RADAR

Plano de Contingência e Continuidade dos Negócios

Junho de 2022

I. Introdução

O Plano de Continuidade de Negócios ("Plano de Contingência") visa definir os procedimentos emergenciais a serem seguidos pela equipe ("Colaboradores") da Radar Gestora de Recursos Ltda. ("Radar" ou "Gestora"), para evitar o risco de descontinuidade operacional, em situações de falta de acesso ao escritório sede ou aos recursos indispensáveis ao seu funcionamento normal. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da RADAR sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

Essas situações são classificadas de forma geral como contingências e implicam na modificação da rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, à Radar.

II. Disposições Gerais

Os incidentes mais comuns que podem resultar em descontinuidade operacional são incêndios, enchentes, interrupção de serviços públicos, roubos, assaltos, tumultos, greves, ataques de hackers, vírus de computador, sabotagem, acidentes e erros humanos.

O Plano de Contingência não tem como objetivo impedir a ocorrência dos incidentes acima, mas sim assegurar o funcionamento normal das atividades da Radar apesar da sua eventual ocorrência, bem como reduzir os danos ou prejuízos que deles possam resultar.

O Plano de Contingência tem como objetivo subsidiário identificar as responsabilidades das empresas e dos indivíduos que desenvolvem ações específicas para mitigar riscos e coordenar os procedimentos emergenciais, bem como a estrutura voltada à prevenção dos riscos.

Para atendimento às necessidades mínimas de manutenção dos serviços/atividades da Radar, foi definida uma estrutura mínima física, tecnológica e de pessoal, e procedimentos que devem ser adotados toda vez em que uma situação seja caracterizada como uma contingência às operações da Radar.

Foram identificados os seguintes focos de preocupação relativos às atividades da Radar que necessitam estar contemplados neste Plano de Contingência, de forma a garantir o regular funcionamento da Gestora:

(i) Espaço Físico: local onde são realizadas as operações da Radar. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades de gestão de recursos;

(ii) Tecnologia: fundamental para o funcionamento da Radar relativamente às suas

atividades, no sentido de que todas as comunicações com clientes, corretoras, administradores de fundos etc., são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios). Também é fundamental para a realização de registros de operações (compras e vendas de títulos, aplicações e resgates em fundos de investimento, transferência de recursos e pagamento de despesas da Radar, dentro outros); e

(iii) Pessoal: responsáveis pela operação da Radar, incluindo a análise e decisão para realização ou não de investimentos, equipe responsável pelo *compliance* e pela gestão de risco das carteiras etc.

Tendo identificado esses 3 (três) focos de preocupação do ponto de vista da estrutura da Radar e dos processos sob sua responsabilidade na qualidade de gestora de recursos, os riscos que podem ocasionar o acionamento do Plano de Contingência foram identificados da seguinte forma:

(i) Problemas de Infraestrutura: os problemas dessa ordem são, dentre outros, falta de energia elétrica, falha nos links de internet, falha nas linhas telefônicas, falhas nos sites das empresas que fornecem sistemas de uso da Radar, falta de água etc.;

(ii) Problemas de acesso ao local/recursos: os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso ao local onde se localiza o escritório. Essa impossibilidade pode ser causada por eventos como greves, greves de transporte público, interdições pelas autoridades do prédio ou do entorno do escritório da Radar etc.; e

(iii) Falta impactante de colaboradores: os problemas dessa ordem são, dentre outros, o término de vínculo repentino com pessoas chave para o funcionamento da Radar (notadamente seus diretores), o não comparecimento de número expressivo de colaboradores em razão de doenças ou qualquer outro tipo de impedimento etc.

Com base no levantamento da estrutura da Radar relativa às suas atividades e no mapeamento de riscos, a Radar tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações e/ou no caso de falta impactante de colaboradores ao local de trabalho.

III. Situação de Emergência

Uma situação de emergência é aquela em que há risco de descontinuidade operacional, aqui entendido como o impedimento à execução de qualquer atividade essencial da Radar, ou processo do qual dependa uma atividade essencial.

São atividades essenciais:

(i) Atendimento ao cotista;

(ii) Disponibilização das informações diárias ao cotista via e-mail ou website;

(iii) Boletagem de operações ativas e passivas;

(iv) Compra e venda de ativos para os Fundos Geridos;

(v) Conferência e liberação das carteiras diárias dos Fundos Geridos; e

(vi) Acesso aos sistemas de informação.

Nesse sentido, a configuração de uma situação de emergência independe do fato do escritório sede encontrar-se ou não disponível para funcionamento parcial, ou seja, mesmo que a limitação existente não impeça a execução de outras atividades não listadas acima.

No entanto, para caracterizar uma situação de emergência, o impedimento à execução da atividade essencial deve ser por tempo prolongado ou indeterminado. Considera-se tempo prolongado sempre que o tempo transcorrido desde a interrupção da atividade alcance 2 (duas) horas, a expectativa de tempo até a solução da interrupção for superior a 2 (duas) horas, quando o tempo remanescente para a conclusão da atividade for insuficiente para sua execução no mesmo dia ou se a não execução imediata da atividade puder provocar prejuízo para os fundos de investimento sob gestão.

Uma vez constatada a situação de emergência, os Colaboradores da Radar devem seguir os procedimentos definidos nesse Plano de Contingência e, se necessário, entrar em contato com o Diretor de Compliance, Risco e PLD, para obter orientação adicional.

III.1. Situações de Emergência – Ambiente Físico

- Impedimento ao uso do Escritório-Sede: sempre que o acesso ao escritório sede estiver vedado, por qualquer razão, o primeiro Colaborador que constatar a situação deverá acionar imediatamente o Diretor de Compliance, Risco e PLDpara comunicar o fato, caso este não esteja no local.

Caso o motivo do impedimento seja a ocorrência de sinistro no escritório que possa implicar risco para segurança de terceiros – como incêndio, acidente grave, invasão, assalto, etc – antes de qualquer outra providência, o Colaborador deve comunicar o fato para o serviço público de emergência aplicável, conforme o caso, para só então acionar o Diretor de Compliance, Risco e PLD.

A ocorrência de qualquer incidente no escritório que impeça a execução de atividade essencial ou a interrupção por tempo prolongado ou indeterminado de qualquer dos serviços públicos de energia elétrica, telefonia ou banda larga, caracterizam uma situação de emergência.

No momento da constatação da interrupção do serviço público, o Diretor de Compliance, Risco

e PLD ou quem este indicar deverá contatar imediatamente o fornecedor do mesmo, para esclarecer a causa e o tempo estimado para a solução do problema.

III.2. Acesso Remoto

Conforme indicado acima, a rede da Radar utiliza um servidor de processamento centralizado em que são criadas máquinas virtuais acessíveis diretamente pelos usuários locais. Tal arquitetura permite que outros terminais ou redes locais possam ser utilizados para acessar a máquina virtual de cada Colaborador.

Quando constatada a situação de emergência, o Diretor de Compliance, Risco e PLD deverá, assim que possível, comunicar aos Colaboradores os motivos que deram origem a situação de emergência, e instruí-los a fazer *login* nos servidores por meio de acesso remoto.

Caso o escritório sede da Radar necessite ser evacuado, se a situação de emergência permitir, o Diretor de Compliance, Risco e PLD deve assegurar que este seja fechado após a saída de todos, para impedir o acesso de pessoas não autorizadas.

Uma vez tenha sido sanada a causa da situação de emergência, os Colaboradores em trabalho por acesso remoto deverão retornar imediatamente para o escritório sede da Radar.

III.3. Situações de Emergência – Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a Radar possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela Radar para as atividades de seu dia a dia e garantia de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da Gestora, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, softwares e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

Todos os sistemas utilizados pela Radar são acessados através de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da Radar. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência da Radar, de forma a que estes também tenham conhecimento da situação tão logo ela ocorra, buscando impactar o mínimo possível a operação da Radar.

III.4. Situações de Emergência – Pessoal

O ambiente pessoal envolve todos os colaboradores e prestadores de serviços existentes na Radar relacionados às suas atividades. Suas funções devem atender às necessidades de funcionamento da Radar em situações consideradas de normalidade bem como em situações consideradas de contingência.

Este Plano de Contingência visa atribuir prioridades e responsabilidades à equipe da Radar de forma a impactar o mínimo possível em suas atividades em situação de contingência.

O principal ponto identificado de risco é a não existência de um *back-up* de atividades executadas por um determinado funcionário. Esse risco, no entanto, não é considerado como relevante pois a estrutura da Radar já conta hoje com a definição e treinamento dos funcionários para atuação como *back-up* das funções e responsabilidades de seus colegas de Radar. Tal medida já existe e é praticada regularmente quando, por exemplo, um determinado colaborador se ausenta da Radar (por férias ou licença) e suas atividades continuam sendo executadas pelo seu *back-up* designado.

IV. Prevenção e Segurança

A Radar, por meio do seu Diretor de Compliance, Risco e PLD, deverá adotar procedimentos de prevenção de incidentes e disponibilização de recursos de segurança patrimonial e pessoal, de forma a evitar, dentro do possível, a ocorrência de situações de emergência.

V. Disponibilidade e Segurança da Informação

Além de assegurar a disponibilidade e acesso das informações para o funcionamento normal de atividades essenciais, a Radar tem claramente definida a importância de se preservar a integridade e o sigilo dos dados relativos aos ativos (investimentos) e passivos (cotistas) dos fundos de investimento sob gestão. Para maiores detalhes, recomenda-se a leitura da Política de Segurança da Informação da Radar.

VI. *Responsabilidade Pelo Plano de Continuidade de Negócios e Prazo para Acionamento*

A responsabilidade maior pela execução dos procedimentos de emergência é do Diretor de Compliance, Risco e PLD, e subsidiariamente, de todos os sócios da Radar, dentro das suas respectivas áreas de atuação. Nesse sentido, no que diz respeito à execução dos procedimentos aqui descritos, o Diretor de Compliance, Risco e PLD possui autoridade sobre os demais, inclusive para delegar e determinar atribuições durante a situação de emergência. Não obstante, para a efetiva coordenação de todas as ações necessárias em situações de contingência bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da Radar, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance, Risco e PLD (Coordenador de Contingência); e

- Diretor de Gestão.

Ademais, mesmo considerando a clara definição de responsabilidades acima, para assegurar a continuidade dos negócios, é imprescindível que todos os Colaboradores da Radar, tenham sempre presente a importância do espírito de prevenção de incidentes que levem a situações de emergência, bem como o pleno conhecimento e estrita observância deste Plano de Contingência, independentemente da sua função ou nível hierárquico na Radar.

O modo contingencial será acionado quando for identificada qualquer ocorrência ou situação que dificulte ou impeça a rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, aos clientes da Gestora e à Gestora.

O Coordenador de Contingência deverá acompanhar todo o processo descrito neste Plano de Contingência até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela Radar e reportar eventuais alterações e atualizações da contingência aos demais colaboradores.

VII. *Aspectos Gerais e Testes Específicos para o Plano de Continuidade de Negócios*

Este Plano de Contingência é de uso restrito dos Colaboradores da Radar e **não** pode ser divulgado para terceiros, exceto se autorizado pela Equipe de Contingência.

É responsabilidade do Coordenador de Contingência manter este Plano atualizado, bem como a realização de validação **anual** dos procedimentos estabelecidos neste Plano de Contingência.

Ainda, o Diretor de Compliance, Risco e PLD realizará testes de contingências que possibilitem que a Gestora esteja preparada para eventos desta natureza, proporcionando à Gestora condições adequadas para continuar suas operações.

Sendo assim, anualmente, é realizado um teste de contingência para verificar:

a) Acesso aos sistemas;

b) Acesso ao e-mail corporativo;

c) Acesso aos dados armazenados; e

d) Qualquer outra atividade necessária para continuidade do negócio.

O resultado do teste é registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

CONTROLE DE VERSÕES

Histórico das atualizações		
Data	Versão	Responsável
Junho de 2022	2ª e Atual	Diretor de *Compliance*, Risco e PLD