PLANO DE RECUPERAÇÃO DE DESASTRES E CONTINUIDADE DOS NEGÓCIOS

Definições

Termo	Definição
ANBIMA	Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.
Código ANBIMA de ART	Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.
Colaboradores	Todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, de estágio, comercial, profissional, contratual ou de confiança com as empresas da Gestora.
CVM	Comissão de Valores Mobiliários
Diretor de Compliance	É o diretor estatutário da Gestora indicado em seu respectivo Formulários de Referência como responsável pelo cumprimento de regras, políticas, procedimentos e controles internos e pelo combate e prevenção à lavagem de dinheiro e ao financiamento do terrorismo.
Diretor de Distribuição	Quando aplicável, é o diretor estatutário indicado como responsável pela atividade de distribuição das respectivas sociedades que integram à Gestora.
Diretor de Investimentos	É o respectivo diretor estatutário responsável pela administração de carteiras de valores mobiliários da Gestora, conforme identificado em seu respectivo Formulário de Referência.
Gestoras	ASA Asset 2 Gestão de Recursos Ltda (“ASA” ou “Gestora”.)
Recursos Humanos	É a Equipe de Recursos Humanos da Gestora.

1. OBJETIVO

O Plano de Recuperação de Desastres e Continuidade dos Negócios – PCN, deve assegurar à Gestora a recuperação e manutenção de suas atividades em caso de uma interrupção das operações normais do negócio. O PCN visa estabelecer estratégias e ações que possam mitigar incidentes de grandes proporções, sendo de origem interna e/ou externa.

Este PCN trata de um conjunto de estratégias e procedimentos que visam garantir o mínimo de interrupção das atividades que impactam no negócio, além de proteger os processos críticos no caso de alguma falha.

2. VIGÊNCIA E ATUALIZAÇÕES

As diretrizes contidas neste PCN entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser mantidas atualizadas, de acordo com a alteração de legislação aplicável, ou ainda, se houver alteração no modelo de negócios, previamente validado pelo Compliance.

A aprovação deste PCN e posterior atualizações deverão ser realizadas pelo Comitê de Compliance, com aprovação registrada em ata.

3. ABRANGÊNCIA

Este PCN tem como público-alvo todos Colaboradores da Gestora, bem como prestadores de serviços que realizem atividades em seu nome.

4. METODOLOGIA

A estratégia para desenvolvimento deste PCN partiu da identificação dos riscos e definição das medidas preventivas para os riscos identificados, objetivando reduzir a possibilidade de interrupção da Gestora.

.

5. DIRETRIZES

As diretrizes e regras estabelecidas abaixo devem ser interpretadas como determinações obrigatórias:

O ambiente operacional da Gestora é arquitetado para alta disponibilidade do ambiente operacional, garantindo contingência contra incidentes e desastres

originados por fatores sistemáticos, físicos ou sociais. Os colaboradores, mediante a aprovação e liberação da Área de Segurança da Informação podem conectar remotamente (qualquer lugar) via VPN, não será designado site de contingência externo, a contingência será realizada em home office.

6. TECNOLOGIA

As informações geradas internamente, adquiridas no mercado ou absorvidas pela Gestora são consideradas patrimônio, devendo ser tratadas como ativo e confidencial. No caso de exceção, informações cuja divulgação seja obrigatória ao mercado e clientes por exigência de órgãos reguladores deve ser cuidadosamente avaliada e passar por autorização da Diretoria. Tal autorização deve ser respeitada durante todo o ciclo de vida desta informação.

Todos os sistemas utilizados pela Gestora estão em nuvem e os acessos se dão através de login e senha de cada usuário.

7. ARQUITETURA DO AMBIENTE COMPUTACIONAL

O ambiente operacional da Gestora é arquitetado para alta disponibilidade do ambiente operacional, garantindo contingência contra incidentes e desastres originados por fatores sistemáticos, físicos ou sociais. Existem dois sites na cidade de São Paulo, com uma réplica sobressalente de seu datacenter primário, ademais, os serviços em nuvem estão alocados em múltiplas regiões por meio de provedores de cloud com presença mundial. Os colaboradores, mediante a aprovação e liberação da área de Segurança da Informação podem conectar remotamente (qualquer lugar) via VPN para acesso aos servidores e máquinas virtuais.

8. ANÁLISE DE IMPACTO

A análise de impacto do negócio foi sumarizada para garantir que os plano de ação responda a maior parte dos desastres, incidentes e consequentes possíveis perdas ao negócio. São eles:

- Indisponibilidade de acesso ao escritório: Falha nos equipamentos de telecomunicação, impossibilidade total ou parcial de acesso ao escritório.
    - Ameaças Consideradas:

- Incêndios
- Explosões
- Falta de energia
- Distúrbios sociais
- Falha em equipamentos de telecomunicação

- Plano de Ação:
  - O colaborador está em posse do seu notebook ou máquina Desktop, e pode realizar a conexão através de VPN cliente-servidor para executar e acessar os sistemas, incluindo os sistemas de comunicação, como telefonia e mensageria. Ademais, esse modelo também permite acesso a uma máquina virtual dentro da estrutura em Nuvem da Gestora.

- Indisponibilidade de um ou mais sistemas na Nuvem e em uma das réplicas: Falha nos equipamentos de telecomunicação, impossibilidade total ou parcial dos sistemas.
  - Ameaças Consideradas:
    - Incêndios
    - Explosões
    - Falta de energia
    - Falha em equipamentos de informática
    - Falha de sistemas
    - Falha em equipamentos de telecomunicação

  - Plano de Ação:
    - Inativar o uso da réplica com incidente e manter somente a réplica que está em plena integra no ar.

- Indisponibilidade do Datacenter Primário: Falha nos equipamentos de telecomunicação, impossibilidade total ou parcial dos sistemas.
  - Ameaças Consideradas:
    - Incêndios
    - Explosões

- Falta de energia
- Falha em equipamentos de informática
- Falha de sistemas
- Falha em equipamentos de telecomunicação

- Plano de Ação:
  - Inativar o Datacenter Primário e efetuar o uso somente do Datacenter Secundário.

- **Indisponibilidade dos links de acesso:** Falha nos equipamentos de telecomunicação, impossibilidade total ou parcial dos sistemas.
  - Ameaças Consideradas:
    - Incêndios
    - Explosões
    - Falta de energia
    - Falha em equipamentos de informática
    - Falha de sistemas
    - Falha em equipamentos de telecomunicação

  - Plano de Ação:
    - O colaborador está em posse do seu notebook ou máquina Desktop, e pode realizar a conexão através de VPN cliente-servidor para executar e acessar os sistemas, incluindo os sistemas de comunicação, como telefonia e mensageria. Ademais, esse modelo também permite acesso a uma máquina virtual dentro da estrutura em Nuvem da Gestora.

9. GESTÃO DE CRISE E RECUPERAÇÃO DE DESASTRES

Será nomeado um Coordenador de Gestão de Crise e Recuperação de Desastres, que será o responsável pelas aprovações e tomadas de decisão em momentos de crise e desastres, assim como também para a retomada dos serviços e processos ao seu estado original. As responsabilidades deste coordenador serão atribuídas pela Diretoria de Compliance.

10. IDENTIFICAÇÃO E CLASSIFICAÇÃO

Tendo identificado os fatores principais que integram seu PCN do ponto de vista da estrutura da Gestora e dos processos sob sua responsabilidade, os riscos que podem ocasionar o acionamento do PCN foram identificados da seguinte forma:

- Problemas de Infraestrutura: os problemas dessa ordem são, dentre outros, falha e/ou interrupção no fornecimento de serviços essenciais como a falta de energia elétrica, falta de água, falha nas conexões de rede, falha nos links de internet, falha nas linhas telefônicas, falhas nos sites das empresas que fornecem sistemas de uso;
- 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, por exemplo, de transporte público, interdições pelas autoridades do prédio ou do entorno do escritório.

Com base no levantamento da estrutura da Gestora e no mapeamento de riscos, a Gestora tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações.

Neste sentido, conforme avaliação de risco da Gestora, foram definidos 2 (dois) ambientes básicos que devem ser considerados nas ações a serem tomadas quando da ativação deste PCN. Esses ambientes são: Físico e o Tecnológico.

(i) Ambiente Físico

O ambiente físico é definido como o espaço onde as operações diárias da Gestora são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e equipamentos necessários a essa operação, como também o acesso seguro a esses recursos.

Em ocorrendo situações de problemas de acesso às suas dependências, os colaboradores da Gestora devem continuar a desempenhar suas atividades a partir do PCN.

O PCN contempla acesso remoto aos ambientes da Gestora na nuvem, através do qual, os usuários-chaves para continuidade dos negócios têm, através de

uma VPN e seu login único e individual de usuário, acesso a todos os sistemas e arquivos necessários para realizar suas atividades.

(i) Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a Gestora possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela empresa em seu dia a dia e a garantia de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da empresa, 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 Gestora no ambiente da gestão 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 Gestora. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência, de forma a que também estes tenham conhecimento da situação, de forma a impactar o mínimo possível a operação.

A Gestora conta com colaboradores que prestam serviços de Tecnologia e Segurança da Informação, os quais estarão 100% (cem por cento) disponíveis na hipótese de uma situação de contingência.

As informações relativas a backup, hardware, firewall, servidores, telefonia, rede, e-mails etc. estão cobertas no PCN.

11. DECLARAÇÃO DE CONTIGÊNCIA

Caso seja detectada alguma das situações descritas no item 11, o Coordenador de Gestão de Crise e Recuperação de Desastres deverá ser contatado imediatamente.

O Coordenador de Gestão de Crise e Recuperação de Desastres deverá acompanhar todo o processo até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela Gestora e reportar eventuais alterações e atualizações da contingência aos demais colaboradores.

12. TESTES DE CONTIGÊNCIA

Os ambientes de contingência deverão ser testados pelo menos 1 (uma) vez ao ano, garantido o bom funcionamento do ambiente, caso necessário. Os testes devem ser evidenciados e documentados para constante melhorias no processo.

13. SITES DE CONTIGÊNCIA

Definimos como sites remotos as residências e/ou, escritórios, como ferramentas definimos utilizar de: webmail, celulares com serviço de e-mail e acesso remoto que permitem que os funcionários possam realizar tarefas fora do ambiente do escritório.

Se necessário, ainda poderá ser avaliado a utilização das instalações de empresas cujo controle societário seja o mesmo da Gestora, que conta com estrutura segregada e independente.

14. DIVULGAÇÃO DA POLÍTICA E DOCUMENTOS ACESSÓRIOS

Regras gerais para a divulgação da política, de forma a permitir livre acesso e ciência por todos os cobertos pelo seu manto, mantendo a consistência e atualidade dos documentos diante de mudanças.

É implementado um controle de versões online da política e dos documentos acessórios associados. O controle de versões permite:

- Que os usuários tenham conhecimento da versão da política e documentos acessórios vigentes; e
- Possam consultar as versões históricas e seus respectivos períodos de vigência.

Qualquer mudança na política ou nos documentos acessórios:

- É acompanhada de ampla divulgação do necessário e suficiente para a ciência, de facto, dos usuários;
- A divulgação é completa, incluindo a política e documentos acessórios vigentes e a data de sua vigência;

- Versões anteriores e suas vigências ficam disponíveis para ampla consulta por qualquer usuário, a qualquer tempo;
- A divulgação de novas versões incorporará facilidades indicando de forma resumida as mudanças.

O gerenciamento e disponibilização para os usuários do controle de versões, incluindo seu conteúdo e seu processo de divulgação:

- É de responsabilidade da área de Segurança da Informação;
- É a fonte primária de consulta da política e seus documentos acessórios por parte dos usuários;
- É um veículo administrativo obrigatório, sem prejuízo de qualquer outro, para divulgação e ciência das obrigações por parte dos usuários;
- As versões históricas com suas vigências é a fonte de consulta para verificação de regras e responsabilidades de eventuais eventos ocorridos à época de suas respectivas vigências.

15. EXCEÇÕES

Situações que não se encaixem ou estejam em desacordo de qualquer maneira com este PCN, deverão ser submetidas para Área de Segurança da Informação, que analisará as circunstâncias e fundamentos e deliberará em conjunto com os Diretor de Compliance e de Recursos Humanos da Gestora.

HISTÓRICO DAS ATUALIZAÇÕES DO PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGOCIOS

Histórico das atualizações desta Política		
Data	Versão	Responsável
Janeiro de 2020	1ª	Diretor de Compliance
Dezembro de 2020	2ª	Diretor de Compliance
Junho de 2021	3ª	Diretora de Compliance e Risco
Outubro de 2021	4ª	Diretora de Compliance
Outubro de 2022	5ª	Diretor de Compliance
Agosto de 2024	6ª e atual	Atualização de layout