PLANO DE CONTINGÊNCIA, CONTINUIDADE DOS NEGÓCIOS E

RECUPERAÇÃO DE DESASTRES

M7 IB SOLUÇÕES FINANCEIRAS LTDA.

CNPJ 60.391.854/0001-78

1. OBJETIVO

O presente "*Plano de Contingência, Continuidade dos Negócios e Recuperação de Desastres*" ("Plano") tem por finalidade estabelecer diretrizes e procedimentos que assegurem a resiliência organizacional e a manutenção das atividades críticas da **M7 IB SOLUÇÕES FINANCEIRAS LTDA.**, inscrita no CNPJ sob o nº 60.391.854/0001-78 ("M7 IB"), em situações adversas que comprometam a normalidade operacional.

Este Plano foi estruturado com base nas melhores práticas de mercado, normativos da Comissão de Valores Mobiliários ("CVM"), autorregulação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") e demais regulamentações aplicáveis ao setor de oferta de valores mobiliários. Seu propósito central é garantir a mitigação de riscos operacionais, tecnológicos e estratégicos, por meio de:

i. preservação da continuidade dos processos essenciais à atividade-fim da M7 IB;

ii. asseguramento da integridade, confidencialidade e disponibilidade de informações e dados sensíveis;

iii. redução de impactos financeiros, legais, reputacionais e regulatórios em caso de incidentes críticos;

iv. restauração célere das condições normais de funcionamento após interrupções parciais ou totais das operações;

v. capacitação permanente dos colaboradores para resposta eficaz a incidentes, promovendo cultura de resiliência organizacional; e

vi. cumprimento de exigências regulatórias da CVM, ANBIMA e demais órgãos competentes.

O Plano é de caráter dinâmico, sujeito a revisões e melhorias contínuas, e sua eficácia depende do comprometimento de todas as áreas da organização.

Todos os colaboradores recebem orientação sobre os procedimentos e são capacitados, pelo Departamento de Compliance, para atuação em situações de contingências.

2. APLICABILIDADE

Este Plano aplica-se a todos os processos, sistemas, recursos e pessoas diretamente envolvidos na cadeia operacional da M7 IB. Seu escopo abrange não apenas os departamentos centrais da empresa, como também os prestadores de serviços terceirizados críticos para a operação.

São considerados abrangidos por este Plano:

i. processos operacionais de mercado de capitais: incluindo emissão, estruturação e distribuição de valores mobiliários;

ii. relacionamento com clientes e parceiros: canais de atendimento, plataformas digitais, envio de extratos e informações obrigatórias;

iii. infraestrutura de tecnologia da informação: servidores, sistemas de *Customer Relationship Management*, bases de dados, redes, serviços de nuvem e recursos de comunicação corporativa;

iv. atividades de *backoffice* e administrativas: como controle financeiro, compliance, jurídico, contabilidade e recursos humanos.

A aderência a este Plano é obrigatória para todos os colaboradores da M7 IB, e eventuais exceções devem ser formalmente autorizadas pelo Diretor de Compliance.

3. SITUAÇÕES DE ATIVAÇÃO

O Plano será acionado quando a operação normal da M7 IB for comprometida por eventos que impossibilitem parcial ou totalmente o funcionamento das atividades críticas.

As situações que justificam a ativação do Plano incluem, mas não se limitam a ("Situações de Ativação"):

i. desastres naturais e acidentes físicos: como incêndios, inundações, desabamentos, quedas de energia elétrica de longa duração e outras ocorrências que impactem a sede física da empresa ou de fornecedores essenciais;

ii. falhas tecnológicas graves: indisponibilidade de sistemas essenciais, pane generalizada de software, corrupção ou perda de dados críticos;

iii. ataques cibernéticos: invasões, *ransomware*, vazamento de dados, negação de serviço (DDoS) ou qualquer evento de segurança da informação que comprometa a integridade ou disponibilidade de sistemas;

iv. interrupções de serviços essenciais: queda prolongada de *internet*, indisponibilidade de serviços de nuvem, falhas em data centers ou operadoras de telecomunicações;

v. eventos pandêmicos ou de saúde pública: que impeçam o deslocamento de colaboradores ou exijam operação remota compulsória;

vi. falta de pessoal chave: por greve, absenteísmo em massa, eventos de força maior, entre outros.

A avaliação e a decisão de ativação cabem ao Diretor de Compliance, em conjunto com os responsáveis das áreas afetadas.

4. ESTRATÉGIAS E SOLUÇÕES ADOTADAS

Diante da ocorrência de qualquer uma das Situações de Ativação, a M7 IB adotará, de forma coordenada e escalonada, as seguintes medidas:

i. Gerenciamento inicial do incidente:

   a. identificação e classificação do evento conforme sua gravidade e impacto; e

   b. ativação do Comitê de Compliance e definição das prioridades operacionais imediatas;

ii. Garantia da segurança física e das pessoas:

   a. evacuação da sede, conforme protocolo de segurança do prédio, com uso exclusivo das escadas de emergência; e

   b. acionamento de serviços públicos (bombeiros, polícia, concessionárias, Defesa Civil), se necessário.

iii. Continuidade operacional remota:

   a. ativação das estações de trabalho em regime remoto, com acesso seguro aos sistemas críticos por meio de VPN, autenticação multifator (MFA) e sistemas em nuvem redundante; e

   b. comunicação estruturada com todos os colaboradores e departamentos sobre as diretrizes temporárias de trabalho.

iv. Restauração de infraestrutura e sistemas:

   a. recuperação dos ambientes afetados com base em backups em nuvem;

b. substituição de equipamentos danificados por unidades reserva ou locação emergencial; e

c. testes de integridade de dados e validação de sistemas antes do retorno à operação integral.

v. Comunicação institucional:

a. envio de comunicados a clientes, parceiros, prestadores de serviço e órgãos reguladores, conforme a criticidade do evento; e

b. disponibilização de canal exclusivo para atualizações e suporte durante a contingência.

vi. Retomada das atividades presenciais (quando aplicável):

a. liberação da área afetada somente após inspeção de segurança e laudo técnico; e

b. monitoramento contínuo dos riscos até o restabelecimento completo da normalidade.

5. *BACKUP* E SEGURANÇA DA INFORMAÇÃO

A política de *backup* e segurança da informação da M7 IB é baseada nos princípios de disponibilidade, integridade, confidencialidade e resiliência cibernética.

i. Procedimentos de backup:

a. realização de backups automáticos e diários de todos os dados sensíveis, bases de clientes, registros operacionais e documentos críticos;

b. armazenamento redundante em ambiente de nuvem certificado, com replicação geográfica em diferentes localidades;

c. retenção dos dados por período mínimo definido pela política de governança de dados, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018.

ii. Segurança da informação:

a. criptografia de dados em repouso e em trânsito;

b. gestão de acessos com base em credenciais individuais e políticas de menor privilégio;

c. auditorias internas regulares para verificação da eficácia dos mecanismos de controle e da política de *backup*.

iii. Recuperação de dados:

a. testes semestrais de restauração de backups críticos para validação da integridade dos dados armazenados;

b. *logs* de restauração mantidos pelo departamento de tecnologia da informação e revisados periodicamente pelo Departamento de Compliance.

6. TESTES E SIMULAÇÕES

A M7 IB realiza, de forma estruturada e regular, testes de recuperação e simulações de incidentes como parte essencial de sua estratégia de melhoria contínua.

i. Tipos de testes realizados:

a. simulações de falha sistêmica: interrupções controladas de sistemas críticos para avaliar o tempo de resposta e a efetividade dos planos de contingência;

b. testes de recuperação de backup: restauração parcial ou completa de bases de dados críticas, com validação técnica e funcional;

c. testes de comunicação em crise: acionamento do comitê de crise e verificação da fluidez na troca de informações entre as áreas;

d. simulações de trabalho remoto: verificação da capacidade de operação 100% (cem por cento) remota de todas as áreas, incluindo acesso seguro, estabilidade da VPN e comunicação por canais alternativos.

ii. Frequência e avaliação

a. os testes são realizados pelo menos duas vezes ao ano, com abrangência total ou setorial;

b. cada simulação gera um relatório formal, contendo os resultados, gaps identificados, lições aprendidas e plano de ação corretiva.

iii. Treinamento contínuo

a. os colaboradores recebem treinamento anual obrigatório sobre as diretrizes do Plano e os procedimentos de resposta a incidentes

b. novos colaboradores são treinados como parte do processo de integração institucional.

7. DISPOSIÇÕES FINAIS

Este Plano foi elaborado em conformidade com os princípios da gestão de riscos operacionais e de continuidade de negócios aplicáveis ao setor financeiro, observando-se as exigências regulatórias da CVM, da ANBIMA e de demais órgãos reguladores pertinentes.

O conteúdo aqui disposto deverá ser observado por todos os colaboradores, parceiros estratégicos e prestadores de serviços críticos da M7 IB, os quais serão devidamente comunicados e treinados conforme suas atribuições específicas. O descumprimento injustificado das diretrizes previstas neste Plano poderá resultar em medidas corretivas, nos termos da política interna de governança corporativa.

Este documento entra em vigor a partir de maio de 2025, estando sujeito a revisões periódicas para refletir mudanças no ambiente regulatório, tecnológico, organizacional ou em decorrência de lições aprendidas em testes e situações reais de contingência.

As revisões ordinárias deverão ocorrer, no mínimo, anualmente, conduzidas pelo Departamento de Compliance em conjunto com os gestores das áreas envolvidas. Revisões extraordinárias poderão ser realizadas sempre que forem identificadas falhas, mudanças críticas de infraestrutura, aquisições relevantes, ou após a ocorrência de incidentes que comprometam a eficácia das diretrizes aqui estabelecidas.

Dúvidas, sugestões ou comunicações urgentes relativas ao Plano devem ser direcionadas ao responsável institucional:

Ricardo Abrahão Fajnzylber
Diretor de Compliance
Telefone: +55 (11) 95077-4500
E-mail: ricardo.fajnzylber@multisete.com