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 Política de Risco Operacional e Continuidade de Negócios das Gestoras 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 os mesmos seguir as diretrizes aqui apresentadas.

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 que associa-se 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 2.892do 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 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 21, Item 10.4, Anexo E, indica como obrigatória a elaboração de um plano de contingência.

03. ABRANGÊNCIA / ÁREAS ENVOLVIDAS:

- Compliance
- TI

04. RESPONSABILIDADES:

04.01. Responsáveis pela execução das atribuições da Política:

É de responsabilidade das áreas de TI a execução das atividades desta Política.

04.02. Responsáveis pela manutenção da Política:

É responsabilidade das áreas de Compliance 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 baseiam-se nas análises dos Colaboradores realizadas anualmente e nas análises *due diligence* sobre parceiros e terceiros contratados. Ressalta-se que, considerando o risco de imagem, as Gestoras se associam apenas com pessoas físicas e jurídicas que analisou e verificou possuírem caráter integro.

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, executarem 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, destaca-se que as Gestoras possuem uma área de Controle 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 sanados 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 nossa consideração e as melhores contingências/soluções são aplicadas pelo departamento de TI. Destaca-se que 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 execução de atividades relacionadas aos fundos conduzidos pelas Gestoras é gerenciada pelo administrador fiduciário no que lhe é cabível. Entretanto, todos os processos são monitorados 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

O risco legal está associado à inadequação ou ineficiência dos contratos firmados pela instituição, assim como da inobservância da regulamentação em vigor no que se refere 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.

As Gestoras contam com assessoria jurídica interna e consultorias externas, quando necessário.

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 na instituição, 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 na Instituição.

08. Análise de Riscos Potenciais

08.01. Identificação de Cenários

A identificação de cenários é essencial, pois, através deste processo mapeamos os cenários credíveis que podem afetar as Gestoras de forma parcial ou total. Nesta análise consideramos 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:

AMEAÇAS	
OCORRÊNCIAS DIVERSAS	Doenças / Epidemias Sequestro de membros da alta administração Mudança de membros da alta administração Protestos ou Greves Roubo / Furto Problemas de telefonia Ameaças de bombas, invasão (física) Explosões Vírus na rede Perda de informações estratégicas / sigilosas Fraudes Acidente aéreo Falência ou perda de fornecedor Falhas no Hardware, Software Equipamentos quebrados Invasão da rede (lógica) Crescente número de clientes Alteração na legislação que impacta diretamente nos Negócios
NATURAIS	Apagão Incêndio Tempestade Alagamento Terremoto/Abalos sísmicos Raios

Com base nessas possibilidades, classificamos as ameaças 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.
Contingências	Duas operadoras de telefonia; 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.
Pontos Descoberto	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 (aprovado pontualmente para esse cenário); 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 Prédios.
Contingência	Sistemas de Informação (ex: *Bloomberg Anywhere*); E-mail; Terminal Service para acesso remoto aos servidores de arquivo e sistemas.

Pontos Descobertos	O acesso remoto aos servidores que replicam a rede do escritório externamente não é aprovado para todos os Colaboradores.

08.01.04. Cenário COVID-19

Pontualmente em relação ao cenário COVID-19, as Gestoras tomaram diversas ações relacionadas a adaptação ao cenário, dentre elas destaca-se:

- 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;
- Ajuda de custo relacionado ao trabalho em Home Office;
- 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-se em consideração os seguintes parâmetros abaixo:

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 * E-mail Web *Bloomberg Anywhere* (BBG com *Disaster Recovery*) Telefone Virtual
Vendas Institucional	Rotinas de Relatório ou posição Boleta de Resgate ou aplicação	Vital	Acesso Remoto *(incluindo acesso ao Custódia Bradesco) E-mail Web Telefone Virtual
Macroeconomia	Previsão de cenários macroeconômicos internacionais e nacionais	Vital	Acesso Remoto* (incluindo acesso ao ECOWIN) *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 e Reuters) *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 Quantitativos	Gestão de Fundos Quantitativos	Vital	Acesso Remoto* (incluindo acesso ao Redi+) *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
ESG	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* Telefone Virtual

* *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, seis sistemas de contenção de incêndio, cinco geradores de grande porte, sala cofre, câmeras, controle de acesso, vigilância, dentre outros.

Além disso, as Gestoras contam com servidores localizados na própria empresa 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 3 (três) frequências diferentes de *Backup*, sendo elas o *Backup* Diário no qual fazemos um *backup* incremental e, dessa forma, guardamos uma cópia dos arquivos criados ou alterados desde o último backup diário., sendo esta frequência de *backup* retida por trinta dias em disco; o *Backup* Semanal no qual realizamos um *backup* completo de todos os servidores, em que a frequência de *backup* é retida por trinta dias em disco. E, por último, o *Backup* Mensal no qual realizamos um *backup* completo de todos os servidores, sendo a frequência de *backup* retida por 5 (cinco) anos em fita magnética criptografada.

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. Neste caso, o pior cenário seria poder contar apenas com o arquivo mensal de *backup* salvo há 1 (um) mês atrás.

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 datacenter 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. Frisa-se que 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 treze operadoras diferentes, considerado, assim, uma internet de alta disponibilidade.

Além disso, temos uma internet de contingência com o mesmo tamanho de banda do canal principal. Este canal é utilizado em produção pelos Colaboradores mensalmente para garantir seu bom funcionamento.
Outrossim, temos uma terceira opção de saída de internet utilizada para rede *wireless* interna da instituição que é independente das 2 (duas) outras citadas anteriormente, essa terceira opção pode ser utilizada como mais uma "saída" em casos de contingência.

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 datacenter 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 encontra-se indisponível.

Ademais, possuímos mais de um canal de comunicação externa, com operadoras distintas, tanto para entrada quanto para saída de ligações. Importante ressaltar que todos os canais são continuamente testados pelos Colaboradores, pois, são utilizados em produção ativamente.

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

Possuímos antivírus em todas as máquinas gerenciados de forma unificada e centralizada.

A console central se mantém atualizado 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. Frisa-se que para conexão do acesso remoto será exigida a utilização de múltiplos fatores de autenticação e a instalação do aplicativo FortiClient VPN.

09.012. ***Acesso Remoto Contingência***

Possuímos um terminal de acesso remoto para contingência, um recurso que não depende da integridade do datacenter local para funcionar. 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 diretor 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 ausência do diretor titular.

09.014. Manual Operacional de Acesso ao Servidor de Contingência

Disponibilizamos na rede corporativa e orientamos os 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. 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.

011. ANEXO
N/A

012. CONSIDERAÇÕES FINAIS:

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

013. LEGISLAÇÃO / REGULAÇÃO RELACIONADA:

- Resolução n° 3.380 – Banco Central do Brasil;
- Circular n° 3.718 – Banco Central do Brasil;
- Resolução 21 - CVM;
- Código de Administração e Gestão de Recursos de Terceiros - ANBIMA.

014. REFERÊNCIA INTERNA:

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

15. BIBLIOGRAFIA
N/A

16. GLOSÁRIO
N/A