

## **Plano de Contingência, Continuidade de Negócios e Recuperação de Desastres**

\*parte integrante do Manual de Compliance da SWM

A SWM adota um plano de contingência, continuidade de negócios e recuperação de desastres com o objetivo de garantir a continuidade das atividades em tempo hábil para cumprimento de suas responsabilidades e evitar a perda definitiva de dados, documentos e informações.

O plano contempla diversas medidas a serem tomadas visando a proteção, recuperação e acesso a processos e informações relevantes em casos de contingência.

O acesso a sistemas e documentos digitais, em casos de contingência, pode ser feito remotamente pelos administradores e funcionários autorizados, estes últimos com acesso restrito apenas ao conteúdo necessário à execução das suas atividades.

O acesso remoto é configurado, monitorado e protegido pela área de Tecnologia, sob orientação e supervisão do diretor estatutário responsável pelos recursos tecnológicos da SWM, através de ferramentas seguras e apropriadas para esse fim.

A área de Tecnologia da SWM realiza periodicamente cópia de segurança de todas as informações, documentos, arquivos e registros eletrônicos da empresa, sendo os dados digitais mantidos em nuvem (*cloud*) ou em mídias de armazenamento (*hard disk* ou meios equivalentes) mantidas em local físico distinto da sede.

Caso ocorra algum evento (desastre) que possa ocasionar a perda ou impossibilidade de acesso aos dados, sistemas, documentos e informações, a área de Tecnologia restaurará os *backups* em equipamentos localizados em local seguro a ser indicado pelo Diretor estatutário responsável pelos recursos tecnológicos ou, na sua ausência, pelo Diretor de Gestão de Recursos.

Caberá ao Diretor estatutário responsável pelos recursos tecnológicos avaliar os incidentes e decidir sobre as ações a serem tomadas, bem como



decidir sobre investimentos relacionados à segurança da informação com o objetivo de reduzir riscos.

As medidas de continuidade de negócios e de recuperação de desastres aqui previstas serão objeto de teste e validação, no mínimo, a cada 12 (doze) meses, ou em prazo inferior mediante decisão do Diretor estatutário responsável pelos recursos tecnológicos, visando avaliar se são capazes de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da SWM e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se tais medidas podem ser ativadas tempestivamente.

Os procedimentos de segurança aplicados são revistos e atualizados sempre que necessário, tendo sido revisados pelo Diretor de Compliance e Prevenção à Lavagem de Dinheiro e aprovados pelo Conselho Consultivo da SWM em 09/10/2025.