PERSEVERA
ASSET MANAGEMENT

Política de Gestão de Risco

Data de vigência: Dez/19
Data da última revisão: Dez/19

POLÍTICA DE GERENCIAMENTO DE RISCOS

A Persevera tem por objetivo oferecer aos cotistas de seus fundos retorno consistentemente superior ao benchmark no médio/longo prazo e entende que isso só é possível através de uma filosofia de investimento diferenciada e com atividades de gerenciamento e controle de risco também diferenciados e diretamente relacionados a essa filosofia de investimento. Nesse sentido, o reconhecimento, a mensuração, a análise, o monitoramento, o gerenciamento e o controle de riscos não são considerados atividades segregadas do processo de investimentos – ou apenas 'consequência' dele – mas sim parte fundamental e totalmente integrada ao mesmo. A cultura de risco da Persevera está, portanto, diretamente relacionada à sua filosofia de investimento.

A Persevera entende e considera que o caminho para o sucesso de investimentos de longo prazo tem muito mais relação com controle de risco do que com 'agressividade' dos investimentos. Os grandes gestores destacaram-se – a ainda se destacam – não só pela sua capacidade de gerar retornos consistentes no longo prazo, mas principalmente pela sua capacidade em gerenciar e controlar os riscos dos seus investimentos, tanto em situações de normalidade quanto em situações de ruptura [1].

Apresentaremos nesta parte do manual os aspectos gerais da Gestão de Risco bem como os seus fundamentos e principais controles[2].

Entende-se por Gerenciamento de Risco a identificação, mensuração, monitoramento e comunicação de todos os riscos. Já o Controle de Risco procura limitar o tamanho e a probabilidade de perdas absolutas (perdas não são necessariamente indicação de falhas no gerenciamento de risco. Uma gestão de risco eficiente deve reconhecer que grandes perdas são possíveis e desenvolver planos de contingência que lidem com tais perdas se as mesmas ocorrerem).

1. ASPECTOS GERAIS

(i) Objetivos

Esta Política de Gestão de Risco ("Política de Risco") tem por objetivo descrever a estrutura e metodologia utilizadas pela Gestora na gestão de risco dos Fundos de Investimento cujas carteiras encontram-se sob sua gestão. A estrutura funciona de modo que, qualquer evento que possa interferir negativamente no negócio, possa ser identificado e tratado de forma adequada, rápida e segura.

O gerenciamento de riscos da Gestora parte da premissa de que a assunção de riscos é característica intrínseca dos investimentos nos mercados financeiros e de capitais. Desta forma, a gestão de riscos realizada pela Gestora tem por princípio não sua simples eliminação, mas sim o acompanhamento e avaliação, caso a caso, dos riscos aos quais cada carteira estará exposta e da definição de estratégias e providências para a mitigação de tais riscos, conforme definição do perfil do cliente ou da política de investimento.

(ii) Governança

1. Estrutura

A área de risco da Gestora é formada pelo Comitê de Risco e pela Diretoria de Risco.

2. Comitê de Risco

Responsabilidades: O Comitê de Risco é o órgão da Gestora incumbido de:

a. Dar parâmetros gerais, orientar e aprovar a política de risco;
b. Estabelecer objetivos e metas para a área de risco; e
c. Avaliar resultados e performance da área de risco, solicitar modificações e correções.

---

[1] MARKS, Howard. *The most important thing illuminated – Uncommon sense for the thoughtful investor* – Columbia University Press, 2013 (livre tradução efetuada pela Persevera, págs 71 e 78)

[2] Sugerimos como leitura complementar o documento "Persevera: uma visão de risco diferenciada" disponível no website www.persevera.com.br

Composição: O Comitê de Risco é formado pelo Diretor de Risco e pelos sócios da Persevera membros do comitê executivo, todos com direito a voto, sendo certo que o voto decisório será sempre exclusivamente do Diretor de Risco. Dessa forma, o Comitê reunir-se-á validamente com a presença do Diretor de Risco e da maioria dos seus membros (serão também considerados presentes os membros que participarem por meio de tele ou videoconferência).

O Comitê poderá convidar para participar de suas reuniões colaboradores internos e externos que detenham informações relevantes ou cujos assuntos constem da pauta de discussão e sejam pertinentes à sua área de atuação.

Reuniões: O Comitê de Risco se reúne de forma ordinária, formalmente, trimestralmente e poderá ser convocado extraordinariamente, sempre que necessário.
As convocações ocorrerão com o simultâneo encaminhamento da pauta de assuntos, com antecedência mínima de 3 (três) dias úteis da data da reunião, com exceção de assunto que exija apreciação urgente.

Decisões: As decisões do Comitê de Risco deverão ter o voto favorável, no mínimo, do Diretor de Risco. As decisões do Comitê em matéria de gestão de risco deverão ser tomadas preferencialmente de forma colegiada, sendo sempre garantido exclusivamente ao Diretor de Risco o voto de qualidade e a palavra final em todas as votações. Em relação a medidas corretivas e medidas emergenciais, o Diretor de Risco poderá decidir monocraticamente. As decisões do Comitê de Risco serão formalizadas em ata.

3. Diretoria de Risco

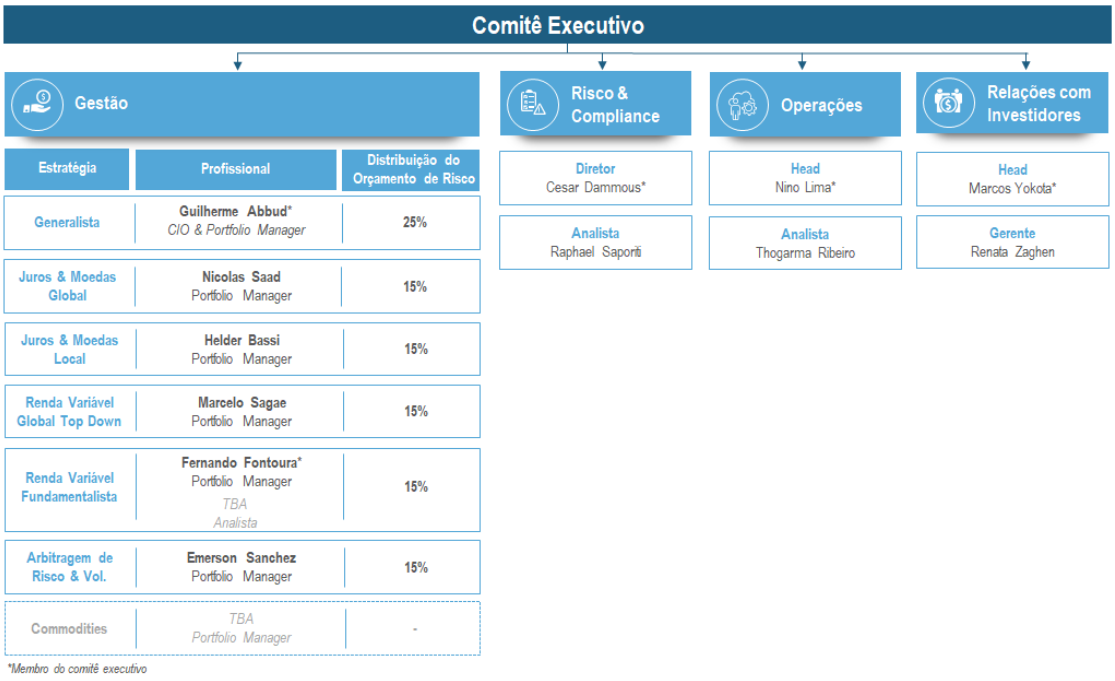
Responsabilidades: A Diretoria de Risco ("Diretoria de Risco") é responsável pela definição e execução das práticas de gestão de riscos de performance, de liquidez, de crédito, e operacionais descritas neste documento, assim como pela qualidade do processo e metodologia, bem como a guarda dos documentos que contenham as justificativas das decisões tomadas.

Funções: A Diretoria de Risco estará incumbida de:

a. Implementar a Política, planejando a execução e executando os procedimentos definidos pelo Comitê de Risco;
b. Redigir os manuais, procedimentos e regras de risco;
c. Apontar desenquadramentos e aplicar os procedimentos definidos na Política aos casos fáticos;
d. Produzir relatórios de risco e levá-los ao Gestor; e
e. Auxiliar o Comitê de Risco em qualquer questão atinente a sua área.

Responsável: o Sr. Cesar Dammous, Diretor de Risco da Persevera.

4. Organograma



(obs.: a entrada de novos gestores poderá alterar o orçamento de risco dos books acima assinalados, mas a estrutura e reporte da área de risco manter-se-á inalterada e independente)

(iii) Garantia de Independência

O Comitê de Risco e a Diretoria de Risco são independentes das outras áreas da empresa e poderão exercer seus poderes em relação a qualquer Colaborador.

2. FUNDAMENTOS DA POLÍTICA DE GESTÃO DE RISCO

(i) Conceitos gerais

Para efeitos desta Política, define-se:

Risco de mercado: possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições ativas e passivas detidas pela Gestora.

Risco de Contraparte e Crédito: define-se como a possibilidade de perdas resultantes pelo não recebimento de valores contratados junto a contrapartes em decorrência da incapacidade econômico-financeira destas.

Risco de Liquidez: assume duas formas, o risco de liquidez de mercado e o risco de liquidez de fluxo de caixa (*funding*). O primeiro é a possibilidade de perda decorrente da incapacidade de realizar uma transação em tempo razoável e sem perda significativa de valor. O segundo está associado à possibilidade de falta de recursos para honrar os compromissos assumidos em função do descasamento entre os ativos e passivos.

Risco operacional: possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

(ii) Precificação

Em relação à precificação dos ativos, a Gestora seguirá a metodologia que vier a ser estabelecida pelos Administradores dos fundos de investimento nos quais atuar como gestora, sem prejuízo de uma verificação e conferência diária da precificação que for estabelecida pelos Administradores para os ativos sob gestão.

3. GESTÃO DE RISCO DE MERCADO

(i) Definição de risco de mercado

"Risco de Mercado" é a perda potencial de valor do fundo ou da carteira decorrente de oscilações dos preços de mercado ou parâmetros que influenciam os preços de mercado. Estes são, entre outros, os riscos relacionados à variação cambial, taxa de juros, preços de ações, de mercadorias (commodities).

O Risco de Mercado pode ser divido entre risco sistemático e assistemático (ou específico). Risco de mercado sistemático é o efeito adverso da oscilação de preços, devido a mudanças nas condições gerais do mercado. Já o risco de mercado assistemático, é o efeito adverso da oscilação de preços em um ativo específico.

(ii) Escopo da gestão de riscos de mercado: Linhas de Defesa

1ª Linha de Defesa: Perfil de Risco da Persevera

Profissionais experientes e pensamento independente (Forte cultura de risco, com uma forte estrutura de risco associados à um comportamento de risco positivo e desejável)

2ª Linha de Defesa: Estruturação dos Produtos

Diversificados por construção; com books independentes, não correlacionados e com diferentes estratégias (renda fixa, renda variável, local e global); orçamentos de risco pré-definidos e não fungíveis; geridos por profissionais com grande experiência em gestão de fundos e especialistas em mercados/estratégias específicas

3ª Linha de Defesa: Gerenciamento de Risco e 4ª Linha de Defesa: Controle de Risco

A Gestão de risco de Mercado da Persevera é feita através do Gerenciamento de Risco (identificação, mensuração, monitoramento e comunicação de todos os riscos, bem como na análise da adequação entre os riscos assumidos e as características e objetivos dos investimentos) e do Controle de Risco (procura limitar o tamanho e a probabilidade de perdas absolutas. Perdas não são necessariamente indicação de falhas no gerenciamento de risco. Uma gestão de risco eficiente deve reconhecer que grandes perdas são possíveis e desenvolver planos de contingência que lidem com tais perdas se as mesmas ocorrerem).

O gerenciamento de Risco é feito através do Stress Test e o limite de stress do fundo é de -20%[3]. Uma vez definido o limite de Stress para o fundo em termos absolutos, cada gestor terá um limite de stress no seu book equivalente e proporcional ao seu orçamento de risco. Caso haja algum desenquadramento (resultado em teste de stress por book maior do que o limite determinado por book), o gestor será comunicado pela área de gestão de risco e deverá fazer as operações necessárias no dia da comunicação para reenquadrar o fundo.

O Controle de Risco é feito considerando-se o resultado do fundo - e de cada book – em janelas de 63 du. A análise é feita considerando-se todos possíveis retornos em janelas de 63 dias úteis onde a Data-Base esteja também incluída, por exemplo:
Retorno 1: Retorno nos últimos 63 du
Retorno 2: Retorno nos últimos 62 du (+) 1 dia de CDI (projetado)
Retorno 3: Retorno nos últimos 61 du (+) 2 dias de CDI (projetado)
(…)
Retorno 62: Retorno nos últimos 1 du (+) 62 dias de CDI (projetado)
Retorno 63: (+) 63 dias de CDI (projetado)

O limite de perda máxima em janelas de 63 du do Master Funds é -4.5% e de cada book -7%.
O orçamento de risco de cada book estará diretamente relacionado à sua performance em janelas de 63 du, de tal forma que à medida que a sua performance for mais negativa, menor será o espaço (% of Risk Budget) para que o gestor assuma novas posições ou mantenha as já existentes, conforme definido pela seguinte tabela:

[3] Vale destacar que a área de Gestão de Risco da Persevera calculará também a volatilidade projetada, o VaR Paramétrico, o VaR Histórico e o VaR Condicional (Expected Shortfall) por book e para o fundo como um todo, e essas informações poderão ser utilizadas tanto pelos Portfolio Managers quanto pela área de gestão de riscos para análises e simulações adicionais, mas os resultados dessas métricas não serão considerados para efeitos de gerenciamento e controle de riscos. A única métrica que será utilizada como referência para o tamanho das posições dos books e do fundo é o Stress Test.

	Minimum Return in 63wd Fund -4,5%	Worst 5% Return in 63wd Book -7,0%	% of Risk Budget (Fund)	% of Risk Budget (Book)
			100,0%	100,0%
1st threshold (in BRL)	-1,0%	-1,5%	90,0%	90,0%
2nd threshold (in BRL)	-2,0%	-3,0%	75,0%	75,0%
3rd threshold (in BRL)	-3,0%	-4,5%	50,0%	55,0%
4th threshold (in BRL)	-4,0%	-6,5%	25,0%	25,0%
Hard Stop (in BRL)	-4,5%	-7,0%	0,0%	10,0%

5ª Linha de Defesa: Limites de Exposição à Fatores de Risco: a diversificação dos nossos fundos é feita de forma estrutural. Ainda assim, eventualmente, mesmo com books independentes e com orçamentos de riscos não fungíveis, o fundo poderia apresentar posições que, conjuntamente, fossem mais relevantes do que o desenho inicial do produto desejava. Por conta disso, como uma linha de defesa adicional, são definidos limites gerenciais de exposição à fatores de risco para o fundo como um todo, como limite de duration local, duration Emerging Market, duration Developed Market, Renda Variável Local, Renda Variável Offshore, Moedas, dentre outros.

(iii) Procedimentos em caso de desenquadramento:

- Stress Test: caso haja algum desenquadramento (resultado em teste de stress por book maior do que o limite determinado por book), o gestor será comunicado pela área de gestão de risco e deverá fazer as operações necessárias no dia da comunicação para reenquadrar o fundo

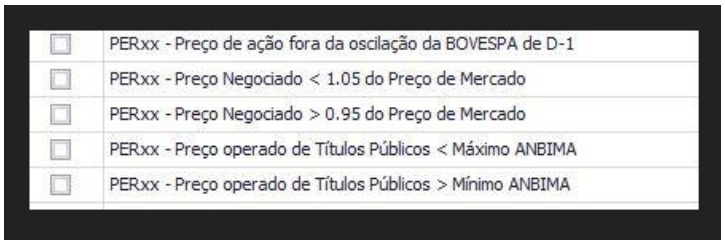
- Limites de Exposição à Fatores de Risco: Caso haja algum desenquadramento nos limites gerenciais de exposição à fatores de risco, a área de Gestão de Risco enviará um alerta para todos os gestores e então poderão ocorrer duas situações específicas:

a) ao receber o alerta o gestor especialista reenquadra imediatamente a sua posição (e o fundo ao limite gerencial) ou;

b) por qualquer motivo, na não ocorrência de a), um Comitê Extraordinário de Risco será convocado para análise e discussão de quais medidas deverão ser tomadas.

(iv) Periodicidade das análises: diária

(v) Túnel de Preço: O monitoramento da aderência dos preços praticados nas operações ("túnel de preços") será feito pelo sistema Compliance Portfolio Manager do Lote 45 e cujas regras e parâmetros encontram-se abaixo:



(vi) Testes de Aderência: A fim de verificar e validar a qualidade das medidas de risco calculadas, a área de Gestão de Risco é responsável por realizar semestralmente um 'Back-Testing', cujos resultados são formalizados e enviados aos membros do Comitê de Risco

4. GERENCIAMENTO DO RISCO DE LIQUIDEZ

(i) Definição de risco de liquidez

O "Risco de Liquidez" é a possibilidade de um fundo ou carteira não estar apto a honrar eficientemente suas obrigações esperadas e inesperadas, correntes ou futuras, inclusive as decorrentes de vinculação de garantias, sem afetar suas operações diárias e sem incorrer em perdas significativas. Também se considera risco de liquidez a possibilidade do Fundo ou carteira não conseguir negociar a preço de mercado uma posição, devida ao seu tamanho em relação ao volume transacionado ou, ainda, por conta de alguma descontinuidade de mercado.

Diferentes fatores podem aumentar esse tipo de risco, destacando-se, exemplificativamente:

- descasamento entre os fluxos de liquidação de ativos e as exigências de recursos para cumprir obrigações incorridas pelos fundos;

- condições atípicas de mercado e/ou outros fatores que acarretem falta de liquidez dos mercados nos quais os valores mobiliários integrantes dos fundos são negociados;
- ativos dos Fundos que são insuficientes para cobrir exigência de depósito de margens junto a contrapartes; ou
- imprevisibilidade dos pedidos de resgates.

(ii) Abrangência

As dificuldades decorrentes da falta de liquidez estão intimamente relacionadas entre si, e podem levar a liquidação antecipada e desordenadas dos ativos do Fundo de Investimento, em prejuízo dos Investidores.

Assim, tendo em vista que o principal objetivo da Gerenciamento de Risco de Liquidez é evitar a transferência de riqueza entre os diversos cotistas de um fundo de investimento, para fins destes procedimentos, considerar-se-ão todos os fundos cujo maior cotista tiver um percentual de alocação no fundo inferior a 100%.

(iii) Elementos da gestão de liquidez

O Gerenciamento de Risco de Liquidez da Persevera será feito através do cálculo de um índice que leva em consideração a relação entre "Caixa Disponível" e "Demanda por caixa" *(Índice de Liquidez)*

O Caixa Disponível será calculado através da análise dos ativos (títulos públicos e privados, cotas de fundos e ações) de cada fundo levando em consideração o volume histórico médio negociado em mercado[4], percentuais desse volume médio (para refletir diferentes cenários) e as obrigações do fundo, incluindo depósitos de margem esperados e outras garantias.

Em função do volume de cada ativo no fundo, dos seus volumes históricos de negociações e dos diferentes percentuais, calculam-se o número de dias para a venda da posição. Cada ativo é ponderado pelo seu peso dentro do portfólio e então calcula-se qual percentual do fundo é liquidado em 1 dia, 2 dias, 3 dias e assim sucessivamente, descontando-se do resultado as obrigações do fundo.

A Demanda por Caixa está diretamente relacionada ao passivo do fundo e aos valores esperados de resgate em situações de normalidade ou extraordinárias.

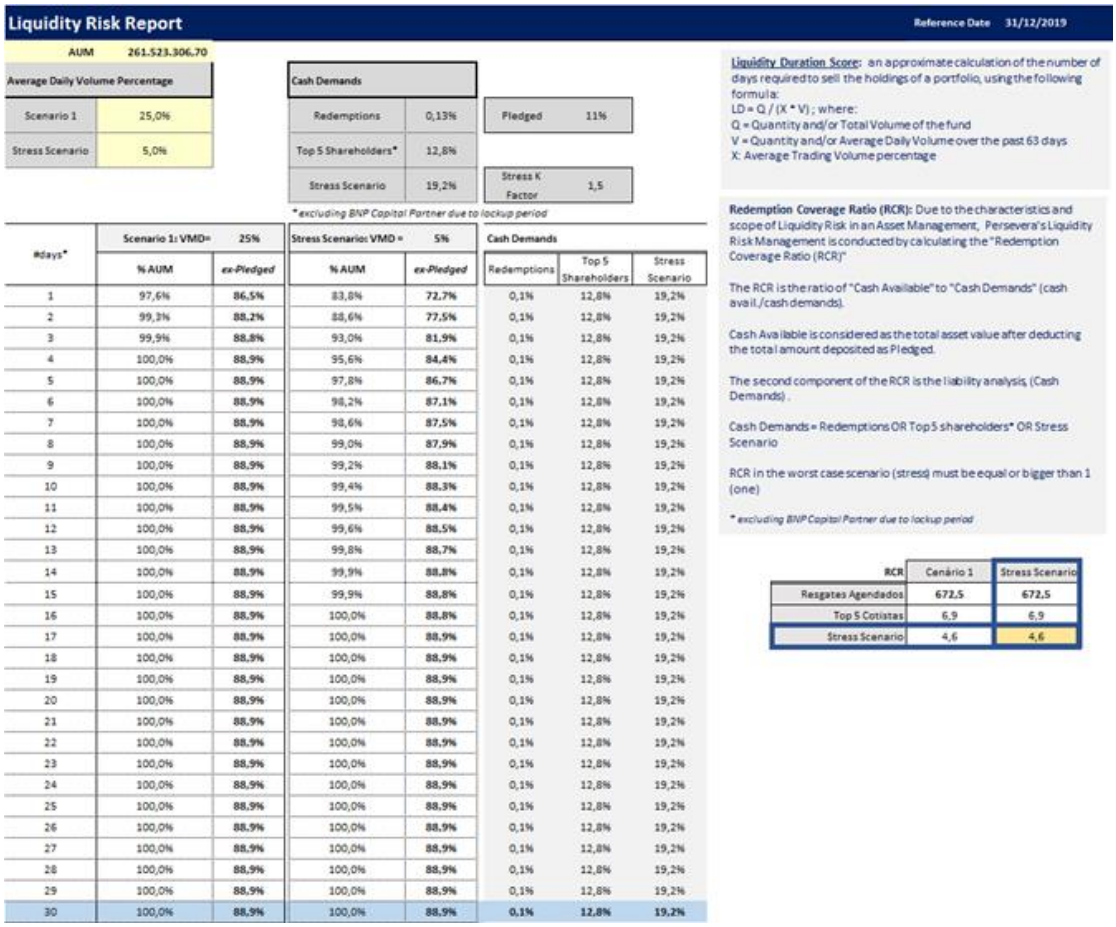
Serão consideradas três situações específicas para a representar a Demanda por caixa:

i) Total de Resgates Agendados;
ii) Somatório dos 5 maiores cotistas e;
iii) Cenário de Stress (maior do que i e ii)

A análise de Liquidez deve ser feita levando-se em consideração as características dos fundos em termos de solicitação, conversão de liquidação dos resgates (características do passivo) e, por conta disso, analisar-se-á o percentual da carteira que pode ser liquidado em X dias (30 dias, no caso do Persevera Compass FIC, por exemplo) versus a demanda por caixa (total de resgates agendados), e o Índice de Liquidez (Caixa Disponível / Demanda por Caixa) deverá ser igual ou maior do que 1 (um). Caso isso não ocorra, um comitê extraordinário de risco será convocado pelo Diretor de Risco e Compliance para análise e definição de eventuais medidas a serem adotadas.

Exemplo:

[4] Fonte: BACEN, Bloomberg e Sistema Lote45. Ativos Offshore são negociados em fundos offshore e os fundos locais investem em cotas de fundos e não em ativos offshore diretamente. Caso isso ocorra, os volumes de negócios dos ativos offshore serão obtidos no sistema Bloomberg.



Liquidity Risk Report — Reference Date 31/12/2019

AUM 261.523.306,70

Average Daily Volume Percentage	
Scenario 1	25,0%
Stress Scenario	5,0%

Cash Demands			
Redemptions	0,13%	Pledged	11%
Top 5 Shareholders*	12,8%		
Stress Scenario	19,2%	Stress K Factor	1,5

*excluding BNP Capital Partner due to lockup period

#days*	Scenario 1: VMD= 25%		Stress Scenario: VMD = 5%		Cash Demands		
	% AUM	ex-Pledged	% AUM	ex-Pledged	Redemptions	Top 5 Shareholders	Stress Scenario
1	97,6%	86,5%	83,8%	72,7%	0,1%	12,8%	19,2%
2	99,3%	88,2%	88,6%	77,5%	0,1%	12,8%	19,2%
3	99,9%	88,8%	93,0%	81,9%	0,1%	12,8%	19,2%
4	100,0%	88,9%	95,6%	84,4%	0,1%	12,8%	19,2%
5	100,0%	88,9%	97,8%	86,7%	0,1%	12,8%	19,2%
6	100,0%	88,9%	98,2%	87,1%	0,1%	12,8%	19,2%
7	100,0%	88,9%	98,6%	87,5%	0,1%	12,8%	19,2%
8	100,0%	88,9%	99,0%	87,9%	0,1%	12,8%	19,2%
9	100,0%	88,9%	99,2%	88,1%	0,1%	12,8%	19,2%
10	100,0%	88,9%	99,4%	88,3%	0,1%	12,8%	19,2%
11	100,0%	88,9%	99,5%	88,4%	0,1%	12,8%	19,2%
12	100,0%	88,9%	99,6%	88,5%	0,1%	12,8%	19,2%
13	100,0%	88,9%	99,8%	88,7%	0,1%	12,8%	19,2%
14	100,0%	88,9%	99,9%	88,8%	0,1%	12,8%	19,2%
15	100,0%	88,9%	99,9%	88,8%	0,1%	12,8%	19,2%
16	100,0%	88,9%	100,0%	88,8%	0,1%	12,8%	19,2%
17	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
18	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
19	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
20	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
21	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
22	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
23	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
24	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
25	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
26	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
27	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
28	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
29	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%
30	100,0%	88,9%	100,0%	88,9%	0,1%	12,8%	19,2%

Liquidity Duration Score: an approximate calculation of the number of days required to sell the holdings of a portfolio, using the following formula:
LD = Q / (X * V) ; where:
Q = Quantity and/or Total Volume of the fund
V = Quantity and/or Average Daily Volume over the past 63 days
X: Average Trading Volume percentage

Redemption Coverage Ratio (RCR): Due to the characteristics and scope of Liquidity Risk in an Asset Management, Persevera's Liquidity Risk Management is conducted by calculating the "Redemption Coverage Ratio (RCR)"

The RCR is the ratio of "Cash Available" to "Cash Demands" (cash avail./cash demands).

Cash Available is considered as the total asset value after deducting the total amount deposited as Pledged.

The second component of the RCR is the liability analysis, (Cash Demands) .

Cash Demands = Redemptions OR Top 5 shareholders* OR Stress Scenario

RCR in the worst case scenario (stress) must be equal or bigger than 1 (one)

* excluding BNP Capital Partner due to lockup period

RCR	Cenário 1	Stress Scenario
Resgates Agendados	672,5	672,5
Top 5 Cotistas	6,9	6,9
Stress Scenario	4,6	4,6

(iii) Procedimentos em situações especiais de iliquidez das carteiras

Em casos excepcionais de iliquidez dos ativos componentes da carteira dos Fundos de Investimento, inclusive em decorrência dos pedidos de resgates incompatíveis com a liquidez existente, ou que possam implicar alteração do tratamento tributário de algum dos Fundos de Investimento ou do conjunto dos cotistas, em prejuízo destes últimos, a Gestora poderá solicitar que a administradora declare o fechamento para a realização de resgates do Fundo que encontre-se em tal situação sem liquidez, sendo obrigatória a convocação de Assembleia Geral, na forma do regulamento do Fundo correspondente, para tratar sobre as seguintes possibilidades:

- reabertura ou manutenção do fechamento do Fundo para resgate;
- possibilidade do pagamento de resgate em títulos e valores mobiliários;
- cisão do Fundo de Investimento; e
- liquidação do Fundo de Investimento.

5. GESTÃO DE RISCOS DE CRÉDITO E CONTRAPARTE

(i) Definição de Risco de Crédito

"Risco de Crédito" é a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas respectivas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas na renegociação e aos custos de recuperação de crédito.

(ii) Escopo

Esta política aplica-se apenas aos investimentos em ativos de crédito feitos pela Gestora.

(iii) Princípios para a gestão de Risco de Crédito

Os fundos da Persevera não têm por objetivo investir em ativos de crédito privado e, portanto, esse tema não será abordado nesse manual. Caso esse posicionamento seja alterado no futuro o seu gerenciamento e controle será apresentado em uma nova versão desse manual.

(iv) *Contraparte*

Apesar de não ser objetivo da Gestora investir em ativos de crédito privado, seus fundos poderão ser expostos a esse risco de maneira passiva, através do 'risco de contraparte' que será calculado – quando aplicável – através da exposição às operações de derivativos no mercado para operações "de balcão" (*over-the-counter*).

Esta exposição será monitorada pela área de risco e o risco de crédito implícito destas contrapartes utilizará, como base, o risco soberano brasileiro e avaliações de agências de rating.

6. GESTÃO DE RISCO DE CONCENTRAÇÃO

(i) Definição de risco de concentração

O Risco de Concentração se caracteriza pela concentração de investimentos de carteiras de valores mobiliárias em um mesmo fator de risco como país, região, emissor, tipo e classe de ativo, dentre outros, que pode potencializar a exposição da carteira.

Caso os regulamentos dos fundos não determinem limites específicos em relação à diversificação da carteira, o gestor deve procurar adotar boas práticas de diversificação que mitigue o risco de concentração, considerando tamanho das posições e a correlação entre as mesmas.

(ii) Procedimento

Haverá monitoramento diário dos riscos descritos acima, seguindo o regulamento de cada fundo e situações que representem um desvio e que demandem algum curso de ação serão reportadas ao Comitê de Risco.

7. GESTÃO DE RISCOS OPERACIONAIS

(i) Definição de risco operacional

O risco operacional é definido como o risco de perda direta ou indireta, resultante de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

Processos - riscos advindos da ocorrência de fragilidades nos processos, que podem ser gerados por falta de regulamentação interna e/ou documentação sobre políticas e procedimentos; deficiência no desenho dos processos, falta de controle.

Sistemas - é o risco originado de situações como:

a) Incapacidade dos sistemas de proverem informações aos tomadores de decisão, em tempo real e com alta confiabilidade;

b) Possibilidade de descontinuidade de atividades que utilizam recursos tecnológicos, por sobrecarga de sistemas de processamentos de dados, de comunicação e elétricos, entre outros.

Pessoas - possibilidade de perdas em função de falhas humanas por situações diversas, inclusive, falta de valores éticos.

Externos - incidente/violação surgindo de fontes externas ou do gerenciamento de fontes externas.

São exemplos de eventos de Risco Operacional:

- fraudes internas;
- fraudes externas;
- demandas trabalhistas e segurança deficiente do local de trabalho;
- práticas inadequadas relativas a clientes, produtos e serviços;
- danos a ativos físicos próprios ou em uso pela instituição;
- aqueles que acarretem a interrupção das atividades da instituição;
- falhas em sistemas de tecnologia da informação; e
- falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.

(ii) Princípios Gerais da gestão de riscos operacionais

1. <u>Simplicidade</u>

Quanto mais complexas forem as nossas atividades, maior o custo de se prevenir e remediar um eventual erro, assim como maior a probabilidade da ocorrência de um erro. Dessa forma, procuramos simplificar a gestão de portfólio e a estrutura administrativa da empresa.

2. Organização

É importante manter as operações organizadas de maneira que os procedimentos sejam facilmente executados e verificados. Procuramos manter um manual de operações para as funções mais críticas de maneira que mesmo um Colaborador não acostumado à execução de tais funções possa executá-las em caso de necessidade.

3. Integridade

Uma cultura de integridade norteia os potenciais conflitos de interesses e a atuação em situações de interpretações ambíguas. Assim, problemas são evitados ainda em estágio preliminar.

4. Diligência

É importante manter a supervisão das várias regras e procedimentos e, igualmente importante, rapidamente agir para a solução de um problema tão logo seja identificado.

5. Matriz de Risco Operacional

O gerenciamento de riscos operacional é feito através de uma matriz que considera os seguintes pontos:

i) Identificação de riscos inerentes ao negócio.
ii) Quantificação dos Riscos: mensuração de probabilidade e impacto dos riscos identificados.
iii) Exposição/Mitigação dos Riscos: definição de controles para mitigar os riscos e mantê-los em níveis aceitáveis.
iv) Matriz Risco Operacional

(i) Identificação de riscos inerentes ao negócio

A identificação dos riscos operacionais é feita inicialmente pelos riscos 'primários' (Processos, Sistemas, Pessoas e Externos) e em seguida pelos riscos secundários, como exemplificado abaixo:

Risco Primario	Risco Secundário	Identificação do Risco
Externo: incidente/violação surgindo de fontes externas ou do gerenciamento de fontes externas.	Interrupção das Atividades	Falha no fornecimento de energia
	Interrupção das Atividades	Instalações indisponíveis por conta de incêndio/desastres, etc
	Interrupção das Atividades	Falha no acesso à Internet

A identificação dos riscos é feita considerando-se as referências nos Códigos e Instruções dos órgãos reguladores (ANBIMA e CVM, por exemplo) bem como a experiência, a expertise e as observações empíricas acerca de cada risco em particular de cada colaborador da Persevera.

ii) Quantificação dos Riscos: mensuração de probabilidade e impacto dos riscos identificados.

- Probabilidade

A cada um dos riscos identificados foi associada uma probabilidade (F) de sua materialização, considerando a frequência do processo (P) e desassociando qualquer controle que pudesse existir para sua mitigação.

Sempre que possível, o cálculo de probabilidade considerou o histórico das operações da instituição ou o histórico do mercado. Quando não foram encontradas referências internas ou externas para realizar a estimativa, os profissionais envolvidos no cálculo consideraram sua própria expertise acerca de cada risco em particular, os aspectos da cultura organizacional e a natureza e complexidade das operações às quais os riscos estavam associados.

Uma estimativa apurada de probabilidade é um dos maiores desafios na construção de qualquer matriz de riscos, principalmente quando não há referências anteriores. Assim, é importante que os profissionais envolvidos com gerenciamento de riscos executem revisões constantes de tais probabilidades de forma a promover a sua depuração e aperfeiçoamento.
A tabela abaixo é utilizada como base e referência para a definição das probabilidades de cada risco:

1	Raro	Até 5%	Desprezível. Poderia ocorrer somente em circunstâncias excepcionais
2	Baixa	Até 25%	Poderia ocorrer em algum momento futuro

3	Média	Até 55%	Deve ocorrer em algum momento
4	Alta	Até 75%	É provável que ocorra em algum momento
5	Muito alta	Acima de 90%	Ocorrerá na maioria das circunstâncias

- *Impactos*

Uma vez identificados todos os riscos e estimada a probabilidade de ocorrência de cada um, foram analisados os impactos (S) que sua materialização teria sobre os objetivos estabelecidos para a organização.

Nesta análise vários aspectos quantitativos e qualitativos foram considerados, tais como a natureza do impacto, a maior perda, a quantidade de itens processados e outros, que tinham como principal objetivo obter uma estimativa razoável acerca da relevância de cada risco em cada atividade e/ou processo.

			Serviço ao cliente	**Atitude da mídia**	**Ação Regulatória**
1	Irrelevante	Até USD 7,5 mil	Clientes não são impactados ou ignoram o problema.	Reputação muito alta, visto como um fornecedor de qualidade	O regulador reconhece o alto nível de aderência e conformidade com os padrões
2	Baixa	Até USD 37,5 mil	Alguns clientes tomam o conhecimento do problema, mas o impacto sobre eles é desprezível. Atendimento prejudicado temporariamente.	Citações normais na mídia ou mencionado na internet sobre bancos	Comentários (advertências) verbais do regulador
3	Médio	Até USD 150 mil	Número significativo de clientes toma o conhecimento do problema e sofre alguma inconveniência.	Artigos críticos na mídia/TV. Crítica pública dos reguladores ou entidades setoriais	Apontamentos nos relatórios de inspeção da verificação regulatória
4	Alto	Até USD 1,5 milhão	Atendimento indisponível por tempo longo (24h)	Notícias múltiplas em vários jornais e/ou TVs, por vários dias.	Violações reincidentes ou múltiplas
5	Muito alta	Acima de USD 1,5 milhão	A maioria dos clientes sofre com o problema que causa uma grande inconveniência.	Preocupação do governo ou repercussão política equivalente. Perda de confiança do público	Sanção do Regulador contra a empresa por violações relevantes. Multas e penalidades muito grandes

- *Perda potencial ou inerente: Score*

O 'Score' da perda inerente esperada (PI) é calculado multiplicando-se o score da probabilidade pelo score do Impacto.

Exemplo:

Risco: Falha do Fornecimento de Energia
Probabilidade de Ocorrência: Baixa (Score 2)
Impacto em caso de ocorrência: Médio (Score 3)
Score Perda Potencial: 2 * 3 = 6

iii) Exposição/Mitigação dos Riscos

Nesta fase são documentados e avaliados os controles existentes. Os controles também são analisados individualmente e correlacionados com cada um dos riscos anteriormente apontados.

É importante registrar que tanto pode ocorrer de um mesmo risco ter vários controles mitigadores, quanto de uma mesma atividade e/ou ferramenta ser utilizada como controle para vários riscos. O importante, nesta etapa, é fazer uma estimativa a mais precisa possível acerca da qualidade dos controles e de sua capacidade para mitigar os riscos apontados.

A tabela abaixo ilustra o score de Exposição/Mitigação

	Mitigação	Controle
1	Alta (exposição muito pequena)	Definição detalhada de responsabilidade que garante a separação clara de funções. Controle automatizados. Controles preventivos.
2	Significativa ((exposição Limitada)	Responsabilidades claras para a maioria das funções. A maioria dos controles é automatizada e preventiva
3	Moderada (exposição média)	Responsabilidades definidas de forma genérica. Alguns problemas pequenos sem follow-up. Controle automatizados e manuais. Preventivos e corretivos.
4	Baixa (exposição significativa)	Não há ações preventivas de longo prazo. A maioria dos controles é manual e corretivos.
5	Irrelevante (exposição muito grande)	Indefinição de nível de controle e de responsabilidades

iv) Matriz de Risco: Perda Potencial vs Exposição

Uma vez identificado o score dos fatores mitigantes de cada risco, podemos estimar a sua classificação final, que é a relação entre a perda potencial e a exposição geral ao risco, conforme abaixo apresentado:

	Exposição (Score)					
Perda Potencial (Score)		1	2	3	4	5
	>10	C+	B	B	A	A
	8-10	C	C	B	B	A
	5-7	C	C	C	B	B
	3-4	D	C	C	C	B
	0-2	D	D	C	C	C

		1	2	3	4	5
Perda Potencial (Score)	25	C+	B	B	A	A
	24	C+	B	B	A	A
	23	C+	B	B	A	A
	22	C+	B	B	A	A
	21	C+	B	B	A	A
	20	C+	B	B	A	A
	19	C+	B	B	A	A
	18	C+	B	B	A	A
	17	C+	B	B	A	A
	16	C+	B	B	A	A
	15	C+	B	B	A	A
	14	C+	B	B	A	A
	13	C+	B	B	A	A
	12	C+	B	B	A	A
	11	C+	B	B	A	A
	10	C	C	B	B	A
	9	C	C	B	B	A
	8	C	C	B	B	A
	7	C	C	C	B	B
	6	C	C	C	B	B
	5	C	C	C	B	B
	4	D	C	C	C	B
	3	D	C	C	C	B
	2	D	D	C	C	C
	1	D	D	C	C	C
	0	D	D	C	C	C

Riscos classificados como “A” ou “B” deverão ser apresentados pelo Diretor de Risco ao Comitê Executivo e medidas e ações corretivas – a fim de reduzir o score final – deverão ser apresentadas, discutidas e um prazo para a sua efetiva implementação deverá ser definido.

(ii) Reporte de Incidentes

Os incidentes de riscos operacionais devem ser registrados com o máximo de detalhes possíveis. Além de formarem a base para futuros cálculos de probabilidade e impactos, o reporte constante de incidentes serve para entendimento e análise dos problemas (erros ou falhas operacionais ocorridas), sejam eles riscos identificados ou não.
O Diretor de Risco e Compliance é responsável pelo registro dos incidentes e eventuais perdas operacionais.

8. GESTÃO DE RISCO CIBERNÉTICO (SEGURANÇA CIBERNÉTICA)

1. Introdução[5]

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.
Esses ataques são geralmente realizados por organizações criminosas ou hackers individuais, organismos de Estado, terroristas, colaboradores, competidores etc. com o objetivo de:

i) obter ganho financeiro,
ii) Roubar, manipular ou adulterar informações,
iii) Obter vantagens competitivas e informações confidenciais de empresas concorrentes,
iv) Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança, v) Promover ideias políticas e/ou sociais,
v) Praticar o terror e disseminar pânico e caos.

Os invasores podem utilizar vários métodos para os ataques cibernéticos, dentre os quais podemos destacar:

- Malware – softwares desenvolvidos para corromper computadores e redes:

[5] Parte dessa introdução foi extraída do ‘Guia de Cibersegurança’ da ANBIMA - Dez/2017

- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
- Spyware: software malicioso para coletar e monitorar o uso de informações; e
- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
  - Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento; - Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
  - Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
  - Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
  -Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de vários computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais.
Apresentamos nesse item os procedimentos e controles de Segurança Cibernética da Persevera Gestão de Recursos Ltda[6].

2. Segurança Cibernética

Os responsáveis pela Segurança Cibernética na Persevera são os colaboradores Cesar Dammous (Diretor de Risco e Compliance) e Fernando Fontoura (Diretor Financeiro e responsável por TI) e os procedimentos e controles efetuados seguem os seguintes pontos:

2.1. Identificação de riscos: identificar os riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção. Essa identificação é feita considerando-se as referências nos Códigos e Instruções dos órgãos reguladores (ANBIMA e CVM, por exemplo) bem como a experiência, a expertise e as observações empíricas acerca de cada risco em particular de cada colaborador da Persevera.

2.2. Ações de Prevenção e proteção: Nesta fase são documentados e avaliados os controles existentes. Os controles também são analisados individualmente e correlacionados com cada um dos riscos anteriormente apontados. É importante registrar que tanto pode ocorrer de um mesmo risco ter vários controles mitigadores, quanto de uma mesma atividade e/ou ferramenta ser utilizada como controle para vários riscos. O importante, nesta etapa, é fazer uma estimativa a mais precisa possível acerca da qualidade dos controles e de sua capacidade para mitigar os riscos apontados.

Os procedimentos e os controles devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos

[6] Os procedimentos aqui descritos e detalhados foram extraídos da 'Matriz de Risco Operacional' da Persevera. O Gerenciamento de Risco de Risco Operacional (definido como o risco de perda direta ou indireta, resultante de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos) é feito através da: 1. Identificação de riscos inerentes ao negócio; 2. Quantificação dos Riscos: mensuração de probabilidade e impacto dos riscos identificados e; 3. Exposição/Mitigação dos Riscos: definição de controles para mitigar os riscos e mantê-los em níveis aceitáveis.

de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações[7].

A identificação dos riscos bem como as ações de prevenção e controles (fatores mitigantes) estão apresentados no item 3 - ***Tabela Resumo Riscos, Procedimentos e Controles***

2.3. Monitoramento e testes: – detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados

Anualmente, a fim de que os resultados sejam apresentados no último Comitê de Risco e Compliance de cada ano, o responsável por TI e o Diretor de Compliance farão os seguintes levantamentos:

i) Monitoramento de todas as ações de proteção implementadas
ii) Atualização do inventário de hardware e software
iii) Checar se os sistemas operacionais e softwares estão atualizados
iv) Realização periódicas de testes de invasão e pishing
v) Análise regular de logs e trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques

2.4. Criação de plano de resposta – ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

Deve haver critérios para classificação dos incidentes, por severidade. Eles podem requerer desde uma simples duplicação de equipamentos para a continuidade dos serviços, até o uso de instalações de contingência em casos mais severos. Nesses casos, o plano deve prever também o processo de retorno às instalações originais após o término do incidente.
Deve-se atentar para questões de segurança e controles de acesso também nas instalações de contingência.
Esses pontos estão detalhados no documento 'Plano de Continuidade de Negócios'.

2.5. Reciclagem e revisão – Manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Anualmente, no último Comitê de Risco e Compliance de cada ano, o Diretor de Risco juntamente com o responsável pela área de TI apresentarão aos demais membros do Comitê os seguintes pontos:

i) Avaliação de risco (anteriormente identificados e eventualmente novas vulnerabilidades e ameaças identificadas),
ii) Fatores mitigantes,
iii) Planos de resposta
iv) Monitoramento dos ambientes

[7] Resolução BACEN No. 4.658, de 26/04/18

3. Tabela Resumo Riscos, Procedimentos e Controles

Risco Primario	Risco Secundário	Identificação do Risco	Fatores Mitigantes
Externo: incidente/violação surgindo de fontes externas ou do gerenciamento de fontes externas.	Interrupção das Atividades	Falha no fornecimento de energia	Laptops (baterias), no-break (bloomberg e rede) e celulares
	Interrupção das Atividades	Instalações indisponíveis por conta de incêndio/desastres, etc	atual: computadores pessoais + nuvem (melhoria: máquina virtual aws)
	Interrupção das Atividades	Falha no acesso à Internet	Links WAN redundantes + hotspots celulares
	Interrupção das Atividades	Sistema do administrador inoperante	carteira espelho + email + telefonia
	Risco de Terceirização e/ou Fornecedores	Falência de fornecedor essencial para a operação (Lote45, Compli.ly, etc)	Sistemas alternativos (blomberg 'Port') + planilhas
Sistemas : a) Incapacidade dos sistemas de proverem informações aos tomadores de decisão, em tempo real e com alta confiabilidade; b) Possibilidade de descontinuidade de atividades que utilizam recursos tecnológicos, por sobrecarga de sistemas de processamentos de dados, de comunicação e elétricos, entre outros.	Falhas de Sistemas	Falha de Hardware Monitor	Monitor reserva + monitor laptop
	Falhas de Sistemas	Falha de Hardware Laptop	Laptop reserva
	Falhas de Sistemas	Falha de Software COMPLI.LY	Servidores redundantes e sincronizados
	Falhas de Sistemas	Falha de Software LOTE 45	Servidores redundantes e sincronizados
	Falhas de Sistemas	Falha de Software Bloomberg	Outros fornecedores de Market Data
	Falhas de Sistemas	Falha de Software Valor Pro	Outros fornecedores de Market Data
	Falhas de Sistemas	Falha de Software Broadcast	Outros fornecedores de Market Data
	Falhas de Sistemas	Falha no armazenamento de dados em nuvem	SLA 99,9% + Backup Nuvem-Nuvem
	Infração de Segurança de Sistemas (Risco de ataques Cibernéticos)	Invasões externas (Malware): vírus, cavalo de troia, spyware, ransomware	Antivírus + Laptop Spare + Nuvem
	Infração de Segurança de Sistemas (Risco de ataques Cibernéticos)	Engenharia social (métodos de manipulação para obter informações confidenciais):Pharming, Phishing, Vishing, Smishing, Acesso pessoal	Autenticação em 2 fatores
	Infração de Segurança de Sistemas (Risco de ataques Cibernéticos)	Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços	Firewall + Ausência de servidores locais
	Infração de Segurança de Sistemas (Risco de ataques Cibernéticos)	Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico	Firewall + Ausência de servidores locais + Antivírus
	Infração de Segurança de Sistemas	Acesso inapropriado à diretórios específios	Permissionamento específico com autorização prévia do responsável por TI e Diretor de Compliance
	Infração de Segurança de Sistemas	Acesso inapropriado à sistemas e/ou sites	Permissionamento específico com autorização prévia do responsável por TI e Diretor de Compliance

9. RELATÓRIO GERENCIAL

Será elaborado um relatório gerencial de risco, em periodicidade mínima mensal, pelo Diretor de Risco da Persevera, sendo encaminhado por e-mail - com confirmação de recebimento - aos demais diretores e sócios da Gestora, para ciência e acompanhamento, em observância ao disposto no Artigo 23 da Instrução da Comissão de Valores Mobiliários nº 558/15.

10. PLANO DE CONTINUIDADE DOS NEGÓCIOS

(i) Objetivo

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal, a Persevera possui uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada funcionário, administrador ou colaborador na execução do Plano de Continuidade de Negócio ("PCN").

O PCN é um plano traçado para que seja possível dar continuidade à execução de atividades consideradas críticas para a prestação de serviços pela Persevera, de forma que os interesses dos clientes da Persevera não sejam prejudicados.

O PCN estabelecido neste Manual é de responsabilidade da do Diretor de Risco e Compliance, a quem cumprirá garantir que o PCN esteja em concordância com as leis e normas dos órgãos reguladores cabíveis, bem como zelar por sua atualização e cumprimento do cronograma de treinamento previsto.

Na eventual ocorrência de qualquer evento que impossibilite seu acesso ou permanência nas dependências da Persevera, os Colaboradores devem imediatamente contatar o Diretor de Risco e Compliance que avaliará as atividades em andamento e

orientará os Colaboradores quanto à continuidade das atividades fora das dependências da Persevera, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

(ii) Principais contingências mapeadas e respostas do PCN

Apresentamos os riscos potenciais identificados diretamente relacionados à continuidade dos negócios e as principais contingências mapeadas e respostas do PCN (os riscos associados à Infração de Segurança de Sistemas são apresentados no item "Segurança Cibernética"):

1. Falha no fornecimento de energia

Todos os colaboradores possuem laptops (baterias) e em caso de falta de energia, a empresa possui um No-break para até 5 (cinco) horas. Em caso de períodos maiores que 5 (cinco) horas, o acesso dos dados e arquivos deve ser feito remotamente.
O Diretor de Risco e Compliance é o responsável em monitorar e avaliar a situação e orientar os demais colaboradores quanto à continuidade das atividades fora das dependências da Persevera, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

2.Queda do link para acesso à internet

Dois links redundantes de operadoras diferentes. Caso nenhuma das contingências funcionem, é possível fazer o acesso remoto aos arquivos hospedados na nuvem, que podem ser acessados através de outros provedores.
O responsável por TI é o responsável em monitorar e avaliar a situação e buscar, dentre as contingências supracitadas, as melhores alternativas.

3. Sistema do administrador inoperante

Caso o sistema do administrador esteja inoperante e não seja possível executar as atividades de importação e exportação de informações, a mensageria será feita por email e/ou telefone. Além disso, o sistema Lote45 será utilizado a fim de obtenção e uma 'cota-espelho' e batimento de quantidades e operações junto às corretoras.

4. Impossibilidade de executar as ordens junto às corretoras

As ordens serão primariamente executadas pelos operadores junto às corretoras de forma eletrônica e/ou de forma verbal e/ou escrita (as ordens verbais deverão ser sempre realizadas através de ligações telefônicas gravadas).
Uma vez realizada a ordem e concretizada a negociação, as operações serão automaticamente atualizadas no sistema de portfólio compliance e gerenciamento de risco de mercado através do sistema 'trades hunter' do Lote45 e os gestores, bem como a área de risco e performance, poderão acompanhar as operações *on-line.*

5. Falha de hardware Monitor e Laptop

Contingência Monitor: monitor laptop + monitor reserva
Contingência Laptop: laptop reserva

6. Falha do armazenamento de dados na nuvem

A Gestora trabalha com o backup de seus dados na nuvem, possibilitando o acesso à pelo menos as últimas 30 (trinta) versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).
Todas os dados e arquivos da Gestora, do banco de dados dos clientes e os modelos dos analistas são armazenados na nuvem.
Os principais executivos da Gestora possuem acesso remoto aos seus e-mails e à nuvem de arquivos da empresa, de modo que possam acessá-los de fora do escritório, se necessário.
Contingência: SLA 99,9% + Backup Nuvem-Nuvem
O responsável por TI é o responsável em monitorar e avaliar a situação e buscar, dentre as contingências supracitadas, as melhores alternativas.

7. Falha de Software COMPLI.LY e Falha de Software Lote45

Contingência: Fornecedores apresentam servidores redundantes e sincronizados

8. Falha de Software Bloomberg, Valor Pro e Broadcast

Contingência: em caso de falha de 01 (ou 02 softwares simultaneamente) haverá sempre, no mínimo, um terceiro fornecedor de Market Data

9. Contingências para e-mail

Serviço de e-mail é hospedado em nuvem, com redundância e acordo de nível de serviço elevados, garantindo a continuidade do acesso remoto. Há possibilidade de comunicação nos celulares dos funcionários e via chat do Bloomberg.

10. Contingências com serviço de telefonia

Contrato de suporte com prazo de atendimento para suporte à central de telefonia. Disponibilidade de linha telefônica de backup fornecida pela provedora de internet. Há possibilidade de comunicação nos celulares dos funcionários e via chat do Bloomberg.

11. Instalações Indisponíveis por conta de incêndio/desastres, etc

Na impossibilidade de se utilizar o espaço físico do escritório, os colaboradores poderão acessar remotamente, de qualquer computador, *máquinas virtuais* hospedadas na nuvemjá configuradas com os mesmos sistemas utilizados em produção.
O Diretor de Risco e Compliance é o responsável em monitorar e avaliar a situação e orientar os demais colaboradores quanto à continuidade das atividades fora das dependências da Persevera, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

(iii) validação e/ou testes

Alguns riscos potenciais supracitados poderão ser validados e testados à medida que situações específicas ocorrerem já que não são eventos extremamente raros (falha de energia e queda de link da internet, por exemplo).

De qualquer forma será criada uma rotina de testes anual onde algumas situações específicas serão simuladas a fim avaliar se as contingências desenvolvidas são capazes de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da instituição e manter a integridade, a segurança e a consistência dos bancos de dados e se os planos adotados podem ser ativados tempestivamente.

O Diretor de Risco e Compliance é responsável pela atualização e cumprimento do cronograma de testes.