empresa especializada, que pode ser utilizada como escritório alternativo de trabalho no caso de indisponibilidade da sede em São Paulo. O site alternativo do Rio de Janeiro está disponível para recepcionar até 07 (sete) Colaboradores considerados Pessoas Chave.

Ambos os escritórios contam com computadores com acesso à internet, sendo possível acessar toda a base de dados e sistemas, salvos "na nuvem", por meio do serviço contratado com a Google (Google Drive; Vault), bem como telefones fixos e notebooks para utilização dos Colaboradores. O escritório da DOMO conta com redundância de acesso a internet (banda larga). O endereço residencial dos 03 (três) Sócios- Diretores também está preparado para receber até 04 (quatro) Pessoas Chave, caso necessário.

6 Proteção e Recuperação de Dados e Documentos

Os dados eletrônicos da DOMO são mantidos "na nuvem", em servidores Google, sendo realizados *backups* diários das informações da Gestora.

Além do procedimento de *backup* diário, uma cópia física dos arquivos é feita por cada um dos 03 (três) Sócios, e, alternativamente, o uso de backup adicional (Dropbox) também está contratado.

A área de Compliance supervisionará o acesso às informações contidas nos *backups* e somente se utilizará dessas informações para fins internos ou nos termos previstos na lei.

Incluem-se no Plano de Contingência os incidentes de tecnologia da informação e cibersegurança, tais como ataques cibernéticos, vazamento de dados, indisponibilidade de sistemas, falhas de backup, acessos indevidos e corrupção de bases de dados. Tais eventos deverão ser comunicados imediatamente às áreas de Risco e Compliance para avaliação, mitigação e, quando aplicável, comunicação às autoridades e partes afetadas, observada a legislação aplicável, inclusive a Lei nº 13.709/2018 (LGPD).

7 Comunicação Pública

Caso ocorra um evento ou ameaça cujo resultado seja a inacessibilidade temporária ou permanente do escritório, a área de Compliance é responsável por elaborar comunicado formal aos Investidores, terceiros contratados e ao mercado em geral.

Na impossibilidade de atuação da área de Compliance, somente a Diretoria Executiva está autorizada a realizar esta função, sendo absolutamente vedado aos demais Colaboradores a comunicação pública sobre o ocorrido.

Quando aplicável, a área de Compliance avaliará a necessidade de comunicação à CVM, ANBIMA e demais partes regulatórias relevantes acerca do evento de contingência, nos termos da regulamentação vigente.

8 Avaliação e Testes Periódicos

O Plano de Contingência deverá ser avaliado e testado periodicamente, à critério da área de Compliance, em virtude das mudanças naturais ocorridas na Gestora, tais como entrada e saída de

Colaboradores, troca de sistemas, mudança de estratégia de proteção e etc. Fica estabelecido que a execução deste teste é de responsabilidade da área de Compliance.