MILES CAPITAL

MANUAL DE CONTROLES INTERNOS *(COMPLIANCE)*

Versão	Atualizada em	Responsável:
3	Janeiro/2019	**Otávio Mendonça Barros**

ÍNDICE

1. INTRODUÇÃO E OBJETIVO

O termo *compliance* é originário do verbo, em inglês, *to comply*, e significa "estar em conformidade com regras, normas e procedimentos".

Visto isso, a **Miles Capital Ltda.** ("Gestora") adotou em sua estrutura as atividades de "Controles Internos" ou "*Compliance*". O diretor responsável pelo *compliance* ("Diretor de *Compliance*") tem como objetivo garantir o cumprimento das leis e regulamentos emanados de autoridades competentes aplicáveis às atividades de Gestora, bem como as políticas e manuais da Gestora, e obrigações de fidúcia e lealdade devidas aos investidores de fundos geridos ("Investidores"), prevenindo a ocorrência de violações, detectando as violações que ocorram e punindo ou corrigindo quaisquer de tais descumprimentos.

Este Manual de Controles Internos *(compliance)* ("Manual de *Compliance*") foi elaborado para atender especificamente às atividades desempenhadas nesta data pela Gestora, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica nos termos do item 2 abaixo.

Este Manual de *Compliance* é aplicável a todos os sócios, diretores, funcionários, e estagiários da Gestora (em conjunto os "Colaboradores" e, individualmente e indistintamente, o "Colaborador").

Este Manual de *Compliance* deve ser lido em conjunto com o Código de Ética da Gestora, que também contém regras que visam a atender aos objetivos aqui descritos.

2. PROCEDIMENTOS

2.1. Designação de um Diretor Responsável

A área de *compliance* da gestora é formada pelo Diretor de *Compliance*, **Otávio Mendonça Barros**, devidamente nomeado no contrato social da Gestora, e por um analista com relevante experiência na área.

O Diretor de *Compliance* exerce suas funções com plena independência e não atua em funções que possam afetar sua independência, dentro ou fora da Gestora. Da mesma forma, a área de *compliance* não está sujeita a qualquer ingerência por parte da equipe de gestão.

O Diretor de *Compliance* é o responsável pela implementação geral dos procedimentos previstos neste Manual de *Compliance*, e caso tenha que se ausentar por um longo período de tempo, deverá ser substituído ou deverá designar um responsável temporário para cumprir suas funções durante este período de ausência. Caso esta designação não seja realizada, caberá aos sócios da Gestora fazê-lo.

O Diretor de *Compliance* tem como principais atribuições e responsabilidades o suporte a todas as áreas da Gestora no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Gestora com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

São também atribuições do Diretor de *Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*:

(i) Implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles;

(ii) Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;

(iii) Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no "Código de Ética", assim como avaliar as demais situações que não foram previstas nas Políticas Internas (conforme abaixo definido);

(iv) Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;

(v) Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;

(vi) Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse;

(vii) Reconhecer situações novas no cotidiano da administração interna ou nos negócios da Gestora que não foram planejadas, fazendo a análise de tais situações;

(viii) Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Gestora;

(ix) Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem da Gestora, assim como das pessoas envolvidas no caso.

2.2. Revisão Periódica e Preparação de Relatório

O Diretor de *Compliance* deverá revisar pelo menos semestralmente este Manual de *Compliance* para verificar a adequação das políticas e procedimentos aqui previstos, e sua efetividade. Tais revisões periódicas deverão levar em consideração, entre outros fatores, as violações ocorridas no período anterior, e quaisquer outras atualizações decorrentes da mudança nas atividades realizadas pela Gestora.

O Diretor de *Compliance* deve encaminhar aos diretores da Gestora, até o último dia do mês de janeiro e julho de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las, que deverá seguir o formato previsto no Anexo I.

O relatório referido no parágrafo acima deverá ficar disponível para a Comissão de Valores Mobiliários ("CVM") na sede da Gestora.

2.3. Treinamento

A Gestora possui um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre as Políticas Internas, inclusive este Manual de *Compliance,* aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento.

O Diretor de *Compliance* deverá conduzir sessões de treinamento aos Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste manual, e deve estar frequentemente disponível para responder questões que possam surgir em relação aos termos deste Manual de *Compliance* e quaisquer regras relacionadas a *compliance*.

A periodicidade mínima do processo de reciclagem continuada será anual.

Os materiais, carga horária e grade horária serão definidos pelo Diretor de *Compliance*, podendo inclusive contratar terceiros para ministrar aulas e/ou palestrantes sobre assuntos pertinentes.

2.4. Apresentação do Manual de Compliance e suas Modificações

O Diretor de *Compliance* deverá entregar uma cópia deste Manual de *Compliance*, e de todas as políticas internas da Gestora, inclusive o Código de Ética, Política de Investimento Pessoal e Política de Gestão de Risco ("Políticas Internas"), para todos os Colaboradores por ocasião do início das atividades destes na Gestora, e sempre que estes documentos forem modificados. Mediante o recebimento deste Manual de *Compliance*, o Colaborador deverá confirmar que leu, entendeu e cumpre com os termos deste Manual de *Compliance* e das Políticas Internas, mediante assinatura do termo de adesão que deverá seguir o formato previsto no Anexo II.

2.5. Atividades Externas

Os Colaboradores devem obter a aprovação escrita do Diretor de *Compliance* antes de envolverem-se em negócios externos à Gestora. "Atividades Externas" incluem ser um diretor, conselheiro ou sócio de sociedade ou funcionário ou consultor de qualquer entidade ou organização (seja em nome da Gestora ou não). Os Colaboradores que desejam ingressar ou engajar-se em tais Atividades Externas devem obter a aprovação prévia por escrito do Diretor de *Compliance* por meio da "Solicitação para Desempenho de Atividade Externa" na forma do Anexo III.

Não será necessário a prévia autorização do Diretor de *Compliance* para Atividades Externas relacionadas a caridade, organizações sem fins lucrativos, clubes ou associações civis.

2.6. Supervisão e Responsabilidades

Todas as matérias de violações a obrigações de *compliance*, ou dúvidas a elas relativas, que venham a ser de conhecimento de qualquer Colaborador devem ser prontamente informadas ao Diretor de *Compliance*, que deverá investigar quaisquer possíveis violações de regras ou procedimentos de *compliance*, e determinar quais as sanções aplicáveis. O Diretor de *Compliance* poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

2.7. Sanções

As sanções decorrentes do descumprimento das regras estabelecidas neste Manual de *Compliance* e/ou das Políticas Internas serão definidas e aplicadas pelo Diretor de *Compliance*, a seu critério razoável, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente, sem prejuízo da aplicação de penalidades pela CVM e do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio dos procedimentos legais cabíveis.

3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

Nos termos da Instrução CVM nº 558, de 26 de março de 2015, especialmente o Artigo 24, III e Artigo 25, II, a Gestora adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Gestora é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não colaboradores ou a Colaboradores não autorizados.

3.1. Segurança da Informação Confidencial

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de *Compliance*.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Gestora.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pela área de *compliance*.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Gestora.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

O Diretor de *Compliance* também monitorará e, será avisado por *e-mail* em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O Diretor de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Gestora. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

A Gestora se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador. O Diretor de *Compliance* é encarregado de, trimestralmente, monitorar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente pelo Diretor de *Compliance*.

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com *backup*.

Em caso de divulgação indevida de qualquer informação confidencial, o Diretor de *Compliance* apurará o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

3.2. Propriedade intelectual

Todos os documentos desenvolvidos na realização das atividades da Gestora ou a elas diretamente relacionados, tais quais, sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise etc., são de propriedade intelectual da Gestora.

A utilização e divulgação de qualquer bem sujeito à propriedade intelectual da Gestora dependerá de prévia e expressa autorização por escrito do Diretor de *Compliance*.

Uma vez rompido com a Gestora o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

4. INFORMAÇÃO PRIVILEGIADA E *INSIDER TRADING*

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios da Gestora que possa influir de modo ponderável: *(a)* na rentabilidade dos valores mobiliários administrados pela Gestora; *(b)* na decisão de Investidores de comprar, vender ou manter cotas de fundos de investimento administrados pela Gestora; e *(c)* na decisão dos Investidores de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Gestora.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso do Colaborador tiver acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente ao Diretor de *Compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros membros da Gestora, profissionais de mercado, amigos e parentes, e nem a usar, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido ao Diretor de *Compliance*.

4.1. Insider Trading e "Dicas"

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo a própria Gestora e seus Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício para a compra e venda de títulos ou valores mobiliários.

É proibida a prática dos atos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da Gestora ou de terceiros.

A prática de qualquer ato em violação deste Manual de *Compliance* pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de

dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de *Compliance*, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Instrução CVM nº 358, de 03 de janeiro de 2002.

É de responsabilidade do Diretor de *Compliance* verificar e processar, periodicamente, as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas" devem ser analisados não só durante a vigência do relacionamento profissional do Colaborador com a Gestora, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

5.1. Segregação física

Todas as áreas da Gestora são segregadas, especialmente a área de gestão de recursos, sendo o acesso restrito aos Colaboradores integrantes da área, por meio de controle de acesso nas portas.

Para garantir que não exista circulação de informações que possam gerar conflito de interesses ("chinese wall"), além do controle de acesso para as diferentes áreas da Gestora, as paredes contêm isolamento acústico.

Não será permitida a circulação de Colaboradores em seções que não destinada ao respectivo Colaborador.

Reuniões com terceiros não colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não colaborador, inclusive clientes, sendo este encaminhado diretamente à devida sala.

É de competência do Diretor de *Compliance*, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções, sendo, ainda, informado imediatamente por *e-mail* se o acesso às áreas restritas for negado aos Colaboradores por mais de 5 (cinco) vezes. O Diretor de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções. Eventual infração à regra estabelecida será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pelo Diretor de *Compliance*.

A propósito, as tarefas contábeis da empresa serão terceirizadas, de modo que sejam exercidas no local de atuação das empresas contratadas.

5.2. Segregação Eletrônica

Adicionalmente, a Gestora segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais Colaboradores, sendo que haverá impressora e fax destinados exclusivamente à utilização da área de administração de recursos.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, informamos que o acesso aos arquivos/informações técnicas será restrito e controlado, sendo certo que tal restrição/segregação será feita em relação a: (i) cargo/nível hierárquico; e (ii) equipe.

Ademais, cada Colaborador possuirá um código de usuário e senha para acesso à rede, o qual é definido pelo responsável de cada área, sendo que somente os Colaboradores autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, a rede de computadores da Gestora permitirá a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Ainda, cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

5.3. Especificidades dos mecanismos de controles internos

A Gestora, por meio do Diretor de *Compliance*, mantém disponível, para todos os Colaboradores, quaisquer diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

(i) Definição de responsabilidades dentro da Gestora;

(ii) Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da empresa;

(iii) Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

(iv) Contínua avaliação dos diversos riscos associados às atividades da empresa; e

(v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Gestora estão sendo alcançados, se os limites estabelecidos e

as leis e regulamentos aplicáveis estão sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Caso qualquer Colaborador identificar situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise do Diretor de *Compliance*.

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e *softwares* sobre os quais a Gestora possua licença de uso, acesso à *internet*, bem como correio eletrônico interno e externo com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios da Gestora. A esse respeito, o Diretor de *Compliance* poderá disponibilizar a diretriz para utilização de recursos de tecnologia, detalhando todas as regras que devem ser seguidas por todo e qualquer Colaborador, independentemente do grau hierárquico dentro da Gestora.

São realizados testes mensais de segurança para os sistemas de informações utilizados pela Gestora para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

Para garantir a segurança dos sistemas de informações utilizados pela Gestora, a Gestora contrata empresa especializada na instalação, manutenção e reparação de sistemas e de toda infraestrutura utilizada pela Gestora, conforme previsto nas "Diretrizes de Segurança da Informação" anexo ao presente Manual de *Compliance* como Anexo IV.

6. DIVULGAÇÃO DE MATERIAL DE *MARKETING*

Todos os Colaboradores devem ter ciência de que a divulgação de materiais de *marketing* deve ser realizada estritamente de acordo com as regras emitidas pela CVM e pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, e que não devem conter qualquer informação falsa ou que possa levar o público a erro.

Materiais de *marketing* devem ser entendidos como qualquer nota, circular, carta ou outro tipo de comunicação escrita, destinada a pessoas externas à Gestora, ou qualquer nota ou anúncio em qualquer publicação, rádio ou televisão, que ofereça qualquer serviço de consultoria ou gestão prestado pela gestora, ou um produto de investimento da Gestora no mercado de valores mobiliários (incluindo fundos geridos).

Quaisquer materiais de *marketing* devem ser previamente submetidos ao Diretor de *Compliance*, que deverá verificar se está ou não de acordo com as várias regras aplicáveis, incluindo sem limitação a Instrução CVM nº 400, de 29 de dezembro de 2003, a Instrução CVM nº 476, de 16 de janeiro de 2009, a Instrução CVM nº 555, de 17 de dezembro de 2014 ("Instrução CVM 555"), o Código ANBIMA de Regulação e Melhores Práticas de Fundos de Investimento, e diretrizes escritas emanadas da ANBIMA. O Diretor de *Compliance* deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito do Diretor de *Compliance* é que qualquer material de *marketing* deve ser utilizado.

Abaixo encontra-se uma lista não exaustiva de regras aplicáveis a materiais de *marketing* de fundos de investimento.

Nos termos da Instrução CVM 555, qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

(i) ser consistente com o regulamento e com a lâmina, se houver;

(ii) ser elaborado em linguagem serena e moderada, advertindo seus leitores para os riscos do investimento;

(iii) ser identificado como material de divulgação;

(iv) mencionar a existência da lâmina, se houver, e do regulamento, bem como os endereços na rede mundial de computadores nos quais tais documentos podem ser obtidos;

(v) ser apresentado em conjunto com a lâmina, se houver;

(vi) conter as informações do item 12 do Anexo 42 da Instrução CVM 555, se a divulgação da lâmina não for obrigatória;

(vii) conter informações: (a) verdadeiras, completas, consistentes e não induzir o Investidor a erro; (b) escritas em linguagem simples, clara, objetiva e concisa; e (c) úteis à avaliação do investimento; e (d) que não assegurem ou sugiram a existência de garantia de resultados futuros ou não isenção de risco para o Investidor.

Informações factuais devem vir acompanhadas da indicação de suas fontes e ser diferenciadas de interpretações, opiniões, projeções e estimativas.

Qualquer divulgação de informação sobre os resultados de fundo só pode ser feita, por qualquer meio, após um período de carência de 6 (seis) meses, a partir da data da primeira emissão de cotas.

Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade do fundo, deve obrigatoriamente:

(i) mencionar a data do início de seu funcionamento;

(ii) contemplar, adicionalmente à informação divulgada, a rentabilidade mensal e a rentabilidade acumulada nos últimos 12 (doze) meses, não sendo obrigatória, neste caso, a discriminação mês a mês, ou no período decorrido desde a sua constituição, se inferior, observado que a divulgação de rentabilidade deve ser acompanhada de comparação, no mesmo período, com índice de mercado compatível com a política de investimento do fundo, se houver;

(iii) ser acompanhada do valor do patrimônio líquido médio mensal dos últimos 12 (doze) meses ou desde a sua constituição, se mais recente;

(iv) divulgar a taxa de administração e a taxa de performance, se houver, expressa no regulamento vigente nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; e

(v) destacar o público alvo do fundo e as restrições quanto à captação, de forma a ressaltar eventual impossibilidade, permanente ou temporária, de acesso ao fundo por parte de Investidores em geral.

Caso o administrador contrate os serviços de empresa de classificação de risco, deve apresentar, em todo o material de divulgação, o grau mais recente conferido ao fundo, bem como a indicação de como obter maiores informações sobre a avaliação efetuada.

Ficam incorporadas por referência, ainda, as disposições das “Diretrizes para Publicidade e Divulgação de Material Técnico de Fundos de Investimento” da ANBIMA, disponível publicamente no *website* desta instituição.

7. APROVAÇÃO DE CORRETORAS E *SOFT DOLLAR*

O Diretor de *Compliance* manterá uma lista de corretoras aprovadas com base nos critérios estabelecidos pela Gestora. O *trader* executará ordens exclusivamente com corretoras constantes referida lista, exceto se receber a autorização prévia do Diretor de *Compliance* para usar outra corretora. O Diretor de *Compliance* atualizará a lista de corretoras aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

Os custos de transação mais relevantes tais como corretagem, emolumentos e custódia, devem ser constantemente monitorados, com objetivo de serem minimizados. Semestralmente o time de gestão da Gestora deve elaborar um ranking com critérios objetivos de corretoras levando em consideração qualidade do serviço e preço, visando encontrar a melhor equação e prezando o dever fiduciário que temos para com os nossos Investidores. A Gestora somente utilizará as corretoras melhores classificadas, sendo que o fator "preço" será sempre o fator de maior relevância.

A equipe de gestão e o Diretor de *Compliance* devem rever o desempenho de cada corretora e considerar, entre outros aspectos: a qualidade das execuções fornecidas; o custo das execuções, acordos de *soft dollar* e potenciais conflitos de interesse.

7.1. Política de Soft Dollar

Quaisquer acordos envolvendo *soft dollars* devem ser previamente aprovados pelo Diretor de *Compliance*. *Soft dollars* podem ser definidos como quaisquer benefícios oferecidos por uma corretora a uma gestora que direcione ordens para a corretora, que podem incluir, sem limitação, *researches* e acesso a sistemas de informações de mercado como o *Bloomberg*.

Acordos de *soft dollar* somente poderão ser aceitos pelo Diretor de *Compliance* se quaisquer benefícios oferecidos (i) possam ser utilizados diretamente para melhorias da tomada de decisão de investimento pela Gestora; (ii) forem razoáveis em relação ao valor das comissões pagas; e (iii) não afetarem a independência da Gestora.

Os acordos de *soft dollars* não criam nenhuma obrigação para a Gestora operar exclusivamente junto às corretoras que concedem os benefícios.

Atualmente, a Gestora não possui qualquer acordo de *soft dollar*.

8. POLÍTICA DE *KNOW YOUR CLIENT* (KYC) E PREVENÇÃO À LAVAGEM DE DINHEIRO

O termo "lavagem de dinheiro" abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal, para simular uma origem legítima. A Gestora e seus Colaboradores devem obedecer a todas as regras que previnem a lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, em especial a Lei nº 9.613/1998 conforme alterada, e a Instrução CVM nº 301, de 16 de abril de 1999 ("Instrução CVM 301"), ambas refletidas neste Manual de *Compliance*.

O Diretor de *Compliance* será responsável perante a CVM pelo cumprimento de todas as normas e regulamentação vigentes relacionados ao combate e à prevenção à lavagem de dinheiro.

O Diretor de *Compliance* estabelecerá o devido treinamento dos Colaboradores da Gestora – na forma deste Manual de *Compliance* – para que estes estejam aptos a reconhecer e a combater a lavagem de dinheiro, bem como providenciará novos treinamentos, se necessários, no caso de mudanças na legislação aplicável.

A periodicidade mínima do treinamento acima referido será anual, observado que os Colaboradores poderão ser submetidos a seminários, workshops, fóruns de discussão e outros cursos de especialização, a critério do Diretor de *Compliance*, levando em consideração a exposição dos Colaboradores ao risco de lavagem de dinheiro nas suas atividades.

Os materiais, carga horária e grade horária do treinamento serão definidos pelo Diretor de *Compliance*, podendo inclusive contratar terceiros para ministrar aulas e/ou palestrantes sobre assuntos pertinentes.

O Diretor de *Compliance* deve estabelecer mecanismos de controle interno para o combate à lavagem de dinheiro e reportar certas operações à CVM e/ou ao Conselho de Controle de Atividades Financeiras, na forma do estabelecido na Instrução CVM 301, especificamente nos respectivos Artigos 7º e 7º-A. Geralmente, as obrigações contra a lavagem de dinheiro são:

(i) identificação dos clientes e dos beneficiários finais (incluindo os sócios de sociedades empresariais e seus procuradores) e manutenção dos registros atualizados dos clientes;

(ii) constituição e manutenção dos registros de envolvimento em transações;

(iii) reporte à CVM das transações que envolvam certas características específicas, ou que sejam geralmente suspeitas de lavagem de dinheiro;

(iv) identificação de pessoas politicamente expostas;

(v) verificação das relações comerciais com pessoas politicamente expostas, especialmente, propostas para o início de relações comerciais e demais operações das quais pessoas politicamente expostas sejam parte; e

(vi) estabelecimento e manutenção de regras e procedimentos de controle internos destinados à identificação da origem dos recursos utilizados nas operações cujos clientes ou beneficiários finais sejam identificados como pessoas politicamente expostas.

A Gestora adota procedimentos que permitem o monitoramento das faixas de preços dos ativos e valores mobiliários negociados para os fundos de investimento geridos pela Gestora, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas, e se for o caso, comunicados aos órgãos competentes.

Nos termos da regulamentação e ofícios circulares da CVM, bem como do *Guia de Prevenção à "Lavagem de Dinheiro" e ao Terrorismo no Mercado de Capitais Brasileiro da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais*, a responsabilidade primária pelo processo de identificação de clientes (cadastro) e dos procedimentos de *Know Your Client* em fundos de investimento, no que diz respeito aos Investidores do Fundo (passivo), cabe ao respectivo administrador fiduciário, instituição intermediária ou distribuidor, conforme o caso. Tais partes devem possuir normas e procedimentos internos referentes às atividades acima destacadas que sejam passíveis de verificação pela Gestora, especialmente no que se refere a: (i) política de prevenção à lavagem de dinheiro e financiamento do terrorismo, (ii) identificação de clientes, (iii) política de Know Your Client, (iv) monitoramento de transações, (v) inspeção de órgãos reguladores e auditorias internas, realizadas por áreas independentes, e externas, contratadas pelas instituições, (vi) comunicação de situações que possam configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613/1998, ou a eles relacionadas, entre outras verificações que a instituição julgar necessárias. Sendo assim, as regras de identificação de clientes (cadastro) e dos procedimentos de *Know Your Client* referidos nesta política não se aplicam à Gestora na qualidade de gestora de fundo de investimento, sem prejuízo da responsabilidade da Gestora pela análise, avaliação e monitoramento dos investimentos realizados pelo fundo de investimento (ativo) e suas contrapartes, nos termos aqui descritos, exceto nas seguintes hipóteses, para as quais a Gestora não está obrigada a realizar o controle de contraparte:

(i) Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM;

(ii) Ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;

(iii) Ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida;

(iv) Ativos e valores mobiliários cuja contraparte seja instituição financeira ou equiparada; e

(v) Ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (i) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (ii) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

Nas operações ativas (investimentos) realizadas pelo fundo de investimento, que não se enquadrem nas situações listadas acima, o "cliente" deve ser entendido como a contraparte da operação, sendo a Gestora responsável por tomar todas as medidas necessárias, segundo as leis aplicáveis e as regras de KYC ("conhecer seu cliente") presentes neste Manual de *Compliance* e na legislação vigente, para estabelecer e documentar a verdadeira e completa identidade, situação financeira e o histórico de cada contraparte. Estas informações devem ser obtidas de uma potencial contraparte antes que a Gestora a aceite como tal.

(i) Pessoa Física: Se a contraparte for pessoa física, a Gestora deve obter, no mínimo, as seguintes informações: *(a)* nome completo, sexo, profissão, data de nascimento, naturalidade, nacionalidade, estado civil, filiação, nome do cônjuge ou companheiro; *(b)* natureza e número do documento de identificação, nome do órgão expedidor e data de expedição; *(c)* número de inscrição no Cadastro de Pessoas Físicas ("CPF/MF"); *(d)* endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP) e número de telefone; *(e)* endereço eletrônico para correspondência; *(f)* ocupação profissional e entidade para a qual trabalha; *(g)* informações sobre os rendimentos e a situação patrimonial; *(h)* datas das atualizações do cadastro; *(i)* assinatura do cliente; *(j)* cópia dos seguintes documentos: documento de identidade e comprovante de residência ou domicílio; e *(k)* cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

(ii) Pessoa Jurídica: Se o cliente for pessoa jurídica, a Gestora deve obter, no mínimo, as seguintes informações: *(a)* a denominação ou razão social; *(b)* nomes e CPF/MF dos controladores diretos ou razão social e inscrição no Cadastro Nacional de Pessoa Jurídica

("CNPJ") dos controladores diretos; *(c)* nomes e CPF/MF dos administradores; *(d)* nomes dos procuradores; *(e)* número de CNPJ e NIRE; *(f)* endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP); *(g)* número de telefone; *(h)* endereço eletrônico para correspondência; *(i)* atividade principal desenvolvida; *(j)* faturamento médio mensal dos últimos doze meses e a situação patrimonial; *(k)* denominação ou razão social de pessoas jurídicas controladoras, controladas ou coligadas; *(l)* qualificação dos representantes ou procuradores e descrição de seus poderes; *(m)* datas das atualizações do cadastro; *(n)* assinatura do cliente; *(o)* cópia dos seguintes documentos: CNPJ, documento de constituição da pessoa jurídica devidamente atualizado e registrado no órgão competente, e atos societários que indiquem os administradores da pessoa jurídica, se for o caso; e *(p)* cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

(iii) Contrapartes no Exterior: Para operações com ativos e fundos de investimentos no exterior, deverão ser observadas as norma e preceitos da Instrução CVM 555, especialmente o Artigo 98 e seguintes.

As contrapartes devem informar a Gestora a respeito de quaisquer alterações que vierem a ocorrer nos seus dados cadastrais, conforme acima. Não obstante, os Colaboradores da Gestora deverão atualizar o cadastro de todas suas contrapartes em intervalos não superiores a 24 (vinte e quatro) meses.

A Gestora deve: (i) adotar continuamente medidas de controle que procurem confirmar as informações cadastrais de suas contrapartes, de forma a identificar os beneficiários finais das operações; (ii) identificar as pessoas consideradas politicamente expostas[1]; (iii) supervisionar

[1] Nos termos da Instrução CVM 301, *pessoa politicamente exposta* é aquela que desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo. O prazo de 5 (cinco) anos deve ser contado, retroativamente, a partir da data de início da relação de negócio ou da data em que o cliente passou a se enquadrar como pessoa politicamente exposta. No Brasil, são consideradas *pessoas politicamente expostas*: (i) os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União; (ii) os ocupantes de cargo, no Poder Executivo da União: (a) de Ministro de Estado ou equiparado; (b) de natureza especial ou equivalente; (c) de Presidente, Vice-Presidente e diretor, ou equivalentes, de autarquias, fundações públicas, empresas públicas ou sociedades de economia mista; ou (d) do grupo direção e assessoramento superiores - DAS, nível 6, e equivalentes; (iii) os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal e dos tribunais superiores; (iv) os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal; (v) os membros do Tribunal de Contas da União e o Procurador-Geral do Ministério Público junto ao Tribunal de Contas da União; (vi) os Governadores de Estado e do Distrito Federal, os Presidentes de Tribunal de Justiça, de Assembleia Legislativa e de Câmara Distrital e os Presidentes de Tribunal e de Conselho de Contas de Estados, de Municípios e do Distrito Federal; e (vii) os Prefeitos e Presidentes de Câmara Municipal de capitais de Estados. Considera-se (i) *cargo*: emprego ou função pública relevante exercido por chefes de estado e de governo, políticos de alto nível, altos servidores dos poderes públicos, magistrados ou militares de alto nível, dirigentes de empresas públicas ou dirigentes de partidos políticos; e (ii) *familiares da pessoa politicamente exposta*: seus parentes, na linha direta, até o primeiro grau, assim como o cônjuge, companheiro e enteado.

de maneira mais rigorosa a relação de negócio mantida com pessoa politicamente exposta; e (iv) dedicar especial atenção a propostas de início de relacionamento e a operações executadas com pessoas politicamente expostas oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política.

Se algum Colaborador perceber ou suspeitar da prática de atos relacionados à lavagem de dinheiro ou outras atividades ilegais por parte de qualquer cliente, este deverá imediatamente reportar suas suspeitas ao Diretor de *Compliance*. O Diretor de *Compliance* deverá, então, instituir investigações adicionais, para determinar se as autoridades relevantes devem ser informadas sobre as atividades em questão. Entre outras possibilidades, uma atividade pode ser considerada suspeita se:

(i) operações cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial ou financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas;

(ii) operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;

(iii) operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;

(iv) operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;

(v) operações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;

(vi) operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);

(vii) operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;

(viii) operações com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;

(ix) operações liquidadas em espécie, se e quando permitido;

(x) transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;

(xi) operações cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do cliente ou de seu representante;

(xii) depósitos ou transferências realizadas por terceiros, para a liquidação de operações de cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;

(xiii) pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do cliente;

(xiv) situações em que não seja possível manter atualizadas as informações cadastrais de seus clientes;

(xv) situações e operações em que não seja possível identificar o beneficiário final; e

(xvi) situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas.

A Gestora deverá dispensar especial atenção às operações em que participem as seguintes categorias de clientes:

(i) clientes não-residentes, especialmente quando constituídos sob a forma de *trusts* e sociedades com títulos ao portador;

(ii) clientes com grandes fortunas geridas por áreas de instituições financeiras voltadas para clientes com este perfil (*private banking*); e

(iii) pessoas politicamente expostas.

A Gestora deverá analisar as operações em conjunto com outras operações conexas e que possam fazer parte de um mesmo grupo de operações ou guardar qualquer tipo de relação entre si.

Os Colaboradores não devem divulgar suas suspeitas ou descobertas em relação a qualquer atividade, para pessoas que não sejam o Diretor de *Compliance*. Qualquer contato entre a Gestora e a autoridade relevante sobre atividades suspeitas deve ser feita somente pelo Diretor de *Compliance*. Os Colaboradores devem cooperar com o Diretor de *Compliance* durante a investigação de quaisquer atividades suspeitas.

A Gestora deve manter atualizados os livros e registros, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pela CVM, na hipótese de existência de processo administrativo.

O Diretor de *Compliance* deve assegurar que a Gestora previna qualquer danificação, falsificação, destruição ou alteração indevida dos livros e registros por meio de adoção de métodos necessários e prudentes.

Consideram-se operações relacionadas com terrorismo ou seu financiamento aquelas executadas por pessoas que praticam ou planejam praticar atos terroristas, que neles participam ou facilitam sua prática, bem como por entidades pertencentes ou controladas, direta ou indiretamente, por tais pessoas e as pessoas ou entidades que atuem sob seu comando.

9. PLANO DE CONTINUIDADE DO NEGÓCIO

É necessário que exista um plano de continuidade de negócios que assegure a continuidade ou a rápida retomada das atividades em caso de falhas ou interrupções dos negócios. O plano de contingência e continuidade de negócios deve identificar, monitorar e acompanhar suas atividades chaves a fim de assegurar que as operações da Gestora sejam rapidamente retomadas em caso de incidentes graves, conforme previsto no "Plano de Continuidade dos Negócios", cuja cópia consta anexa ao presente como Anexo V.

Como previsto no Plano de Continuidade dos Negócios, anexo, a Gestora possui site de contingência em local afastado de sua sede, com acesso a todos os sistemas necessários para a plena continuidade dos trabalhos, além disso, também é prevista a possibilidade de acesso a todos os sistemas e programas essenciais à atividade da Gestora em qualquer lugar com acesso à internet, por meio de VPN (Virtual Private Network).

ANEXO I - Modelo de Relatório Anual de Compliance

São Paulo, _____ de janeiro de _____.

Aos diretores,

Ref.: Relatório Anual de *Compliance*

Prezados,

Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos da **MILES CAPITAL LTDA.** ("Gestora"), nos termos do Manual de Controles Internos *(compliance)* da Gestora ("Manual de *Compliance*"), e do Artigo 22 da Instrução nº 558, de 26 de março de 2015, da Comissão de Valores Mobiliários ("Instrução CVM 558"), e na qualidade de diretor responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos e controles internos constantes do Manual de *Compliance* e da Instrução CVM 558, informo o quanto segue a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20[--].

Por favor, encontrem abaixo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de deficiências e cronogramas de saneamento; e (iii) minha manifestação, na qualidade de responsável por ajustar a exposição a risco das carteiras da Gestora, assim como pelo efetivo cumprimento da "Política de Gestão de Riscos" da Gestora, a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las.

I. Conclusão dos Exames Efetuados:

[●]

II. Recomendações e Cronogramas de Saneamento

[●]

III. Manifestação sobre Verificações Anteriores

[●]

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

_____

Otávio Mendonça Barros
Diretor de Compliance e Risco

ANEXO II - Termo de Adesão

Eu, ..., portador da Cédula de Identidade nº ..... e/ou Carteira de Trabalho e Previdência Social nº ..... série ....., declaro para os devidos fins que:

1. Estou ciente da existência do "Manual de Controles Internos *(Compliance)*" da **MILES CAPITAL LTDA.** ("Manual de *Compliance*" e "Gestora", respectivamente) e de todas as políticas internas da Gestora, inclusive o "Código de Ética", a "Política de Investimento Pessoal" e a "Política de Gestão de Risco" ("Políticas Internas"), que recebi, li e tenho em meu poder.
2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, do qual declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pela Gestora, e comprometo-me a comunicar, imediatamente, aos sócios-administradores da Gestora qualquer quebra de conduta ética das regras e procedimentos, que venha a ser de meu conhecimento, seja diretamente ou por terceiros.
3. Tenho ciência e comprometo-me a observar integralmente os termos da política de confidencialidade estabelecida no Manual de *Compliance* da Gestora, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.
4. O não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos pela Gestora e/ou os respectivos sócios e administradores, oriundos do não-cumprimento do Manual de *Compliance* e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal.
5. Participei do processo de integração e treinamento inicial da Gestora, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Gestora, notadamente aquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado.
6. As normas estipuladas no Manual de *Compliance* e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada pela Gestora, mas servem de complemento e esclarecem como lidar em determinadas situações relacionadas à minha atividade profissional.
7. Autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei a Gestora a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra.

8. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Manual de *Compliance*, salvo conflitos decorrentes de participações em outras empresas, descritos na "Política de Investimento Pessoal", os quais tenho ciência que deverão ser especificados nos termos previstos no Manual de *Compliance*:

_____

_____

_____

_____

_____

_____

_____

_____

_____

São Paulo, ... de ..... de 20..... .

_____

[DECLARANTE]

ANEXO III - Solicitação para Desempenho de Atividade Externa

1. Nome da instituição na qual será realizada a Atividade Externa / descrição da Atividade Externa:_____
_____
_____.

2. Você terá uma posição de diretor ou administrador? [ ] sim [ ] não

3. Descreva suas responsabilidades decorrentes da Atividade Externa:_____
_____
_____.

4. Tempo estimado que será requerido de você para desempenho da Atividade Externa (em bases anuais):
_____.

5. Você ou qualquer parte relacionada irá receber qualquer remuneração ou contraprestação pela Atividade Externa: [ ] sim [ ] não
Se sim, descreva:_____.

O Colaborador declara que a Atividade Externa que pretende desempenhar, conforme acima descrita, não viola nenhuma lei ou regulamentação aplicável, ou os manuais e códigos da **MILES CAPITAL LTDA.** ("Gestora"), e que não interfere com suas atividades na Gestora, não compete ou conflita com quaisquer interesses da Gestora. O Colaborador declara e garante, ainda, que irá comunicar ao diretor de *compliance* da Gestora quaisquer conflitos de interesses que possam surgir com relação à Atividade Externa acima descrita.

São Paulo, _____ de _____ de 20_____

_____
Assinatura do Colaborador

Resposta do Diretor de *Compliance:*

[ ] Solicitação Aceita [ ] Solicitação Negada

_____
Otávio Mendonça Barros
Diretor de *Compliance*

ANEXO IV – Diretrizes de Segurança da Informação

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Sumário Executivo

Este documento têm o objetivo de estabelecer normas, critérios e responsabilidades sobre a segurança da informação da Rede Corporativa da **MILES CAPITAL**, garantindo à mesma confidencialidade, integridade e disponibilidade.

Os itens considerados como fazendo parte do escopo em termos de Segurança da Informação são os seguintes:

- Controle e classificação dos ativos;
- Segurança pessoal;
- Segurança física;
- Controle de acesso às informações;
- Desenvolvimento e manutenção de sistemas;
- Gerenciamento da continuidade dos negócios;
- Conformidade.

Esta norma se aplica à todos os usuários da rede corporativa da **MILES CAPITAL**.

* As informações contidas neste documento ou nos documentos a ele anexados são de uso exclusivo da **MILES,** durante a vigência do contrato de governança de TI, e devem ser tratadas com restrição de distribuição dentro da empresa.

A **MILES CAPITAL** reconhece que este documento é parte integrante da metodologia **Tecnoqualify** e que o mesmo não deve ser divulgado ou distribuído para pessoas fora da **MILES CAPITAL**, sem a devida autorização por escrito da **Tecnoqualify**.

Índice

Normas

Disposições Gerais

Os sistemas de informação, a infra-estrutura tecnológica, os arquivos de dados e as informações internas ou externas, são considerados importantes ativos da empresa, em função da **MILES CAPITAL** apresentar suas operações, dependentes em grande parte da tecnologia para conduzir seus negócios e atender às suas necessidades comerciais e estratégicas.

É necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e também que todos os usuários da informação compartilhem da responsabilidade pelos processos de segurança definidos neste normativo, com a finalidade de se equiparar às boas práticas das organizações globais.

As normas de segurança da informação estabelecem objetivos, funções, ações, mecanismos de delegação e responsabilidades pelos processos, manipulação da informação e controles internos.

Os processos de segurança da informação devem assegurar a integridade, a disponibilidade e a confidencialidade dos ativos de informação da **MILES CAPITAL**.

- As normas de segurança da informação devem:
    - Proteger os ativos da **MILES CAPITAL** contra ameaças, internas ou externas, intencionais ou acidentais;
    - Limitar a um nível aceitável a exposição a perdas ou danos que possam resultar em falhas de segurança;
    - Minimizar as ameaças potenciais à segurança das informações, garantindo a manutenção da integridade, disponibilidade e confidencialidade;
    - Assegurar que os recursos adequados estarão disponíveis para implementar e manter um programa de segurança efetivo;
    - Conscientizar os associados e usuários da informação, sobre aspectos relacionados à segurança das informações.

Uso da Informação

Aplicam-se as seguintes atribuições aos usuários da informação:

- O proprietário é responsável pela geração, exatidão e classificação das informações;
- O gestor é responsável pela gerência das informações e pela definição dos direitos de acesso às mesmas;
- O custodiante é responsável pela guarda e disponibilidade das informações;
- O usuário é responsável pelo uso adequado das informações e seus ativos a que tenha acesso.

Responsabilidades

- Da Diretoria:
    - Direcionar os esforços e recursos propostos para a segurança da informação, de acordo com a estratégia de negócios da empresa;
    - Aprovar as normas de segurança da informação e suas atualizações;
    - Aprovar os controles a serem utilizados para garantir a segurança das informações;
    - Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI;
    - Comunicar o responsável por *Compliance* os casos de violações à Norma de Segurança da Informação para as providências necessárias;
    - Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados;
    - Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação;
    - Delegar as funções de segurança da informação aos profissionais responsáveis.

- Da Empresa Prestadora de Serviços de TI:
    - Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;
    - Orientar os testes da infra-estrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;
    - Assessorar as demais áreas da empresa no processo de classificação das informações;

- Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;
- Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;
- Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;
- Manter a infraestrutura que suporta o ambiente controlado;
- Manter a infraestrutura e sistemas atualizados;
- Garantir a implementação e operação dos indicadores de segurança;
- Notificar imediatamente os incidentes de segurança à diretoria;
- Garantir a rápida tomada de ações em caso de incidentes de segurança.

♦ Do responsável por Compliance

- Desenvolver, manter e implementar programas de treinamento e de conscientização aos colaboradores com vínculo empregatício com a empresa e colaboradores prestadores de serviço, sobre a Norma de Segurança da Informação, a forma como ela está estruturada e os principais conceitos de segurança da informação;
- Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação, juntamente com os gestores dos envolvidos;
- Emitir o Termo de Compromisso, conforme modelo do Manual de Ética e *Compliance* e garantir a ciência deste entre todos os colaboradores;
- Gerenciar a assinatura do Acordo de Confidencialidade quando da contratação de terceiros ou prestadores de serviços, conforme modelo do Manual de Ética e *Compliance*;
- Em conjunto com os demais membros do Comitê de *Compliance*, determinar as sanções cabíveis de acordo com a legislação em vigor.

♦ Dos Auditores Independentes:

- Garantir, mediante verificações de conformidade, que a **MILES CAPITAL** esteja operando de acordo com os princípios e controles estabelecidos na Norma de Segurança da Informação;
- Emitir pareceres para a Diretoria da **MILES CAPITAL**;

- Revisar periodicamente a Norma de Segurança da Informação e sugerir as alterações necessárias.

Itens Abordados pela Segurança da Informação

Controle e Classificação dos Ativos

Este tópico visa assegurar que todos os ativos, físicos ou lógicos, estejam identificados, classificados e que sejam controlados.

- Todos os ativos da **MILES CAPITAL**, sejam estes físicos ou lógicos, devem ser adequadamente controlados pela administração. Os ativos devem ser protegidos de acordo com o grau de criticidade que representam para o negócio da **MILES CAPITAL**;
- É necessário que todos os ativos sejam classificados de acordo com os critérios definidos pela Diretoria da **MILES**;
    - Com base nessa classificação, devem ser adotados controles que garantam as três propriedades básicas desses ativos: integridade, disponibilidade e confidencialidade, em um nível proporcional à criticidade que representam para o negócio da **MILES CAPITAL**.
- Em caso de dúvida, nenhuma informação deve ser divulgada.

Segurança de Pessoal

Neste caso, a norma visa assegurar que todos os usuários da informação tenham conhecimento dos requisitos e das obrigações definidos pela Norma de Segurança da Informação, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos, e de falhas no processo de conscientização sobre segurança.

- Todos os usuários da informação e clientes devem conhecer e adotar as definições de segurança da informação instituídas pela **MILES CAPITAL** e suas responsabilidades na manutenção da segurança corporativa;
- Os usuários da informação devem ser orientados sobre os procedimentos e o uso correto dos recursos de processamento das informações, por meio de treinamentos, de forma a minimizar possíveis riscos de segurança.

Segurança Física

Em termos de segurança física, a norma deve definir os requisitos mínimos de segurança física que os ambientes considerados críticos, onde há informações sigilosas da **MILES CAPITAL**, devem possuir para assegurar a proteção de seus ativos contra fatores que possam causar interrupção das atividades, alteração ou vazamento das informações e consequente prejuízo financeiro.

- Todas as áreas classificadas como críticas na **MILES CAPITAL** devem estar protegidas por controles físicos apropriados;
    - Esses controles devem ser proporcionais à criticidade dos equipamentos, dos sistemas e das informações mantidas e manuseadas nestas áreas.
- As áreas classificadas como críticas devem estar devidamente protegidas por acesso não autorizado, dano ou interferência.

Controle de Acesso à informações

O controle de acesso às informações deve definir os requisitos necessários para que o usuário da informação obtenha acesso ao ambiente de tecnologia da **MILES CAPITAL**.

- O acesso a todos os sistemas e informações da **MILES CAPITAL** deve ser concedido de acordo com as necessidades da função do usuário para a execução de suas atividades;
- O responsável pelos sistemas ou da informação é o responsável pela concessão de acesso a todos os recursos que estejam sob sua responsabilidade. Os acessos concedidos deverão ser periodicamente revisados;
- Os usuários devem se restringir às informações e ambientes aos quais estão autorizados, devendo acessá-los somente se houver a necessidade para desempenho de suas atividades profissionais.

Desenvolvimento e Manutenção de Sistemas

Este item enumera os requisitos de segurança para desenvolvimento, manutenção e parametrização de sistemas.

- Todos os sistemas desenvolvidos pela **MILES CAPITAL** ou por empresas contratadas por esta, deverão atender aos requisitos de segurança definidos pela Norma de Segurança da Informação.

Gerenciamento da Continuidade dos Negócios

A Norma de Gerenciamento da Continuidade dos Negócios deve identificar atividades chaves que compõem um Plano de Continuidade de Negócios, a fim de assegurar que as operações da **MILES CAPITAL** sejam rapidamente retomadas em caso de incidentes graves.

- É necessário que exista um Plano de Continuidade de Negócios que assegure a continuidade ou a rápida retomada das atividades em caso de falhas ou interrupções dos negócios;
    - O Plano de Continuidade de Negócios deve incluir os processos, procedimentos e alternativas para recuperação de qualquer interrupção do negócio, independentemente do agente causador, além da proteção dos processos críticos da **MILES CAPITAL** contra efeitos de desastres significativos.

Conformidade

A Norma de Conformidade deve definir as ações necessárias para que a **MILES CAPITAL** não viole nenhuma lei civil ou criminal, estatutos, regulamentações ou obrigações contratuais referentes a quaisquer requisitos de segurança.

- A empresa deve estar em conformidade com todas as regras e regulamentos instituídos por lei. Isto inclui qualquer lei civil ou criminal, estatutos ou obrigações contratuais feitas envolvendo a **MILES CAPITAL**;
- É responsabilidade de todos os usuários de informações auxiliar na manutenção dos requisitos de segurança e nos regulamentos ditados por lei.

Controle do Documento

Esta seção do documento têm o objetivo de:

- Controlar as alterações realizadas no documento, através do estabelecimento de um controle de versões;
- Relacionar os responsáveis pelo controle, confecção e aprovação do documento;
- Estabelecer as diretrizes para atualização do documento;
- Definir como o documento deve ser distribuído.

Resumo das Atualizações

Versão	Data Publicação	Resumo	Nº da Revisão
1.0	05/2017	Versão Inicial	-

Responsáveis

Responsabilidade	Responsável	E-mail
Criador	Cleber Campos	cleber@tecnoqualify.com.br
Revisor	Clayton Campos	clayton@tecnoqualify.com.br
Aprovador		

Plano para Revisão do Documento

Este documento deverá ser revisto e atualizado, quando ocorrer qualquer uma das seguintes premissas:

- Quando necessário, para corrigir ou incluir informações;
- Quando ocorrerem mudanças organizacionais significativas e que afetem diretamente o processo definido;
- Após 6 meses da data de sua publicação, para efeito de melhoria contínua.

Sempre que ocorrer uma revisão do documento sua versão será alterada, conforme o seguinte critério:

- Alterações pouco significativas: Será mantido o número principal de versão e será alterada a númeração secundária de versão. (Exemplo: versão 1.1, 1.2, 1.3 ... 1.n)
- Alterações significativas ou revisões semestrais: Será alterado o número principal da versão para o número seguinte de numeração, começando sempre com o número secundário em 0. (Exemplo: versão, 2.0, 3.0, 4.0 ... n.0)

Distribuição do Documento

Este documento será distribuído eletrônicamente para todos os usuários da **MILES CAPITAL**, sempre que necessário.

Existirá uma versão impressa do documento, que estará organizada em uma pasta de documentação e que ficará disponível para consulta dos envolvidos, no processo da **MILES CAPITAL**.

Quando ocorrerem revisões ou atualizações no documento, todos os envolvidos e os aprovadores receberão uma nova versão eletrônica. Uma nova versão impressa substituirá a versão anterior existente na **MILES CAPITAL** e todas as versões anteriores deverão ser descartadas.

O Aprovador do documento é o responsável pela distribuição do mesmo na **MILES CAPITAL.**

ANEXO V – Plano de Contingências e Continuidade dos Negócios

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

Sumário

B.1 –Plano de Contingência e Continuidade dos Negócios

B.1.1 – Introdução ao BCP

O objetivo do Plano de Contingência e Continuidade dos Negócios ("BCP") é possibilitar que a Miles Capital Ltda. ("MILES") continue com as suas operações e serviços essenciais mesmo nos cenários de crise.

O presente documento define os procedimentos que deverão ser seguidos pela MILES, no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da MILES sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da MILES dentro do contexto de seu negócio.

B.1.1.1 – Cenários de Crise

A *Alternative Investment Managment Association* (AIMA) lista em seu documento "*Business Continuity Management for Hedge Fund Managers – version June 2012*" 24 possíveis cenários de crise:

1. Explosão em uma grande área;	2. Fogo;	3. Falta localizada de energia;
4. Explosão localizada;	5. Inundação;	6. Falha de circuito / terminal;
7. Explosão na vizinhança;	8. Pandemia;	9. Falha de hardware;
10. Bomba radiológica;	11. Clima extremo;	12. Virus / hackers;
13. Guerra ou insurreição civil;	14. Interrupção de transportes;	15. Roubo / sabotagem;
16. Alerta de segurança;	17. Acidentes (dentro ou fora do escritório);	18. Falha no sinal de telecom (internet e/ou voz);
19. Vazamento de gás;	20. Eletrocução;	21. Falha no hardware de telecom e
22. Terremoto;	23. Falta geral de energia (apagão);	24. Falha na rede de celular

Uma vez que ocorra algum incidente parecido com estes 24 cenários ou algo que chame a atenção do colaborador, o líder do BCP – que é o Compliance Officer ou na ausência deste o seu back-up – deverá ser imediatamente comunicado. (Ver B.1.4 – lista de contatos de emergência)

B.1.1.2 – Desdobramentos

A lista de cenários apresentadas em B.1.1.1 não tem a pretensão de ser definitiva. Além disto, cenários de crise são por definição imprevisíveis. No entanto os cenários acima geralmente levam a combinação de um ou mais dos desdobramentos abaixo:

1. **Perda de Acesso ao Prédio:** significa que todos os colaboradores e contratados da MILES que estiverem no prédio no momento do incidente deverão evacuá-lo e quem estiver fora não poderá entrar.

2. **Perda de Pessoal:** afeta o *staff* e prestadores de serviços da MILES. Inclui ferimentos, doenças, morte e incapacidade de chegar no escritório (ou potencialmente trabalhar de casa).

3. **Perda de Infraestrutura de TI: i**nclui falha parcial ou completa da rede de TI, incluindo hardware e softwares essenciais. O fator-chave é envolver os prestadores de serviços assim que possível para instaurar os sistemas de *back-up*.

4. **Perda de Infraestrutura de Telecom: i**nclui falha parcial ou completa da rede de telecomunicações, incluindo equipamentos, telefones fixos, celulares e a internet).

5. **Perda de Energia Elétrica:** Falta de energia devido a apagões ou interrupção da rede elétrica devido a chuvas e/ou quedas de árvores.

B.1.2 – Gestão da Crise, Recuperação e Retomada

Uma vez que o líder do BCP foi acionado devido a uma potencial crise, caso seja possível ele convocará (pessoalmente ou via *call-tree*) os colaboradores-chave da MILES para formar o comitê de crise e avaliar conjuntamente a situação e próximos passos.

Na impossibilidade de decisão em conjunto - devido a situação onde a pressão é extrema - o líder do BCP poderá tomar decisões sozinho sobre os próximos passos para gerenciar a crise.

Existem geralmente três etapas a serem percorridas após a ocorrência de um evento:

1. **Gestão da Crise;**
2. **Recuperação e**
3. **Retomada**

B.1.2.1 - Gestão da Crise

1. **Etapa Inicial:** engloba vários aspectos e decisões fundamentais a serem tomados imediatamente após o incidente:
   - 1.1. Avaliação dos impactos: o foco da reunião do time de crise deve ser em
     - 1.1.1. Entender o que aconteceu;
     - 1.1.2. Quais são as consequências imediatas e gravidade da situação;
     - 1.1.3. Como manter o staff a salvo e
     - 1.1.4. O que nós devemos fazer AGORA e decidir pela formalização ou não da CRISE (Em caso afirmativo os próximos passos são seguidos)
   - 1.2. Comunicação ao restante dos colaboradores
   - 1.3. Evacuação do prédio coordenada em conjunto com a administração predial;
   - 1.4. Acionar assistência médica imediata se necessário;
   - 1.5. Notificação dos serviços de emergência (bombeiros, polícia, SAMU) se necessário;
   - 1.6. Condução de chamada para ver os membros do staff e visitantes presentes;
   - 1.7. Retomada da reunião do comitê de crise;
   - 1.8. Realocação do staff:
     - 1.8.1. Quem vai para casa e quem vai para o site de contingência;
     - 1.8.2. Combinar como serão as próximas comunicações (telefone, WhatsApp)
   - 1.9. Notificação de parceiros-chave estratégicos: prestadores de serviços de TI e Telecom (Tecnoqualify); prime broker (CS) e administrador do fundo (CSHG).

Tomar cuidado para manter a consistência da comunicação ao informar terceiros. Apenas os colaboradores autorizados a falar em nome da empresa deverão fazer isto (ver lista de autorizados no Manual de Compliance).

   - 1.10. Iniciar a redundância de TI (caso seja aplicável) em conjunto com a Tecnoqualify e
   - 1.11. Redirecionamento das linhas de telefone para os celulares (caso seja aplicável)

2. Recuperação de Desastre – TI

Após determinar a necessidade ou não de redundância de TI, o comitê de crise deverá atuar em conjunto com a Tecnoqualify para garantir que qualquer aplicativo e hardware críticos continuem a operar via redundância/back-up. Isto inclui:

- acesso ao servidor de e-mails;
- acesso aos principais servidores (aplicativos e arquivos)
- acesso remoto aos sistemas.

3. Telecom

Caso a redundância de telecom seja necessária, o provedor deve ser instruído a desviar linhas de dados/e-mail.

4. Comunicação Externa

A gestão de relacionamentos externos durante uma interrupção das atividades normais é crítica para o curto e médio prazo da MILES. No curto prazo os prestadores de serviços críticos devem ser avisados para que eles adaptem os seus processos para a nova circunstância. No longo prazo, prover uma comunicação clara, pontual e consistente a clientes, distribuidores e contrapartes fortalece a confiança na organização

O comitê de Crise produzirá um script padrão para comunicar interna e externamente (demais prestadores de serviços, clientes, dentre outros). É muito importante que a comunicação externa seja consistente uma vez que confusão poderá resultar em perda de confiança.

Caso algum colaborador (que não esteja autorizado a falar em nome da empresa) seja questionado por terceiros, o colaborador deverá direcionar o terceiro para alguém que esteja autorizado.

B.1.2.2 – Recuperação

A fase de recuperação começa após a crise inicial ter sido contornada, ou seja, o staff já foi recolocado, a redundância de TI acionada e terceiros-chave notificados.

A fase de recuperação é composta das subfases a seguir:

1. **Comunicação Interna**: *call* diário de acompanhamento do comitê de Crise e outro *call* com os demais membros da MILES. Ambos devem ser minutados pelo líder do BCP e conter os *action points* (atividade/dono/deadline);
2. **Ações Iniciais de Recuperação**:

2.1. Comitê de Riscos e Compliance: deverá se reunir assim que possível para avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações;
2.2. Comitê de Investimentos: o CIO e o CRO devem juntamente convocar uma reunião para verificar se todas as informações necessárias ao portfólio estão seguras. Dados faltando ou corrompidos devem ser comunicados ao comitê de crise. O time de Gestão e o CRO devem decidir se decisões de investimento são requeridas embora o *trading* discricionário deva ser minimizado de acordo com as novas condições operacionais da empresa.
2.3. Operações (*Middle* Office): este time deverá continuar a manter informados o administrador do fundo, prime brokers e outros contrapartes operacionais-chave.

3. **Cobertura de funções críticas**: todas as áreas funcionais deverão ter previamente identificado as suas atividades críticas e o seu pessoal-chave necessário. Estas funções deverão ser conduzidas com qualquer problema sendo escalado ao comitê de crise.
4. **Data Management**:
   4.1. Migração dos trabalhos conduzidos externamente durante a crise para os sistemas essenciais (ou back-up)
   4.2. Back-up de dados em ambiente de Recuperação
5. **Comunicação Externa:** stakeholders-chave externos devem ser atualizados regularmente.
6. **Cenários de Retificação/ Contingência**
   6.1. Acesso ao prédio: no caso de o prédio ter sido evacuado, ou o acesso a ele estar negado, é provável que documentos ou hardware importantes estejam dentro
   6.2. Buscar acomodação alternativa: no caso de o prédio ter sido gravemente danificado ou destruído e a reocupação não seja possível a médio prazo (ou nunca mais).

B.1.2.3 – Retomada

A terceira fase é a transição entre estar trabalhando em "modo recuperação" para voltar ao modo normal (*business as usual*). Deve ser tratada – e gerida – como um projeto incluindo atividades, *checklists* e gráficos de Gantt com uma clara linha do tempo.

Os temas cobertos por esta fase são dependentes do evento ocorrido mas podem incluir:

- Como a organização volta a estar em *compliance* novamente?
- Algum sistema necessita ser reconstruído?

- A empresa irá mudar para um novo escritório?

B.1.3 – Redundâncias e Contingências

Em caso de eventos de crise, a MILES possui contingências e redundâncias de forma a permitir a continuação de suas atividades mesmo em condições adversas.

B.1.3.1 – Redundância de TI / Back-up de Arquivos

Backup Server: O servidor possui software de backup (backup Windows 2016 e Ibackup), responsável pela realização de backup predefinido pela política da MILES.

A MILES disponibiliza em seus servidores o serviço de backup e restore de arquivos, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

Os Backups são feitos através da ferramenta de backup do Windows 2016 Server e Ibakcup e são salvos em disco externo e cloud com agenda diária das pastas de dados de toda a empresa, devendo ser usado em casos em que não é mais possível a recuperação do arquivo danificado ou perdido.

O serviço de e-mail da MILES é garantido por parceiro *Microsoft* que provém suporte 24/7, serviço de anti spam, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A MILES possibilita o acesso remoto de todas as mensagens pelos colaboradores.
O serviço de e-mail da MILES é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, Antivirus (software) é ativado em cada computador individual na rede de escritório.

B.1.3.2 – Redundância de Infraestrutura (Telecom, Internet e Energia)

Telefonia
A MILES conta com 03 tipos de links de Telefone sendo 10 linhas VOIP e 2 linhas analógicas. Em caso de falhas nas linhas telefônicas, os colaboradores da MILES ainda possuem celulares que podem substituir a telefonia fixa.

Internet
O acesso à internet é disponibilizado por 3 links de velocidade de 50 mbps no link da VIVO Fibra Speedy, 10 mbps link Mundivox, e de 120 mbps link NET Virtua.

Energia

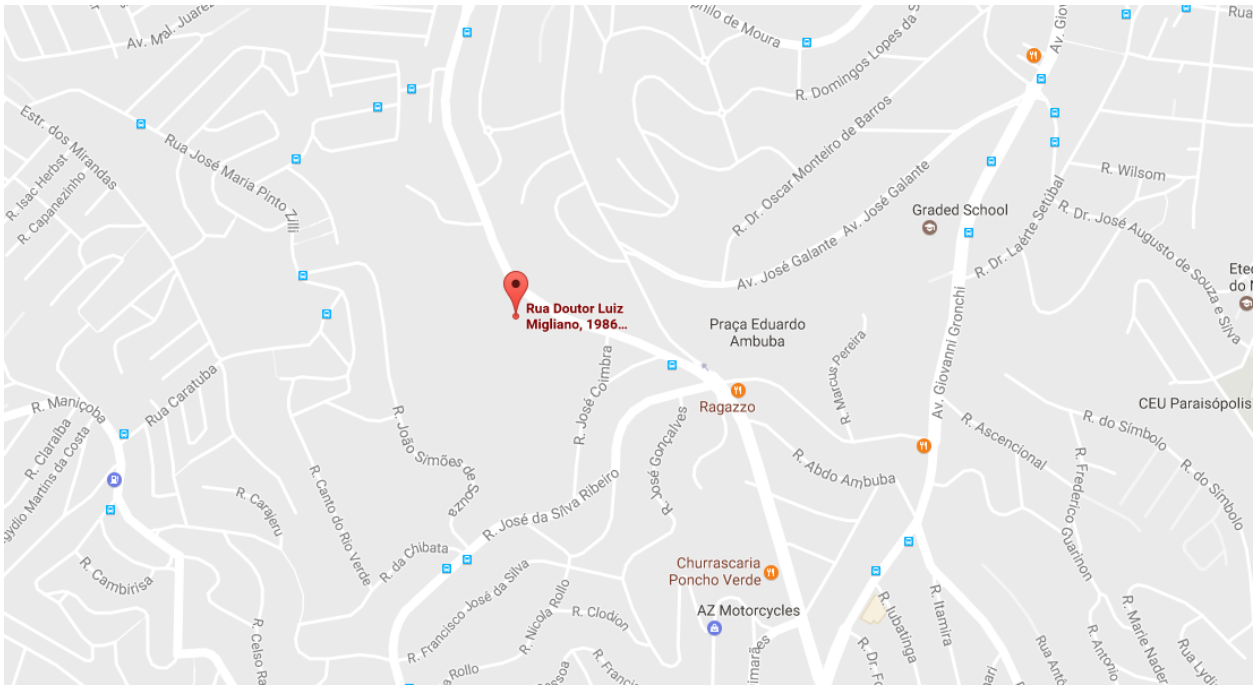
Em caso de falha de fornecimento de energia, a MILES possui nobreak para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de 2 estações de trabalho (desktops) para a efetiva continuidade dos negócios durante 5 horas. Após este período caso não retorne a energia a equipe será deslocada para o site backup.

Teste de *nobreak* realizado duas vezes por ano. Log de segurança analisado a cada visita técnica. Teste de restore realizado uma vez por mês.

B.1.3.3 – Site de Contingência e Home-Office

O escritório da MILES encontra-se na Rua Joaquim Floriano, 1052, 1 andar, sala 11, Itaim. Em caso da perda de acesso a este edifício, os colaboradores poderão: (a) acessar o site de contingência ou (b) trabalhar de casa com acesso VPN (*home-office*).

O site de contingência é o escritório do prestador de serviços (Tecnoqualify) cujo endereço é:
Rua Dr. Luiz Migliano, 1986 - 10 andar - São Paulo - SP
São Paulo/SP - CEP: 05711-001



O site de contingência fica a cerca de 8 km da sede da MILES e pode ser acessado através de grandes vias como a Marginal Pinheiros. Em tráfego normal, pode-se chegar em 30 minutos.

No site de contingência, a MILES possui 03 Desktops dedicados e devidamente autorizados. Estes desktops possuem a "software-padrão" dos aplicativos essenciais da MILES para operação e sistemas (EZE e Sirsan).

A MILES também conta com acesso remoto via VPN à sua rede de dados e alguns aplicativos para os colaboradores que optarem pelo *home-office*. Tal acesso encontra-se disponível a todos os colaboradores autorizados pelo Compliance Officer.

Os aplicativos essenciais da MILES estão listados abaixo bem como os a disponibilidade de acesso no site de contingência e no home-office via VPN:

Aplicativo	Site de Contingência	Home-Office (acesso VPN)
Email Outlook	✓	✓
Sophos Antivirus	✓	✓
Base de Dados	✓	✓
Bloomberg	✓ O software está instalado nos desktops de contingência. Basta acessar via *token* da Bloomberg o serviço. (Item B.1.4 – Lista de Contatos de Emergência)	✓

As informações dos portfólios além de estarem nos sistemas internos da MILES são disponibilizadas diariamente pelo administrador, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos.

B.1.4 – Lista de Contatos de Emergência

A MILES desenvolveu uma lista de Contatos de Emergência que inclui os nomes, telefones, endereços de e-mail dentre outras informações críticas para o negócio. Esta lista inclui colaboradores-chave, distribuidores de fundos, clientes de carteiras administradas, contrapartes prestadores de serviços essenciais dentre outros contatos. Esta lista será revista e atualizada ao menos anualmente.

Nome	Empresa /Função	Telefone	Celular	E-mail

Colaboradores

João Siqueira	MILES (líder BCP)		11 95961 0174	joao.siqueira@milescapital.com.br
Fabiano Custodio	MILES (back-up BCP)		11 99627 9581	fabiano.custodio@milescapital.com.br

Prestadores de Serviços / Contrapartes

	Contador			
	Bloomberg - representative			
	Bloomberg - help desk			
Clayton Campos	MILES (Suporte TI)		11 98244 7988	clayton@tecnoqualify.com.br

Reguladores

	CVM			
	ANBIMA			

Utilidade Pública

Polícia				
SAMU				
Bombeiros				

B.1.5 – Revisão Anual, Atualização, Treinamento e Testes

B.1.5.1 – Revisão Anual e Atualização

O BCP deverá ser revisado anualmente e atualizado sempre que for necessário. Cada revisão deverá ser aprovada pelo Diretor de Compliance (*Compliance Officer*) e as cópias do plano revisado deverão ser distribuídas a todos os colaboradores-chave da MILES. O BCP também será revisto caso aconteça alguma das situações abaixo:

- Mudanças materiais – organizacionais – no negócio da MILES
- Mudanças de pessoal
- Mudança de endereço do escritório da MILES ou abertura de um escritório adicional
- Introdução de novos processos ou alteração dos existentes
- Upgrade ou alterações na infraestrutura de IT e/ou sistemas
- Mudança de prestador de serviço relevante
- Alterações de informações de contatos (p.e., números de telefone)

B.1.5.2 – Treinamento e Testes

O treinamento do staff em relação ao BCP ocorre fundamentalmente com os procedimentos de teste. O único treinamento adicional requerido é uma apresentação do BCP em uma única sessão a ser feita no momento de sua publicação. No caso de um novo colaborador, a equipe de *Compliance* fará para ele(a) a última apresentação elaborada.

O BCP deve ser testado para garantir que o mesmo funcione em caso de necessidade. Diferentes cenários de eventos devem ser testados ao menos anualmente. Os principais testes são elencados a seguir

Call Tree

O líder do BCP começará o teste fora do horário comercial - sem aviso prévio - transmitindo uma palavra código para os participantes do *call tree*. No dia seguinte, todos os participantes deverão reportar a palavra-código transmitida. Este teste avalia a viabilidade do *call tree* e se os números de telefone foram corretamente registrados.

Conectividade Remota e Site de Contingência

Todo o staff que possuir acesso remoto via VPN (*Virtual Private Network*) deverá se logar na rede da MILES a partir de casa e checar se todos os sistemas essenciais e acessos funcionam perfeitamente. Um colaborador da equipe de Gestão e um de *Middle*-Office/Riscos deverão efetuar os testes através dos notebooks localizados no site de contingência.

Redundância de TI
Durante um final de semana, o provedor de serviços de TI (Tecnoqualify) irá acionar o sistema back-up e todo o staff tentará logar no sistema testando as aplicações essenciais. Posteriormente – no mesmo final de semana – o sistema principal/primário será acionado novamente, para testar o processo de retomada.

Redundância de Telecom
Durante um final de semana, todas as linhas fixas de telefone serão testadas e então estes serão testados através de um *call tree* para telefones fixos. Posteriormente – no mesmo final de semana – as linhas fixas serão reativadas e testadas como parte do processo de retomada.

Redundância de Energia (*Nobreaks*)
Durante um final de semana, a energia será desligada e o *nobreak* interno entrará em funcionamento. Os acessos e os sistemas essenciais deverão ser checados. Posteriormente – no mesmo final de semana – a energia será reativada e os acessos novamente testados como parte do processo de retomada.

Teste Completo
Durante um dia útil a ser combinado, a estrutura primária de TI será desligada pela manhã e o sistema de back-up entrará em vigor; os telefones fixos serão desviados para os celulares e nenhum staff (incluindo prestadores de serviços de TI) serão permitidos no escritório. Todo o staff trabalhará de casa [OU SITE DE CONTINGENCIA] priorizando as atividades essenciais da análise de impacto no negócio. O time de Crise gerenciará ativamente o teste organizando *conference calls* conforme planejado. No final do dia, os sistemas primários de IT e a telefonia fixa serão restaurados. No dia seguinte, todo o staff deverá checar se os arquivos foram propriamente salvos nos servidores primários. Este teste também verificará se as atividades chaves foram corretamente identificadas dentre outros.

B.1.6 – Obrigações dos Colaboradores da MILES em relação ao BCP

O BCP somente funcionará com o devido engajamento de todos os colaboradores-chave da MILES. Os colaboradores da MILES deverão obrigatoriamente:

- *Manter uma versão impressa atualizada do BCP em casa e no escritório;*
- *Ter programado no seu celular os números dos telefones do líder do BCP, seus colegas imediatos e do seu supervisor;*

- *Ter o número do conference call do BCP programado no celular e a senha de acesso ao conference room facilmente acessível;*
- *Testar periodicamente o acesso aos sistemas primários e back-ups via VPN (aqueles que tiverem acesso e estrutura computador/internet para o home-office);*
- *Manter uma política de mesa limpa (clean desk policy): no caso de um roubo ou incêndio, os papéis guardados ficam muito mais seguros do que aqueles deixados soltos;*
- *Os colaboradores que gerenciem ou tenham relacionamentos com prestadores de serviços também devem manter programados os contatos destes no celular.*

B.1.7 – Atividades e Responsabilidades relacionadas ao BCP

Os responsáveis pelas atividades relacionadas ao BCP da MILES são listados a seguir:

Atividade	Responsável
Manutenção e Atualização do Plano	
Aprovação, Revisões e conduzir revisão anual	
Treinamento e Teste anual do plano	
Implementação do plano em caso de necessidade	Emergency Response Team
Revisão Trimestral da lista de Contatos de Emergência	
Manutenção e distribuição da lista de Contatos de Emergência	
Prover informações do plano para investidores e CVM	
Revisar BCPs de prestadores de serviços essenciais	

• Na contratação dos serviços • Na revisão anual do BCP da MILES	

B.1.8 – Controle do Documento

O presente documento deve ser aprovado e revisado no mínimo anualmente pelo Comitê de Riscos e Compliance (CRC) da MILES:

Versão	Autor	Data	Comentário
1.0	Clayton Campos		Elaboração do documento