Política de Risco Operacional e Continuidade de Negócios
Bahia AM Renda Variável Ltda. e Bahia AM Renda Fixa Ltda.

01. OBJETIVO:

A Bahia AM Renda Variável Ltda. e a Bahia AM Renda Fixa Ltda. (doravante denominadas em conjunto "Gestoras") visam sua permanente conformidade com as normas cabíveis, bem como reduzir os riscos incorridos diante da natureza de seus negócios.

A presente Política de Risco Operacional e Continuidade de Negócios das Gestoras ("Política) expõe a análise qualitativa dos riscos operacionais e informa o modo pelo qual as Gestoras responderão a possíveis eventos de forma a garantir que as funções críticas do negócio retornem dentro de um prazo conveniente.

Este documento aplica-se a todos os sócios, administradores, empregados e estagiários (doravante denominados em conjunto "Colaboradores") das Gestoras, bem como todas e quaisquer sociedades a elas ligadas destinadas à gestão de recursos de terceiros devendo todos seguirem as diretrizes aqui apresentadas.

As menções aos fundos sob gestão no presente documento devem ser entendidas como menções às classes e subclasses, conforme aplicável, sem prejuízo das características e condições particulares de cada classe e subclasse, em linha com a regulamentação vigente e os respectivos anexos e suplementos.

02. CONCEITUAÇÃO / DEFINIÇÃO:

O Comitê de Basiléia (2003) define enquanto risco operacional o risco de perda resultante de uma falha ou de um inadequado processo interno de controle podendo ele ser gerado pelo homem, pelo sistema ou por eventos externos.

Soma-se à definição de risco operacional, o risco legal e regulatório associado à inadequação ou ineficiência dos contratos firmados pela instituição; à inobservância da regulamentação em vigor no tocante aos produtos/serviços oferecidos pela instituição; bem como às indenizações por danos a terceiros decorrentes de atividades desenvolvidas pela instituição e às sanções advindas de descumprimento de dispositivos legais.

Já a continuidade de negócios pode ser definida como o conjunto de ações estratégicas que, ao serem realizadas, objetivam assegurar a continuidade das operações em eventuais indisponibilidades prolongadas ou totais de recursos essenciais (dados, sistemas da informação, equipamentos e instalações).

A obrigatoriedade da elaboração de um Plano de Risco Operacional e Continuidade de Negócios foi introduzida pelo Sistema Financeiro Nacional, inicialmente restrito às áreas de TI, através da Circular nº 2.892 do Banco Central do Brasil, a qual visava o estabelecimento de ações destinadas a assegurar a continuidade operacional das instituições financeiras contra eventuais emergências capazes de afetar os sistemas eletrônicos na passagem do ano 1999 para o 2000.

Com a Resolução nº 3.380 do Banco Central do Brasil, de 29 de junho de 2006, o Sistema Financeiro Nacional ressaltou a importância de se mitigar os riscos operacionais e organizar um plano de contingência, contendo as estratégias a serem adotadas pelas instituições financeiras para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional.

Por fim, a Resolução CVM nº 21, Item 10.4, Anexo E, indica como obrigatória a elaboração de um plano de contingência, continuidade de negócios e recuperação de desastres adotados. Tal obrigação é reforçada pela autorregulação, conforme Seção IV, do Capítulo II, das Regras e Procedimentos de Deveres Básicos da ANBIMA.

03. ABRANGÊNCIA / ÁREAS ENVOLVIDAS:

- Compliance;
- Risco; e
- TI.

04. RESPONSABILIDADES:

04.01. Responsáveis pela execução das atribuições da Política:

É de responsabilidade das áreas de TI a execução primordial das atividades desta Política. Outras áreas poderão colaborar, conforme definição abaixo.

04.02. Responsáveis pela manutenção da Política:

É responsabilidade das áreas de Compliance, Risco e TI assegurar, através de monitoramento e testes periódicos, a conformidade das atividades com esta Política.

05. DIRETRIZES:

06. Eventos de Risco Operacional

06.01. Fraudes Internas e Externas

Caracterizam-se como fraude os atos intencionais que visam enganar e/ou burlar leis, regulamentações e Políticas da instituição.

As Gestoras se resguardam com relação a possíveis fraudes através de uma cultura forte e controles internos bem definidos. A cultura da empresa é transmitida através do Código de Conduta e Ética, estrutura hierárquica, padrões de desempenho, treinamentos e estilo de liderança; todavia, o não cumprimento das diretrizes do Código de Conduta e Ética pode resultar em advertências ou punições.

Já os controles se baseiam nas análises dos Colaboradores realizadas anualmente e nas análises *due diligence* sobre parceiros e terceiros contratados. Considerando o risco de imagem, as Gestoras se associam apenas com pessoas físicas e jurídicas que foram previamente analisadas e possuem integridade.

06.02. Demandas Trabalhistas e Segurança no Local de Trabalho

As Gestoras envidam seus melhores esforços para a identificação e tratamento tempestivo de erros operacionais referentes a demandas trabalhistas e segurança no local de trabalho de seus Colaboradores.

O departamento de Recursos Humanos e o departamento Jurídico das Gestoras são responsáveis pela verificação, adequação e cumprimento das normas trabalhistas, principalmente no tocante à

segurança no ambiente de trabalho. Sendo assim, identificadas falhas relativas a qualquer aspecto trabalhista, especialmente de segurança do trabalho, o departamento de Recursos Humanos comunicará à área de Compliance para, em conjunto, executem as providências cabíveis para, se possível, evitar a concretização do risco e sanar eventuais consequências da referida falha.

06.03. Práticas Inadequadas Relativas a Clientes, Produtos e Serviços

Todas as obrigações relativas a clientes, produtos e serviços são executados pelo administrador fiduciário dos fundos. Todavia, as Gestoras possuem uma área de Controle de Fundos que monitora e replica as principais funções do administrador relacionadas a clientes, produtos e serviços.

06.04. Danos a Ativos Físicos Próprios

Os ativos físicos dos quais dependem as funções críticas do negócio contam com cópia de segurança e/ou substituto imediato, ou seja, ainda que em situações mapeadas como catastróficas, nas quais todos os ativos físicos podem ser perdidos, as Gestoras possuem contingências para manter os processos de negócio em andamento.

06.05. Aqueles que acarretam a Interrupção das Atividades da Instituição

Os eventos de Risco Operacional que podem acarretar a interrupção das atividades são analisados no item 08 desta Política, chamado “Identificação de Cenários”, e os planos de contingência estão descritos no item 09 desta Política, “Sistemas de Contingência”.

06.06. Falhas em Sistemas de Tecnologia da Informação

Dentre as deficiências de sistemas mais comuns identificamos as seguintes: tecnologia insuficiente ou obsoleta ao negócio; o uso não autorizado ou inadequado da tecnologia; falhas nos equipamentos; hardware inadequado; invasões por hackers; falha na proteção da rede; vírus de computadores; falhas de programação, etc.

Todas essas deficiências identificadas são alvo de consideração e as melhores contingências/soluções são aplicadas pelo TI. Algumas das soluções para as deficiências citadas acima são descritas mais detalhadamente no item 09, “Sistemas de Contingência”.

06.07. Falhas na Execução, Cumprimento de Prazos e Gerenciamento das Atividades

A falha humana, apesar de inevitável, é mitigada mediante a adoção de manuais e políticas internas visando a orientação da conduta dos Colaboradores no desempenho das atividades.

A execução de atividades relacionadas aos fundos conduzidas pelas Gestoras, conforme o que lhe é cabível, é monitorada pela equipe de Controle das Gestoras, com objetivo de prevenir, identificar ou remediar deficiências nas transações que possam afetar clientes ou contrapartes.

06.08. Risco Legal e Regulatório

O risco legal e regulatório está associado à inadequação ou ineficiência dos contratos firmados pela instituição, assim como à inobservância da regulamentação em vigor no que se refere aos produtos/serviços oferecidos pelas Gestoras, bem como às indenizações por danos a terceiros decorrentes de atividades desenvolvidas pelas Gestoras e às sanções advindas de descumprimento de dispositivos legais.

As Gestoras contam com um departamento Jurídico e um departamento de Compliance, além de assessoria jurídica externa, quando necessário.

06.09. Risco oriundo das Corretoras

Com relação ao risco operacional oriundo das corretoras de valores mobiliários utilizadas pelas Gestoras como plataformas para a atividade de gestão das carteiras dos fundos, destaca que as Gestoras operam com mais de uma corretora, de modo que no caso de contingência com uma delas, as operações poderão ser realizadas através das demais com as quais as Gestoras possuem contrato. Assim, em caso de tal contingência, a equipe de Risco é responsável pelo acompanhamento do caso.

A divisão de ordens entre as corretoras visa o aproveitamento da expertise de cada uma delas, de acordo com as características das operações negociadas, incluindo parâmetros de risco e volume, e a sinergia entre as equipes.

Operações realizadas no mercado de balcão são cotadas em mais de uma corretora. Tais procedimentos são complementados com o disposto na Política de Rateio e Divisão de Ordens.

07. Planejamento Estratégico de Continuidade

A presente Política tem a finalidade de demonstrar, em nível estratégico, um programa de continuidade operacional e integridade das informações.

Em suma, a estratégia de Continuidade de Negócios das Gestoras consiste em 2 (dois) pontos, sendo o primeiro garantir que os Colaboradores possam realizar seus processos independentemente de estarem fisicamente nas Gestoras, através de acesso remoto ao computador do escritório e, consequentemente, a todo o seu conteúdo.

Já o segundo volta-se para manter o máximo de sistemas de contenção que preservem a continuidade dos processos em situações de inoperância de recursos técnicos, por exemplo, *no-breaks* e geradores de energia que mantenham o funcionamento das máquinas em caso de queda de luz.

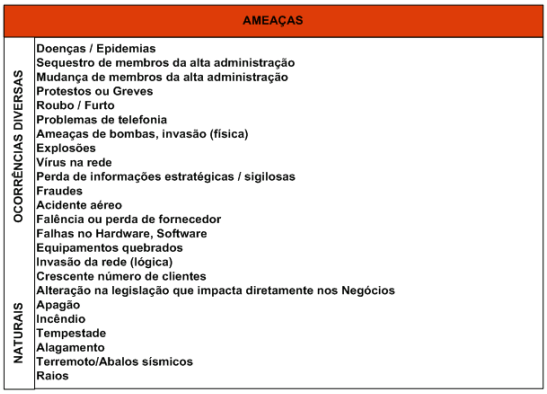
Para o bom funcionamento da estratégia, é necessário que na ocorrência de indisponibilidade de recursos, as pessoas diretamente envolvidas possuam total conhecimento das funções e responsabilidades estabelecidas para, desse modo, minimizar ao máximo o impacto nas Gestoras.

08. Análise de Riscos Potenciais

08.01. Identificação de Cenários

A identificação de cenários é essencial, pois, através deste processo são mapeados os cenários credíveis que podem afetar as Gestoras de forma parcial ou total. Nesta análise são consideradas ameaças que impactam os processos de negócios ou recursos (instalações, equipamentos, sistemas/*softwares*) relacionados.

Quedas de energia elétrica, falhas de *hardware*, vírus na rede são exemplos de problemas operacionais que causam risco aos processos do negócio. As possíveis ameaças podem ser divididas de maneira geral em ocorrências diversas e naturais, conforme listagem abaixo:



Com base nessas possibilidades, as ameaças são classificadas em 3 (três) grandes grupos listando as contingências existentes e os pontos descobertos pelas contingências, sendo que os grupos de ameaças estão segregados pelo nível de severidade e pelo grau de probabilidade do cenário.

08.01.01. Cenário Regular

No cenário regular estão inclusas as ameaças de menor gravidade e maior frequência como, por exemplo, problemas de telefonia, equipamentos quebrados, queda de luz, dentre outros. Neste cenário, o escritório existe e todos os Colaboradores estão presentes.

Ameaças	Problemas de telefonia; Vírus na rede; Perda de informações estratégicas / Sigilosas; Falência ou perda de fornecedor; Equipamentos Quebrados; Roubo / Furto; Falhas em *Hardware* ou *Software*; Queda de Luz; Indisponibilidade de um fornecedor de serviço essencial, tal como uma corretora de valores mobiliários; Impedimento superior a 30 (trinta) dias dos Diretores regulatórios, eleitos para fins de cumprimento dos requisitos da Resolução CVM 21.
Contingências	Antivírus; *Back Up*; *Nobreaks*; Geradores; *Data Center*; Servidor de arquivos duplicado; Servidor de banco de dados duplicado; Duas opções de canal para saída de internet; Internet *Wireless*; Para cada três equipamentos de hardware existe um em contingência; Manutenção de contrato com mais de um fornecer de serviço essencial para a mesma atividade; Capacitação da equipe e manutenção de profissional backup para todas as áreas regulatórias.
Pontos Descobertos	Nenhum.

08.01.02. Cenário Crítico

No cenário crítico estão inclusas as ameaças de média gravidade e de possibilidade factível como, por exemplo, alagamento, protestos, pandemias e greves no derredor, além de qualquer outra situação que impossibilite que os Colaboradores tenham acesso ao escritório. Neste cenário, o escritório existe, entretanto, os Colaboradores não podem estar presentes.

Ameaças	Pandemias/epidemias; Protestos ou Greves; Ameaças de bombas; Invasão física; Tempestades; Alagamento; Raios.
Contingência	Acesso remoto para todos os Colaboradores; Sistemas de Informação (ex: *Bloomberg Anywhere*); E-mail; Terminal Service para acesso remoto aos servidores de arquivo e sistemas.
Pontos Descobertos	Nenhum.

08.01.03. Cenário Catastrófico

No cenário catastrófico estão inclusas as ameaças de alta gravidade e de improvável possibilidade de ocorrer como, por exemplo, incêndio total, explosão ou terremoto. Em ocorrências como estas, o escritório não existe, sendo assim, a principal estratégia é um acesso remoto de contingência que não depende da rede do escritório para funcionar; este acesso remoto se conecta diretamente à rede corporativa que foi replicada no *Data Center* externo.

Ameaças	Incêndio; Explosões; Terremoto/Abalos Sísmicos; Acidente Aéreo; Desabamento do Prédio.
Contingência	Sistemas de Informação (ex: *Bloomberg Anywhere*); E-mail; Terminal Service para acesso remoto aos servidores de arquivo e sistemas.
Pontos Descobertos	Necessidade de aprovação de acesso remoto aos servidores que replicam a rede do escritório externamente para todos os Colaboradores, tendo em vista que hoje tal acesso é permitido apenas para os Colaboradores em cargo de chefia e considerados essenciais para continuidade imediata das atividades em caso de contingência.

08.01.04. Cenário COVID-19

Em relação ao cenário COVID-19, as Gestoras tomaram diversas ações relacionadas a adaptação ao cenário, dentre elas:

- O envio de comunicados com informativos de atitudes de prevenção;
- A disponibilização do trabalho remoto para todos os Colaboradores;
- Intensificação da limpeza no escritório;

- Oferecimento de vacinas de gripe a todos os Colaboradores;
- Oferecimento de testes para o COVID-19 aos Colaboradores que por alguma razão ainda precisavam frequentar o escritório;
- A determinação do uso de máscara no escritório durante o período de calamidade da COVID-19;
- Ajuda de custo relacionado ao trabalho em *Home Office*; e
- Elaboração de uma política temporária com todas as ações citadas e outras.

08.02. Análise de Criticidade:

Neste item específico, a Política analisou a criticidade dos processos de negócios das Gestoras levando em consideração os seguintes parâmetros:

Criticidade dos Processos	
Dispensável	Consegue-se realizar as atividades normais sem o recurso
Substituível	Consegue-se substituir facilmente o recurso por outro
Importante	O recurso é importante e torna-se complicado a realização das atividades com sua ausência
Essencial	Consegue-se dificilmente realizar as atividades sem o recurso, dispêndio de muito tempo
Vital	O recurso é essencial para a realização das atividades e sem ele as rotinas não acontecem

Baseado na análise de criticidade, o presente plano de continuidade enfatiza os processos com nível de criticidade classificado como "Vital", ou seja, aqueles considerados indispensáveis de serem realizados para o bom funcionamento do negócio.

Área	Processos Críticos	Nível de Criticidade	Principais Contingências
Compliance	Acesso a documentos disponíveis na rede corporativa	Vital	Acesso Remoto*
Controle Fundos	Batimento de custódia Batimento de carteiras Enquadramento dos Fundos Especificações de Carteira Conferência de caixa dos fundos Envio de informações para administradores/custodiantes Gestão de Colateral	Vital	Acesso Remoto * (incluindo LSEG Messenger) E-mail Web *Bloomberg Anywhere* (BBG com *Disaster Recovery*)
Vendas Institucional	Rotinas de Relatório ou posição Boleta de Resgate ou aplicação	Vital	Acesso Remoto *(incluindo acesso ao Custódia Bradesco) E-mail Web

Macroeconomia	Previsão de cenários macroeconômicos internacionais e nacionais	Vital	Acesso Remoto* (incluindo acesso a Macrobond) *Bloomberg Anywhere* (BBG com *Disaster Recovery*)
Câmbio	Operar no mercado de câmbio	Vital	Acesso Remoto* *Bloomberg Anywhere* (BBG com *Disaster Recovery*) E-mail Web
Análise de Mercado	Análise de setores e empresas	Vital	Acesso Remoto * (incluindo Broadcast) *Bloomberg Anywhere* (BBG com *Disaster Recovery*) E-mail Web
Preços	Validação dos preços dos ativos Informação do delta das Opções para auxiliar o Controle no enquadramento dos fundos	Vital	Acesso Remoto * *Bloomberg Anywhere* (BBG com *Disaster Recovery*) E-mail Web
Fundos de Mandato	Operação de Hedge	Vital	Acesso Remoto* E-mail Web Bloomberg Anywhere (BBG com *Disaster Recovery*)
Comunicação	Publicação de lâminas, informativos, cartas do Gestor e anúncios de imprensa Remediar matérias negativas sobre as Gestoras	Vital	Acesso Remoto*
Risco de Mercado e liquidez	Acompanhamento de risco de mercado Acompanhamento de posições das mesas de operações	Vital	Acesso Remoto* *Bloomberg Anywhere* (BBG com *Disaster Recovery*) E-mail Web
Sustentabilidade	Acesso a documentos disponíveis na rede corporativa	Vital	Acesso Remoto*
Mesa Renda Fixa	Operações renda fixa	Vital	Acesso Remoto* *Bloomberg Anywhere* (BBG com *Disaster Recovery*) E-mail Web
Jurídico	Acesso a documentos disponíveis na rede corporativa	Vital	Acesso Remoto*
TI	Manutenção de infraestrutura e de sistemas, atendimento a demandas compulsórias, suporte a usuários e monitoramento e controle da segurança do ambiente	Vital	Acesso Remoto*

* O acesso remoto inclui a disponibilidade dos arquivos e sistemas internos.

09. Sistemas de Contingência

As informações e processos dos quais depende a continuidade dos negócios das Gestoras deverão contar com sistema de contingência em ambiente de produção, *backup* e/ou cópias de segurança.

09.01. Infraestrutura de TI

As Gestoras possuem uma área de TI segregada, a qual, entre outras atribuições, é responsável por dar suporte aos processos operacionais e manter os sistemas que assegurem a integridade das informações e processos da instituição.

09.02. Data Center

As Gestoras contam com um *Data Center* externo que armazena todos os servidores institucionais. Este serviço é considerado de alta disponibilidade porque o prestador de serviço segue as melhores práticas de governança na área.

Adicionalmente, o *Data Center* possui seus próprios sistemas de contingência e medidas de segurança de dados como, por exemplo, sistemas de contenção de incêndio, geradores de grande porte, sala cofre, câmeras, controle de acesso, vigilância, dentre outros.

Além disso, as Gestoras contam com servidores localizados na própria sede com acesso restrito a pessoas autorizadas, monitorados por câmeras, refrigeração controlada, *no-breaks* e grupo de geradores.

09.03. Backup

As cópias de segurança das informações dos servidores de produção são armazenadas externamente em fornecedor especializado – guarda externa - que segue as melhores práticas de mercado para garantir a segurança e confiabilidade das informações.

São realizadas 2 (duas) frequências diferentes de *Backup*, sendo elas o *Backup* Diário no qual fazemos um *backup* completo, no qual é guardada uma cópia dos arquivos criados ou alterados desde o último *backup* diário, sendo que essa frequência de *backup* é retida por sessenta dias em nuvem.
É também realizado um *backup* mensal completo de todos os servidores, sendo que essa frequência de *backup* é retida por cinco anos em nuvem.

Considerando a rotina de *backup* descrita acima, na impossibilidade de acesso aos dados que se encontram no *Data Center* externo e interno pode-se recuperar os arquivos de *backup* que estão armazenados na guarda externa.

09.04. Alta disponibilidade do Ambiente Tecnológico

Todos os servidores presentes no *Data Center* externo estão sob uma plataforma virtualizada em ambiente físico de alta disponibilidade, este ambiente conta com as melhores soluções de virtualização e fornecedores de equipamentos físicos.

O ambiente físico conta com redundância de processamento e armazenamento. Em caso de falha de algum equipamento físico, o próprio gerenciador interno do ambiente garante que não haverá interrupção dos serviços ali presentes.

Ademais, contamos com a replicação dos serviços mais críticos no data center local a fim de melhorar a performance e trazer mais segurança, conforto e confiabilidade ao ambiente tecnológico das Gestoras.

09.05. Queda de Energia / Nobreaks

As Gestoras contam com *no-break*s em todos os equipamentos e geradores para se precaver de situações de falta de energia.

A principal finalidade dos *no-breaks* é sustentar os equipamentos por tempo suficiente até o acionamento do gerador, tendo em vista que os *no-breaks* possuem módulos de potência que se sobrepõem em situação de defeito. Esta contingência é testada periodicamente pela área de TI.

As Gestoras possuem, inclusive, geradores que ficam sob gestão do condomínio e possuem capacidade suficiente para gerar energia a todos os andares do edifício.

09.06. Internet

O canal principal de internet tem a possibilidade de funcionar através de quatro operadoras diferentes e com meios físicos distintos, considerado, assim, uma internet de alta disponibilidade.

09.07. E-mail

O serviço de e-mail conta com *data centers* espalhados pelo mundo, em continentes distintos, sendo todos os dados existentes no *data center* primário, instantaneamente, replicados em todos os demais e o dado, inclusive, replicado dentro do próprio *data center*, a fim de garantir altíssima disponibilidade.

Ademais, os *data centers* têm duplicação e armazenagem de dados entre localidades distintas e o serviço pode ser acessado em dispositivos móveis e através de aplicativo web.

09.08. Telefonia

A central telefônica e os aparelhos individuais possuem redundância física contando com um módulo passivo acionado automaticamente quando o primário se encontra indisponível.

09.09. Bloomberg Anywhere

Trabalhamos com 2 (dois) links privados na Bloomberg e uma terceira alternativa, a qual poderá ser utilizada através de um link na internet; ademais, enquanto contingência possuímos a Bloomberg *Anywhere,* que pode ser acessada de qualquer localidade pelos operadores.

Outros serviços de informação como Agência Estado, Reuters e Valor Pro podem ser acessados diretamente pela internet com o uso de *login* e senha sem a necessidade de contingência e dependendo apenas do serviço de internet.

Dessa forma, partindo do princípio de que a internet possui alta disponibilidade, devido às contingências citadas anteriormente, pode-se concluir que o acesso a esses materiais possui alta disponibilidade.

09.010. Antivírus

Todas as máquinas possuem antivírus gerenciados de forma unificada e centralizada.

A console central se mantém atualizada e distribui todas as novas atualizações às estações de trabalho mantendo o parque sempre atualizado.

09.011. Acesso Remoto

O acesso remoto é uma ferramenta que possibilita o acesso dos Colaboradores à rede das Gestoras a fim de que possam, dessa forma, realizar suas rotinas fora do escritório.

O acesso remoto deve ser utilizado tanto para permitir o trabalho remoto (*home office*) quanto para garantir a continuidade dos processos em casos de incidentes de causas naturais ou no ambiente físico do prédio, no qual a estrutura de rede permaneça intacta.

Essa ferramenta é testada continuamente, porque, todos aqueles que possuem o acesso remoto frequentemente o utilizam. Além de ter sido a principal contingência utilizada no cenário de COVID-19. Para a conexão do acesso remoto será exigida a utilização de múltiplos fatores de autenticação e a instalação do aplicativo de VPN.

09.012. Acesso Remoto Contingência

As Gestoras contam com um terminal de acesso remoto para contingência, um recurso que não depende da integridade do *data center* local para funcionar, habilitado em cenários críticos ou catastróficos.

Este terminal possui acesso direto à rede corporativa no *Data Center* externo, sendo assim, os Colaboradores, aprovados pela Diretoria, de todas as áreas com necessidade de uso dos dados internos possuem acesso a este terminal com todos os seus respectivos aplicativos, acessos e dados para a eventual ocorrência do cenário classificado como catastrófico.

09.013. Contingência Gestor de Recursos

As Gestoras possuem Gestor capacitado, e autorizado pela CVM, isto é, com registro de administrador de carteiras de valores mobiliários de pessoa natural, e apto para assumir a posição de Gestor de recursos em caso de impedimento superior a 30 (trinta) dias do Gestor titular.

09.014. Manual Operacional de Acesso ao Servidor de Contingência

É disponibilizado na rede corporativa e orientado aos Colaboradores a ter, com fácil acesso, o Manual Operacional de Acesso ao Servidor de Contingência, sendo esta contingência voltada para o cenário de indisponibilidade total do escritório.

010. Processo de Ativação

Uma emergência é configurada sempre que houver o impedimento à execução de qualquer atividade essencial das Gestoras, ou processo do qual dependa uma atividade essencial, por período igual ou superior a 48 (quarenta e oito) horas, ou com tempo de resposta igual ou superior a 48 (quarenta e oito) horas. Além disso, qualquer situação na qual a não execução imediata de uma atividade acarrete prejuízos às atividades das Gestoras, será considerada uma emergência.

011. Validação/Testes

Os testes buscam periodicamente validar os planos de contingência conforme as mudanças no contexto de negócios das Gestoras.

Todas as contingências citadas acima são testadas periodicamente, pela área de TI, visando atestar a efetividade das estratégias definidas e dos recursos a serem disponibilizados. As evidências são registradas e arquivadas a fim de manter um histórico de ocorrências.

012. ANEXO

N/A

013. CONSIDERAÇÕES FINAIS:

Este documento é de uso estritamente interno não devendo ser disponibilizado a terceiros sem a prévia aprovação do Compliance.

014. LEGISLAÇÃO / REGULAÇÃO RELACIONADA:

- Resolução nº 4.557 do Banco Central do Brasil;
- Resolução CVM nº 21; e
- Código ANBIMA de Administração e Gestão de Recursos de Terceiros.

015. REFERÊNCIA INTERNA:

- Política de Segurança da Informação; e
- Manual de Acesso à VPN.

016. BIBLIOGRAFIA

N/A

017. GLOSÁRIO

N/A