HASHDEX GESTORA DE RECURSOS LTDA.

# PLANO DE CONTINUIDADE DE NEGÓCIOS

# 1. VISÃO GERAL

A Política de Contingência e Continuidade de Negócio (“PCCN” ou “Política”) tem por objetivo estabelecer as medidas e os procedimentos a serem tomados para identificar e prevenir possíveis contingências que poderão trazer um impacto negativo considerável sobre a condução das atividades da Hashdex Gestora de Recursos Ltda. ("Hashdex” ou “Instituição”).

Essa Política foi elaborado com base no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros (“Código ANBIMA”) e demais normas aplicáveis, para orientar sobre questões relacionadas às contingências, podendo ser essas, por exemplo, crises econômicas relacionadas às atividades da Hashdex, controle de acesso às informações, segurança pessoal, segurança física, desenvolvimento e manutenção de sistemas, falhas operacionais, pandemias e/ou desastres naturais.

Desse modo, a presente Política, informa, organiza, orienta, treina, facilita e uniformiza as ações a serem desenvolvidas pela Hashdex em situações que poderiam causar a descontinuidade do negócio. Estão sujeitos aos procedimentos aqui descritos todos os colaboradores, sócios, funcionários e estagiários (em conjunto “Colaboradores” e em separado “Colaborador”) da Hashdex, os quais devem conhecer integralmente as disposições, devendo zelar pelo seu fiel cumprimento, naquilo que lhes couber.

# 2. EVENTOS/AMEAÇAS PREVISTAS

Esta Política prevê dois tipos de Eventos de Interrupção de Negócios Significativos (“EINS”) - internos e externos.

Os EINS internos afetam apenas a capacidade de nossa empresa de se comunicar e fazer negócios, tais como:

- Impossibilidade de acessar fisicamente o prédio de escritórios devido a incêndio, inundação ou questões legais; e
- Quaisquer problemas de infraestrutura com conexão à Internet ou perda de energia.

Os EINS externos impedem a operação dos mercados de valores mobiliários ou de várias empresas, como:

- Ataque terrorista;
- Enchente na cidade;

- Pandemia;[1]
- Qualquer perturbação regional / global em grande escala; e
- Qualquer outra situação que ameace o ambiente da Hashdex, que não descrita acima.

## 3. PRINCIPAIS NORTEADORES

A Hashdex, pautada pelos deveres de diligência e cuidado, e pela responsabilidade que norteiam a condução de seus negócios, em casos de ocorrência de quaisquer eventos ou sinistros que possam inviabilizar, paralisar ou comprometer temporariamente os exercícios de suas atividades seguirá os procedimentos aqui definidos ou, nos casos não previstos, seguir os procedimentos estabelecidos pela sua diretoria.

Utilizando-se do disposto no Código ANBIMA e nas demais normas aplicáveis, consideram-se de forma pragmática os eventos com maior possibilidade de ocorrência, dada a localização e características das instalações da edificação em que se encontra a sede da Instituição, e sua estrutura tecnológica. Desta forma, é possível conhecer e minimizar os prejuízos, reduzindo o tempo para a normalização de suas atividades.

De modo a tornar efetivo a presente Política, todos os Colaboradores da Hashdex deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não), os planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho. A Hashdex buscará sempre identificar antecipadamente quais os riscos relacionados ao seu negócio, sejam eles físicos, patrimoniais ou financeiros.

## 4. AUTORIDADE DE APROVAÇÃO E EXECUÇÃO

Bruno Sousa - Diretor do Compliance da Hashdex - é responsável pela aprovação do plano e pela realização da revisão anual necessária ("Líder do Plano"). O Diretor de Risco, o *Head* de Cibersegurança e Segurança da Informação, o Diretor de Administração Fiduciária e Diretor de Distribuição têm autoridade para executar este Plano e compõe o Comitê de Crise da Hashdex.

Nesse sentido, as funções relacionadas às atividades de contingência estão assim discriminadas:

| Atividades | Responsáveis |
|---|---|

[1] Além das medidas cabíveis previstas no item 5 desta Política, na ocorrência de uma pandemia, há que se observar as considerações do Anexo I.

| | |
|---|---|
| Manutenção e Atualização do Plano | *Head de Cibersegurança* |
| Aprovação, Revisões e conduzir revisão anual | Comitê de Risco Compliance |
| Treinamento e Teste anual do Plano | *Head de Cibersegurança* |
| Emergency Response Team | Diretor de Compliance, Diretor de Risco, Diretor de Administração Fiduciária e *Head de Cibersegurança* |
| Revisão Trimestral da lista de Contatos de Emergência | Diretor de Compliance, Diretor de Risco e *Head de Cibersegurança* |
| Manutenção e distribuição da lista de Contatos de Emergência | Diretor de Compliance |
| Prover informações do plano para investidores e CVM | Diretor de Compliance |
| Revisar Planos de Continuidade de Prestadores de Serviços Essenciais | Diretor de Compliance, Diretor de Risco, Diretor de Administração Fiduciária e *Head de Cibersegurança* |
| Contração dos Serviços Relacionados ao Plano | Diretor de Compliance, Diretor de Risco e *Head de Cibersegurança* |

## 5. Plano de Contingência

Os dados eletrônicos da Hashdex são mantidos em servidores com acesso restrito. A Hashdex utiliza uma plataforma sob o conceito de *Cloud Computing*, permitindo a integração dos serviços de e-mail, agenda e determinados documentos de forma compartilhada, cujos dados são armazenados e transferidos via plataforma Google Workspace de forma segura e possuem persistência por tempo indeterminado, além de replicados em tempo real para um centro de dados de *backup*, que é submetido a revisões de segurança.

Os sistemas e dados dos sistemas usados pelos colaboradores da Hashdex armazenados e transferidos por meio de conexão segura TLS para os servidores da Amazon Web Services, segundo sua política de distribuição por suas 18 zonas geográficas, e que são amplamente reconhecidos como estando entre os melhores serviços do tipo no mundo.

Desta forma, no caso do advento dos eventos descritos no Item 2 acima, a Empresa acionará o Plano de Contingência - que consiste em transferir toda a operação *in loco* da Hashdex para a modalidade *home office*. Isto é possível considerando que todos os sistemas, dados e informações utilizados pela Instituição estão em ambiente de *cloud-computing* (Google Workspace e Amazon Web Services), mantendo a segregação de atividades entre as diferentes áreas da Hashdex - dado que os acessos dos Colaboradores é concedido na medida exata das suas necessidades para o exercício de suas funções e não sofre qualquer alteração com o acionamento do plano de contingência.

Em paralelo, a Hashdex mantém à disposição espaços físicos (salas privativas em *coworking*), mediante contratação sob demanda, que poderão ser utilizados para o desempenho das atividades definidas pelos gestores da cada área da Hashdex em escritórios localizados no Rio de Janeiro e em São Paulo, de acordo com a demanda específica de cada área demandante. As demandas podem incluir reuniões com clientes, prestadores de serviços ou, entre o time da Hashdex. Ainda, tais espaços de escritório podem ser utilizados na hipótese de algum colaborador, que estiver em *home office*, necessitar de acesso a algum local para continuidade de suas funções em razão de algum problema com a infraestrutura de sua residência, como falta de luz ou acesso à internet) Os escritórios contratados possuem redundância de internet e gerador para garantir o funcionamento contínuo dos serviços.

Para utilização destes espaços físicos, o gestor da área ou o colaborador deverão solicitar ao RH esta demanda com, no mínimo, 24 horas de antecedência, exceto em caso de eventual urgência, conforme acima referido. O RH irá avaliar a necessidade da quantidade de salas separadas para fins de manutenção da segregação física e funcional em caso de áreas ou colaboradores conflitantes demandarem concomitantemente, nos termos mencionados na Política de Segregação de Atividades da Hashdex

Caso haja necessidade de utilização destas salas por mais de 5 (cinco) dias úteis consecutivos, o RH deverá diligenciar para que equipamentos e materiais próprios para estrutura de cada área sejam incluídos nos escritórios, de forma que não haja utilização de itens como link de internet e impressora compartilhados com demais usuários do *coworking*.

Ainda sobre a eventual utilização destes espaços físicos, os colaboradores serão sempre orientados a evitar: (i) de circular fora da sala própria com cópias físicas ou digitais de arquivos com informações confidenciais; (ii) discutir em áreas comuns sobre assuntos confidenciais; (iii) utilização de impressora e rede de telefone do *coworking* para assuntos confidenciais da Hashdex, devendo utilizar seus aparelhos próprios – celular e notebook – e impressora disponibilizada pela Hashdex quando necessário; e (iv) quando da utilização de sala de reuniões, de deixar qualquer documento ou anotação sobre a mesa ao sair.

A Hashdex mantém uma lista de Contatos de Emergência que inclui os nomes, telefones, endereços de e-mail dentre outras informações críticas para o negócio. Esta lista inclui colaboradores-chave de cada área e provedores de serviços e será revista e atualizada ao menos anualmente, e está disponível para os Colaboradores:

| **Colaboradores** | **Nome** | **Email** |
|---|---|---|
| **Diretor de Compliance** | Bruno Ramos | bruno.sousa@hashdex.com |
| **Tecnologia da Informação** | Eduardo Gonçalves | eduardo.gonçalves@hashdex.com |
| **Administração Fiduciária** | Bruno Caratori | b@hashdex.com |
| **Operações** | Leonardo Burlá | leonardo.burla@hashdex.com |
| **Distribuição e *Suitability*** | Bruno Leonardo Kmita de Oliveira Passos | bl@hashdex.com |
| **People** | Jeremie Corcos | jeremie.corcos@hashdex.com |
| **Produtos** | Samir Kerbage | samir.kerbage@hashdex.com |
| **Finance** | José Pinto | jose.pinto@hashdex.com |
| **Gestão** | João Cunha | joao.cunha@hashdex.com |
| **Marketing and Growth** | Roberta Antunes | roberta.antunes@hashdex.com |

Abaixo, encontraremos nossa definição de impacto de uma interrupção do serviço em diferentes áreas. Uma interrupção nos negócios pode impactar uma organização de várias maneiras. A Hashdex define cinco categorias principais que são usadas para medir o impacto.

- Segurança e vida humana (S / HL)
- Financeiro (Fin)
- Reputação (Rep)
- Operações (Ops)
- Regulatório e Legal (Leg)

Para cada um dos serviços e processos críticos, determinaremos o impacto em cada uma das categorias aplicáveis com base nos seguintes valores:

| Impacto | Descrição |
|---|---|
| Catastrófico | As consequências ameaçariam a prestação de serviços e processos essenciais, causando grandes problemas para os investidores e exigindo envolvimento e ação imediata dos diretores. As consequências podem incluir grandes danos ou destruição, ameaça iminente à segurança humana, perda de vidas ou ferimentos graves e perdas monetárias extremas |
| Grande | As consequências ameaçariam o fornecimento contínuo e eficaz de serviços e processos e exigiriam o envolvimento dos diretores. As consequências podem incluir danos ou destruição significativos, alguns ferimentos leves ou ameaça à segurança humana sem perda de vidas, grandes perdas monetárias. |
| Moderado | As consequências não ameaçariam o fornecimento de serviços e processos, mas significariam que as operações de negócios poderiam estar sujeitas a uma revisão significativa ou mudanças nas formas de operação. O envolvimento executivo provavelmente seria necessário. As consequências podem incluir perdas monetárias moderadas. |
| Menor | As consequências ameaçariam a eficiência ou eficácia de alguns serviços e processos, mas seriam tratadas na unidade de negócios ou no nível de departamento. As consequências podem incluir nenhuma ou baixas perdas monetárias. |

Além disso, precisamos abordar a sensibilidade do tempo de interrupções de serviço que pode ser determinada calculando o objetivo de tempo de recuperação (RTO) necessário e o objetivo de ponto de recuperação (RPO).

O objetivo do RTO é determinar quando o serviço precisa ser recuperado após uma interrupção, com base na quantidade aceitável de tempo de inatividade e nível de desempenho. Por exemplo,

um RTO de 24 horas com acessibilidade local para serviços de folha de pagamento significa que o aplicativo de folha de pagamento deve estar instalado e funcionando em 24 horas, bem como acessível localmente.

O objetivo do RPO é determinar quantos dados ou informações podem ser perdidos após uma interrupção, com base na quantidade aceitável de dados ou perda de informações. Por exemplo, um RPO de 6 horas para serviços de folha de pagamento significa que os dados da folha de pagamento devem ser copiados a cada 6 horas para que não mais do que 6 horas de dados inseridos no aplicativo de folha de pagamento sejam perdidos após uma interrupção.

Se o risco estiver presente, determine as implicações e se uma estratégia para lidar com tal risco é necessária ou não. Classificaremos os impactos usando os seguintes termos:

| Prioridade de serviço | Objetivo de ponto de recuperação (RPO) | Objetivo de tempo de recuperação (RTO) |
|---|---|---|
| Crítico | 0 (sem perda de dados) | dentro de 24 horas |
| Vital | 0 (sem perda de dados) | dentro de 48 horas |
| Necessário | 24 horas | dentro de 2 semanas |
| Desejado | 48 horas | mais de 2 semanas |

Dado o enorme nível de incerteza em torno de qualquer novo evento, o comitê de Risco e Compliance revisa anualmente a matriz de EINS e todos os serviços críticos, fornecendo informações sobre os departamentos pelos quais eles são usados, sua localização, períodos de criticidade, planos de ação (se disponíveis), interrupção máxima permitida, bem como subjacente serviços ou aplicativos dos quais eles dependem.

O framework para a construção de novos cenários EINS envolve:

- Revisão dos EINS para avaliar se eles seguem pertinentes frente a uma nova ameaça de disrupção
- Revisão da definição de riscos e a análise da adição de novos riscos
- Revisão das matrizes de mitigação de risco e responsabilidades

Todos os colaboradores participam da revisão e treinamento anual da lista de EINS e de suas responsabilidades.

## 6. Procedimento em Caso de Crise

Uma vez que um potencial evento de crise é identificado, o Líder do Plano é deverá convocar os Colaboradores-chave da Hashdex para formar o Comitê de Crise e avaliar conjuntamente a situação e os próximos passos. Caso não seja possível devido à situação emergência, poderá tomar as decisões para gerir a crise individualmente.

Na etapa inicial, aspectos e decisões fundamentais serão analisadas e tomadas após o incidente. O foco da reunião do Comitê ou, se for o caso, do Líder do Plano deverá compreender uma análise do que aconteceu, motivos, extensão, consequências imediatas e gravidade da situação, segurança dos Colaboradores e medidas imediatas, devendo decidir pela formalização ou não da crise.

Se for caracterizado um cenário de crise, devem os membros do Comitê efetuar a comunicação ao restante dos Colaboradores, informando as medidas imediatas, que poderão abranger a evacuação do prédio, acionar assistência médica imediata, notificação dos serviços de emergência, realocação de Colaboradores internos, definindo se o local alternativo será utilizado e por quem, formas de comunicações e notificação de parceiros-chave estratégicos. Com relação à parte de segurança cibernética, a Hashdex deverá definir medidas a serem tomadas, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares e instruir o provedor de Telecom a desviar linhas de dados/e-mail.

O Comitê de Risco e Compliance deverá se reunir também para avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, devendo a área de Gestão verificar se todas as informações necessárias ao portfólio estão seguras e se são necessárias decisões de investimento. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Hashdex, devem ser comunicados ao comitê de crise.

Os colaboradores da área de operações são responsáveis por manter o controle de EINS nos provedores de serviços financeiros como custodiantes, outros administradores, bancos liquidantes e os diversos sistemas de integração financeira, devendo seguir os procedimentos definidos pelos manuais e matrizes de impacto respeitando os RTOs e RPOs definidos e aprovados no comitê de Risco e Compliance.

Após a crise ser contornada, durante período de transição do retorno ao modo normal de operação, o comitê de crise promoverá a análise de projetos, de forma a voltar ao full compliance, a reconstrução de eventuais sistemas, eventuais reformas do escritório e outras mudanças de acordo com o RPO e RTO estimado para o evento.

## 7. Comunicação Pública

Caso ocorra um evento/ameaça cujo resultado seja a inacessibilidade temporária ou permanente do escritório, o Líder do Plano é responsável por elaborar comunicado formal aos investidores, terceiros contratados e ao mercado em geral.

Na impossibilidade de atuação de qualquer um deles, somente a Diretoria está autorizada a realizar esta função, sendo absolutamente vedado aos demais Colaboradores a comunicação pública sobre o ocorrido.

## 8. Avaliação e Testes Periódicos

O Plano deverá ser avaliado e testado ao menos uma vez a cada 12 (doze) meses, em prazo inferior se exigido pela regulação em vigor ou periodicamente em razão das mudanças naturais ocorridas na Hashdex, tais como: entrada e saída de Colaboradores, troca de sistemas, mudança de estratégia de proteção e etc. A execução deste teste é de responsabilidade da área de Compliance, em conjunto com a área de Cibersegurança e Segurança da Informação.

O teste terá como objetivo também se o Plano é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se pode ser ativado tempestivamente - contemplando os seguintes pontos:

1. Acesso aos sistemas;
2. Acesso ao e-mail corporativo remotamente;
3. Acesso aos dados armazenados em procedimento de backup; e
4. Qualquer outra atividade necessária para a 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 desta Política.

## 9. Continuidade do Negócio

Para a continuidade de negócios em momentos de crises, deverão ser mantidos sempre atualizados procedimentos que permitam à Hashdex:

1. Garantir e aumentar a frequência de comunicação com os provedores de serviços financeiros dos quais os fundos geridos e administrados pela Hashdex possuam parceria, visando evitar uma reação em cadeia de disrupção de serviços.
2. Aumentar rapidamente seu contingente de pessoal técnico qualificado e/ou fornecedores caso a demanda por seus serviços aumente rapidamente sem que isso implique na queda da qualidade da prestação dos serviços;
3. Identificar novos potenciais mercados de atuação e/ou produtos caso haja queda, ou longos períodos de recessão, na demanda de seus clientes atuais;

4. Manter-se sempre competitiva e inovadora, de forma a evitar a perda de sua participação no mercado, com a exploração de seus pontos fortes e com a constante diminuição de seus pontos fracos;
5. Valer-se de suas vantagens competitivas no mercado;
6. Ampliar constantemente sua base de clientes, de forma que seja mantido o grau de pulverização na carteira de clientes adequado ao porte da Hashdex e a manutenção da confiabilidade e qualidade dos serviços prestados; e
7. Manter um fluxo de caixa que, à critério da diretoria, seja hábil para fazer frente às despesas imprevisíveis.

# Anexo I

## Questões Específicas sobre Períodos de Pandemia

Tradicionalmente, a maioria dos planos de continuidade de negócios concentra-se no que acontecerá se o edifício, equipamento, produtos ou serviços forem danificados de alguma forma. Os planos também tendem a assumir que as pessoas possam retornar ao prédio, ou começar a reconstruir, quase imediatamente após o evento (como após um incêndio ou tempestade, ou se houver falta de serviços públicos (hidro, gás, etc.)).

No entanto, se houver uma doença infecciosa grave, surto ou pandemia, devemos planejar para que os funcionários não possam comparecer presencialmente no escritório (não relacionado a danos ao prédio). Além disso, durante uma pandemia, empresas, organizações sociais ou escolas podem ser obrigadas a tomar medidas específicas para ajudar a retardar a propagação da doença, incluindo o fechamento por ordem do médico oficial de saúde ou de funcionários de saúde pública. Outras medidas de saúde pública podem incluir limitar ou cancelar reuniões sociais e públicas, parar o transporte público, exigir quarentenas, etc.

Além disso, a recuperação dessas situações pode não ser iniciada imediatamente. É importante ter certeza de que nossas atividades comerciais principais podem ser mantidas por várias semanas ou meses com pessoal limitado.

Neste cenário, é justo presumir que as pessoas podem não ser capazes de trabalhar presencialmente no escritório por muitos motivos, que incluem:

- Estar doente ou em quarentena (casos suspeitos, reais ou pós-infecciosos)
- Desempenhar funções de voluntário na comunidade, incluindo ajudar com serviços de emergência
- Cuidar de crianças em idade escolar (se estiverem doentes ou caso as escolas estejam fechadas) ou outros membros da família
- Preferir ficar em casa, ou sob ordem obrigatória da rede pública de saúde
- Evitando espaços públicos, incluindo reuniões e evitando o transporte público
- Na pior das hipóteses, eles podem ter morrido ou estar com uma deficiência de longo prazo.

Os planos elaborados para estes cenários, além daqueles já previamente definidos no item 5 desta Política de Contingência e Continuidade de Negócio da Hashdex, envolvem também a criação de um cenário de Caso Base assim que o evento for identificado, documentando uma linha do tempo de eventos e revisão dos atuais EINS e eventuais ajustes nos cenários e matrizes de risco para garantir a continuidade das operações essenciais de administração e gestão de recursos financeiros.