mar asset management

Política de Controles Internos

MAR Asset Management Gestora de Recursos Ltda.

Objetivo da Política

Estabelecer um conjunto de regras internas a serem adotadas pela MAR Asset Management Gestora de Recursos Ltda. (“MAR”) e seus Colaboradores (conforme abaixo definido) para delinear as responsabilidades e práticas apropriadas para garantir o cumprimento das regras e normas regulatórias aplicáveis.

A quem se aplica?

Sócios da MAR, assim como os executivos, empregados, colaboradores, prestadores de serviços, consultores, estagiários e temporários da MAR (doravante designados como “Colaborador(es)”).

Sumário

I. Introdução

A Política de Controles Internos da MAR (“Política”) reafirma o compromisso em cumprir a legislação e regulamentação em vigor aliado com um comportamento pautado nas melhores práticas de mercado e os mais altos padrões de ética, integridade, honestidade e profissionalismo, devendo ser analisada em conjunto com o Código de Ética e Conduta da MAR (“Código”) e os princípios ali elencados.

Esta Política foi adotada para auxiliar os Colaboradores no processo de tomada de decisões com a descrição das melhores práticas esperadas pela MAR, assim como orientação em uma variedade de assuntos. Entretanto, não é possível a exaustão de todos os temas relacionados com o presente tema, devendo o colaborador entrar em contato diretamente com o Chief Compliance Officer para sanar eventuais dúvidas.

II. Confidencialidade

As informações obtidas pelos Colaboradores sobre clientes/cotistas não podem, em hipótese alguma, ser divulgadas internamente, exceto caso outro Colaborador deva ter acesso à mesma informação ou se a divulgação for necessária considerando as políticas internas da MAR.

Desta forma, é também proibido o uso de informações confidenciais fora do ambiente de trabalho, seja a sua divulgação, venda ou uso para fins próprios.

No desempenho de suas funções, os Colaboradores deverão assinar, em conjunto com os demais documentos do Formulário "Conheça seu Colaborador" uma declaração de que observará tais regras de confidencialidade, sob pena de demissão por justa causa.

Dada as atuais dimensões da MAR e que a sociedade não realiza a atividade de distribuição dos fundos de investimento, os Colaboradores não terão acesso à um grande número de informações de clientes. Desta forma, a barreira sobre as informações será extensível a todos os Colaboradores que firmarão tal compromisso por meio do referido Formulário "Conheça seu Colaborador".

As informações privilegiadas com relação aos investimentos e estratégias de investimento serão detidas exclusivamente pela equipe de gestão e pelo Chief Compliance Officer, não devendo funcionários ou prestadores de serviços de áreas não-relacionadas ter acesso a esse tipo de informação.

III. Segurança da Informação

Com o intuito de estabelecer um ambiente seguro e confiável para seus clientes, a MAR possui uma barreira de segurança da informação que designa as responsabilidades e informações que são essenciais à cada um dos Colaboradores envolvidos para um controle do risco na realização de negócios e nas informações confidenciais para seus clientes.

Considerando que, atualmente, a MAR não realiza a atividade de distribuição das cotas dos fundos de investimento e realiza somente a gestão, informações confidenciais de clientes são todas mantidas pela sociedade que realiza a distribuição de nossas cotas, sendo de responsabilidade deles a guarda e manutenção de tais informações.

Dessa forma, a segregação da segurança da informação é focada no controle de informações internas, como planilhas, documentos e relatórios de risco, atas e documentos societários, principalmente do Comitê de Ética e Compliance, formulários de "Conheça o Seu Colaborador", dentre outros (em conjunto, tais informações internas serão designadas e referidas como "Informações Confidenciais"). Tal controle se dá pelos seguintes princípios:

- Segregação de atribuições: cada Colaborador será responsável pelas informações da área pela qual é vinculado, não tendo acesso os demais Colaboradores às informações de outras áreas, somente caso seja estritamente necessário, devendo o Chief Compliance Officer controlar o acesso à pastas através do sistema de armazenamento interno Google Drive. Mais detalhes sobre tal segregação podem ser encontrados no capítulo V. Segregação das Atividades desta Política.

- Medidas de Segurança: as medidas de segurança da informação deverão ser selecionadas com base em requerimentos comerciais, por meio de avaliações de risco, eficiência econômica e restrições legais.

- Evitando Incidentes: Os Colaboradores responsáveis por manter as informações deverão monitorar os seus respectivos computadores para detectar quaisquer violações ou anormalidades na segurança, devendo reportar imediatamente ao Chief Compliance Officer qualquer vazamento de informações internas.

- Sistemas Compartilhados: O acesso de Colaboradores aos sistemas específicos de suas áreas será autorizado somente pela Diretoria de cada área que seja responsável por tal

sistema. Desse modo, será responsabilidade de cada usuário fazer a guarda de sua senha e das demais informações de acesso.

- Titulares dos ativos de informação: todos os ativos de Informações Confidenciais deverão possuir um titular explícito, que será responsável pela classificação e definição apropriadas dos requerimentos para a proteção de todos os ativos de informação a eles confiados.

- Treinamentos de Informática: a área de Compliance poderá dar treinamentos específicos sobre o armazenamento de dados da MAR e sobre as medidas de segurança, sendo permitido que convide também especialistas da área de informática ou terceirizados contratados para auxiliar em tais treinamentos específicos.

Um detalhamento maior sobre medidas que auxiliam o seguimento dos princípios da MAR em relação à segurança da informação será dado no capítulo V. Segregação de Atividades.

Eventuais descumprimentos às orientações deste Capítulo serão analisados diretamente pelo Comitê de Ética e Compliance.

III.1. Responsabilidades dos Colaboradores

Os Colaboradores tem as seguintes responsabilidades em relação à esta Política:

- Assegurar que os recursos tecnológicos e informações da MAR sejam utilizados conforme esta Política.

- Informações Confidenciais quando impressas pelos Colaboradores devem ser imediatamente retiradas da impressora e rasgadas, quando não forem necessárias.

- Os Colaboradores não devem deixar papeis contendo Informações Confidenciais sem o devido armazenamento quando estiver fora do local de trabalho (*clean desk policy* - política da mesa limpa), devendo também sempre bloquear os seus computadores quando deixem a sua estação de trabalho.

- Utilizar somente o Google Drive da MAR para salvar as Informações Confidenciais, não sendo permitido o armazenamento de tais informações em sistemas ou programas que

não os autorizados diretamente por esta Política ou expressamente pelo Chief Compliance Officer.

- Proteger as Informações Pessoais contra acessos, modificações, destruição ou divulgação não autorizados pela MAR, sendo responsável pelo uso adequado das informações que possui acesso, o que inclui, além das Informações Confidenciais, as senhas de acesso ao Google Drive, e-mail corporativo, wi-fi, etc., não sendo permitido o compartilhamento de tais informações por pessoas externas.

- Em relação às senhas e informações de acesso, os Colaboradores: (i) não podem compartilhar a senha, anotar em arquivos físicos ou de fácil acesso; (ii) não podem utilizar códigos simples como próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existes no dicionário ou números sequenciais; (iii) devem preferencialmente utilizar senhas distintas para uso corporativo e para uso pessoal; e (iv) trocar as senhas periodicamente e sempre que suspeitar de algo.

- Na utilização do e-mail corporativo, os Colaboradores: (i) devem sempre utilizar o e-mail corporativo para comunicação com contrapartes da MAR ou para tratar de quaisquer assuntos relacionados ao dia-a-dia da MAR, não sendo permitido o uso de contas pessoais para tanto; (ii) ao receber e-mails com links, verificar se o mesmo corresponde ao endereço que aparece na tela; e (iii) não abrir, em hipótese alguma, caso não tenha absoluta certeza da procedência do envio e da legitimidade do e-mail.

- Sobre a utilização da rede compartilhada de internet no ambiente de trabalho, os Colaboradores: (i) não podem fazer upload ou download de softwares ou dados ilegais; (ii) não é permitido fazer o download ou enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais; e (iii) não fazer download de softwares de fontes não conhecidas ou que possam conter vírus ou outros tipos de malware, devendo contatar o Chief Compliance Officer caso tenha dúvidas, o qual irá entrar em contato com o suporte de informática para verificar a questão.

- Entrar imediatamente em contato com o Chief Compliance Officer caso tenha qualquer suspeita de um incidente de segurança, caso julgue necessário ou tenha dúvidas sobre como proceder, não sendo permitido o Colaborador tomar qualquer medida relacionada ao vazamento ou tentativa de acesso às Informações Confidenciais, sem que obtenha autorização do Chief Compliance Officer.

- Fornecer a senha de acesso ao Google Drive e ao e-mail da MAR ao Chief Compliance Officer para que ele possua acesso à todas as informações da conta, assim como para que ele possa verificar como estão sendo salvas as Informações Confidenciais e se as restrições do sistema, conforme serão abaixo listadas no item III.2. Armazenamento de Arquivos estão sendo seguidas estritamente por cada um dos Colaboradores.

III.2. Armazenamento de Arquivos

Em relação à utilização da rede de armazenamento da MAR, qual seja, o Google Drive (GSuite), a utilização seguirá as seguintes diretrizes:

- As pastas internas de armazenamento serão segregadas, possuindo cada usuário um perfil de acesso à cada pasta com dois níveis de segurança - leitura e edição, sendo definido pelo Diretor da área quem possuirá cada tipo de atribuição, devendo ser aprovado pelo Chief Compliance Officer qualquer alteração.

- É proibido o armazenamento de quaisquer arquivos que não sejam de interesse da MAR, assim como não são permitidos arquivos que não são de propriedade da empresa, como música, vídeos e fotos.

- A cópia de arquivos constantes no Google Drive da MAR é terminantemente proibida pelos Colaboradores, somente sendo permitida caso autorizada pelo Chief Compliance Officer.

Adicionalmente, o Google Drive permite que os arquivos compartilhados sejam bloqueados, tanto para edição, quanto para download. Desta forma, quando um Colaborador salvar um arquivo contendo Informação Confidencial, deverá ser incluída a restrição para edição, o que impossibilita o download do documento por pessoas não detentoras da informação.

Do mesmo modo, tal bloqueio permite que, no caso de vazamento de Informações Confidenciais, os responsáveis sejam identificados imediatamente e responsabilizados, tanto internamente, quanto do ponto de vista cível e criminal, caso seja necessário.

Sobre a manutenção de registro da MAR, todas as informações e documentos deverão ser arquivados pelo período mínimo de 05 (cinco) anos, conforme disposto na ICVM 558.

III.3. Testes Periódicos de Segurança

Deverão ser realizados testes períodos de segurança no computador de todos os Colaboradores, com o intuito de detectar previamente falhas de segurança e vulnerabilidades. O teste será realizado de forma mensal pelo Chief Compliance Officer ou por empresa terceirizada através do sistema central de gerenciamento do antivírus contratado pela MAR.

O Chief Compliance Officer deverá monitorar a realização de tais testes e manter os registros internos em caso de falhas e violações desta Política.

Adicionalmente, a área de Compliance deve assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.

Cumpre ressaltar, que certos sistemas, como o Google Drive, não necessitam de testes periódicos de segurança dado os diversos protocolos internos de tal sistema.

III.4. Empresa Terceirizada

A MAR utiliza os serviços de empresa terceirizada para realizar a manutenção e o controle dos computadores, firewall, internet, além dos sistemas de segurança. A estrutura, o funcionamento e os sistemas de controle internos seguem detalhados na forma de Anexo 1 a esta Política.

III.5. Trabalho Remoto

O trabalho de forma remota é permitido para todos os colaboradores, devendo ser utilizado o próprio computador do trabalho, em casos em que seja possível levá-lo ou ser utilizado computador que conte com sistema de antivírus e proteção no mesmo nível dos sistemas internos da Mar.

Caso esteja utilizando um computador pessoal, todos os arquivos relacionados à Mar Asset deverão ser salvos única e exclusivamente no Google Drive, não devendo ser armazenados no computador pessoal sob hipótese alguma.

IV. Treinamentos

A estratégia de treinamentos da MAR tem o intuito de aprimorar o desempenho de seus funcionários em relação às normas internas e regulações relacionadas à atividade de gestão de recursos de terceiros.

A MAR possui um treinamento para novos Colaboradores ("Treinamento de Novos Colaboradores") e um treinamento de renovação contínua ("Programa de Renovação"), ambos de frequência obrigatória por seus Colaboradores, inclusive dos que têm acesso a informações confidenciais e que participem do processo de tomada de decisão de investimento. O Treinamento de Novos Colaboradores e o Programa de Renovação são desenvolvidos pela área de Compliance, que supervisionará os Colaboradores quanto ao seu interesse, comparecimento e dedicação.

No Treinamento para Novos Colaboradores, o Colaborador toma conhecimento da história da MAR e dos seus Diretores e sócios, das atividades que realiza, das principais leis e regulamentos que regem a atividade de gestão de recursos de terceiros, bem como de todas as políticas internas. O Treinamento para Novos Colaboradores é aplicado em até três meses subsequentes ao mês em que novos Colaboradores tenham sido contratados.

O Programa de Renovação é realizado periodicamente, e poderá envolver a participação do Colaborador em cursos, palestras e treinamentos sobre temas relacionados à atividade desenvolvida pela MAR, assim como sobre alguma nova regulamentação que entrou em vigor ou sobre uma nova (ou atualizada) política interna. Seu objetivo é promover a atualização do conhecimento dos Colaboradores nas leis e normas aplicáveis às suas atividades.

V. Segregação das Atividades

Considerando o volume das atividades atualmente realizadas pela MAR e o número de funcionários bem reduzido para o momento, a estrutura organizacional da MAR contempla a segregação total dos arquivos referente à todos os Colaboradores, especialmente dos que desempenham atividades relacionadas à gestão de recursos, de modo a: (i) manter a segregação de atividades exigida pelos artigos 24 e 25 da ICVM 558; (ii) evitar o uso inadequado e indevido de informações confidenciais e informações privilegiadas; e (iii) evitar potenciais conflitos de interesse.

A segregação dos arquivos se dá através da utilização do serviço pago de armazenamento em nuvem Google Drive que oferece todos os requisitos necessários de segurança, conformidade e privacidade dos dados, sendo o acesso à determinados arquivos dados somente pelo Diretor responsável pela área.

O armazenamento por meio do Google Drive também permite uma segurança na contingência em caso de problemas, tendo em vista a possibilidade de acesso em qualquer computador por meio remoto.

Além dos controles acima estipulados, o acesso às instalações físicas da MAR é controlado, sendo permitido somente a permanência de terceiros na sala de reunião ou na sala de convivência, somente enquanto acompanhados de pelo menos um Colaborador. Desta forma, terceiros não possuirão acesso algum aos sistemas ou computadores utilizados pelos Colaboradores.

VI. Compliance

A área de Compliance terá autonomia para atuar nas suas funções com o objetivo de assegurar a conformidade das operações da MAR com o disposto na regulação em vigor, aplicar, monitorar e supervisionar com independência e eficiência o cumprimento das politicas internas e implementar procedimentos para cumprir o disposto nas politicas internas.

São atribuições da área de Compliance, em complemento às dispostas nos artigos 19 e 20 da ICVM 301:

- Implantar e manter dos programas de treinamentos dos Colaboradores assegurando a presença dos presentes.

- Garantir, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissional.

- Encaminhar as denúncias aos órgãos reguladores ou suspeitas levantadas pelos Colaboradores em relação à prevenção à lavagem de dinheiro e financiamento ao terrorismo.

- Elaborar e revisar todas as políticas internas e assegurar o seu alinhamento com a regulamentação em vigor e com a realidade fática da MAR.

- Garantir a confidencialidade das questões trazidas pelos Colaboradores, tanto em relação à assuntos internos, quanto pessoais.

- Definir os métodos de avaliação e monitoramento dos processos de controles internos da MAR, sendo também a única área da MAR responsável pelo atendimento/responder aos órgãos reguladores e autorreguladores.

Tendo em vista o tamanho do número de Colaboradores, a MAR não disporá de um Comitê de Compliance para o momento, sendo todos os temas do dia-a-dia tratados pelo Chief Compliance Officer e os mais sensíveis deverão ser levados pelo Chief Compliance Officer para o Comitê de Ética conforme disposto no Código.

Anualmente, e em conformidade com o disposto no artigo 22 da Instrução CVM nº 558 de 26 de março de 2015 ("ICVM 558"), a área de Compliance da MAR emitirá um relatório de controles internos com a conclusão dos exames efetuados que ficará disponível para a CVM na sede da MAR.

VI.1. Conflitos de Interesse:

Em relação à eventuais conflitos de interesse na MAR, a área de Compliance deverá analisar as situações que tenham sido levadas ao seu conhecimento em relação à conflitos envolvendo investimentos pessoais dos Colaboradores, transações financeiras de Colaboradores com clientes fora do ambiente da MAR, participação dos Colaboradores na administração de outras sociedades, recebimento de presentes ou favores de clientes, análise de empresas em que sejam sócios ou tenham relações pessoais diretas ou indiretas. Para análise dos conflitos de interesse devem ser consultadas outras políticas da MAR, como o Código e a Política de Negociação de Valores Mobiliários por Colaboradores da MAR.

Será vedada a participação dos Colaboradores em cargos da administração de sociedades que atuem em atividades relacionadas às da MAR no mercado financeiro e de capitais, tanto no Brasil, quanto no exterior, como consultorias de valores mobiliários, administradores recursos de terceiros, Family Offices, corretoras de valores mobiliários, bancos de investimento, etc., exceto no caso de cargos consultivos sem qualquer inferência no dia-a-dia da sociedade, para as quais as restrições abaixo deverão ser aplicadas.

Em relação à participação dos Colaboradores na administração de outras sociedades prestadoras de serviço, principalmente, cuja atividade envolva consultoria empresarial, os Colaboradores tem a obrigação de:

- Caso existam sociedades que sejam clientes da sociedade em que o Colaborador ocupa o cargo na administração e comercializem valores mobiliários, tanto no Brasil, quanto no exterior:
  - Caso o Colaborador não participe, por sua posição na MAR, do Comitê de Investimentos, deverá informar à para área de Compliance para que seja avaliada a existência ou não de conflito de interesse;
  - Caso o Colaborador participe do Comitê de Investimentos, caso surja eventual discussão sobre os valores mobiliários de emissão de tal cliente, a existência de

conflito deverá ser levantada imediatamente por tal Colaborador no momento da realização do Comitê, para o qual deverá ser convocado o Chief Compliance Officer e o qual deverá deliberar sobre tal situação de conflito.

- Informar à área de Compliance sobre todas as situações de conflito de interesse que possam surgir tendo em vista informações privilegiadas que tenham acesso durante tal prestação de serviços, devendo a área de Compliance decidir em qual categoria de restrição irá enquadrar o ativo, considerando a Política de Prevenção ao Insider Trading e Práticas Não Equitativas de Mercado da MAR.

- Garantir a segregação de todas as atividades da MAR com as atividades desempenhadas na administração de outras sociedades, não sendo permitido o compartilhamento de informações, o uso de ferramentas corporativas da MAR, uso de e-mail ou outros sistemas da MAR (especialmente de armazenamento), para realizar as outras funções que o Colaborador venha a desempenhar nessa sociedade.

Em relação à posição como membros consultivos de companhias abertas, como Conselho de Administração, o único membro da Mar Asset cuja participação é permitida é o Sr. Luis Moura, que já desempenhava tais funções antes de sua entrada na Mar Asset. Além das medidas acima de prevenção ao conflito de interesses acima, deverão seguir as seguintes orientações específicas para tal caso:

- Caso o Sr. Luis Moura venha a desempenhar a função administrativa em companhia cujos valores mobiliários sejam comercializados, tanto no Brasil, quanto no exterior, todos os colaboradores da MAR, devendo ser descritas amplamente para os Colaboradores todas as medidas que serão tomadas para as regras da comercialização do papel pelos fundos da MAR, considerando a Política de Prevenção ao Insider Trading e Práticas Não Equitativas de Mercado da MAR e o disposto abaixo.

- A área de gestão, caso a companhia participada seja companhia aberta, deverá ser imediatamente informada sobre tal restrição para que sejam respeitadas as regras de quiet period (período de silêncio) nas negociações dos valores mobiliários tais companhias (ou suas controladas e coligadas), tanto em relação às demonstrações financeiras (Instrução CVM No. 358/2002), tanto com o conceito de restrição para ofertas públicas, conforme o conceito criado pelo artigo 48, inciso IV da Instrução CVM No. 400/03. O tratamento de quiet period deverá ser seguido mesmo levando em consideração que o Sr. Luis Moura não faz parte da área de gestão da Mar e não tem poder decisivo.

- Na composição do portfólio de equities, a exposição máxima a sociedades em que o Sr. Luis Moura participe do Conselho de Administração é de 5% (individual ou de forma combinada) do fundo a custo.

VI.2. Seleção, Contratação e Supervisão de Prestadores de Serviços

Em relação à contratação de prestadores de serviços, tanto para a MAR, quanto para os fundos de investimento sob sua gestão, a área de Compliance estabeleceu certos procedimentos e critérios mínimos para orientar os processos de seleção, contratação e manutenção (com o devido monitoramento) de tais prestadores de serviços contratados.

Tais critérios utilizam as melhores práticas de mercado, assim como as orientações constantes nos Manuais e Códigos da ANBIMA, incluindo, mas não se limitando, ao Código de Regulação e Melhores Práticas.

A análise de tais prestadores de serviço, deverá também sofrer uma análise com base nos critérios de Conflitos de Interesse listados no item anterior deste Capítulo em relação aos Colaboradores, devendo ser discutidas as questões de conflito e o nível da relação existente no Comitê de Ética, caso o Chief Compliance Officer, após uma análise inicial, conclua que tal relacionamento é possível com base nos princípios determinados na presente Política e na legislação em vigor.

Cumpre ressaltar, que os procedimentos descritos neste capítulo deverão ser acompanhados e realizados conforme a Política de Práticas de Conheça o seu Cliente, Cadastro, PLD e CFT em relação à alimentação de informações na tabela de controle de contrapartes, sendo ambos os acompanhamentos realizados em conjunto pela área de Compliance.

A. Exceções Específicas

A área de Compliance poderá, por sua deliberação exclusiva, deixar de aplicar certos procedimentos estabelecidos neste item em relação ao acompanhamento caso o terceiro contratado possua: (i) reputação ilibada; (ii) capacidade técnica e econômico-financeira para o desempenho das atividades; (iii) seja associada à ANBIMA ou aderente aos Código

ANBIMA de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros (“Código").

B. Procedimento Prévio de Seleção dos Prestadores

Conforme disposto anteriormente, o processo de seleção das contrapartes será realizado diretamente pela área de Compliance, devendo ser obtidas diversas informações sobre o terceiro na fase pré-seleção, dentre as quais: (i) breve histórico da empresa; (ii) documentos societários; (iii) informações sobre a administração e sócios do prestador de serviços; (iv) autorizações para atuação na atividade, caso aplicável; (v) breve histórico do prestador de serviços; (vi) reportagens e informações gerais sobre os sócios, diretores e sobre a sociedade, em si, que possam ser encontradas na internet de forma pública; (vii) questionário ANBIMA de due diligence, quando aplicável.

Além dos critérios acima listados, a área de Compliance poderá determinar critérios específicos para pesquisa considerando a atuação específica de certa contraparte ou seu histórico, podendo pedir documentos e informações adicionais.

C. Contratação dos Prestadores de Serviço

Após os procedimentos prévios de contratação, a área de Compliance deverá aprovar, ou não, o prestador de serviços. Caso seja aprovado, seguirá com a assinatura do contrato de prestação de serviços alinhado com o mínimo exigido pelo Código, contendo:

(i) As obrigações e deveres das partes envolvidas;
(ii) A descrição das atividades que serão contratadas e exercidas por cada uma das partes;
(iii) A obrigação de cumprir as atividades em conformidade com as disposições do Código, caso aplicável;
(iv) Prazo da prestação de serviço, remuneração a ser paga, confidencialidade; e
(v) Obrigação do prestador de serviço de deixar à disposição do administrador fiduciário todos os documentos e informações exigidos pela regulamentação em vigor para elaboração dos informes periódicos obrigatórios, salvo os considerados confidenciais.

D. Contratação de Corretoras

Além dos procedimentos descritos acima para contratação de prestadores de serviço, especificamente para as corretoras contratadas pela MAR, a área de Compliance deverá solicitar o questionário da ANBIMA preenchido, além de

E. Classificação dos Prestadores de Serviço

Com o intuito de definir e evidenciar os terceiros com maior risco à MAR ou aos fundos por ela geridos que sejam os contratantes, conforme for o caso, a área de Compliance deverá criar um sistema de classificação a ser utilizado e incluído na tabela de controle de contrapartes.

O sistema de classificação será estabelecido nos níveis de baixo, médio ou alto risco que utilizarão os seguintes critérios de classificação: (i) histórico da contraparte; (ii) notícias e reportagens negativas na mídia envolvendo escândalos ou suspeitas de corrupção; (iii) membros da administração envolvidos em notícias e informações relacionadas à corrupção; (iv) existência de PEP ou vínculos com PEP; (v) transparência na estrutura societária; (vi) ser companhia aberta; (vii) o fato da contraparte não ser associada à ANBIMA ou aderente à Códigos da ANBIMA; e (viii) demais fatores específicos de certas contrapartes.

F. Corretoras de Valores Mobiliários

Especificamente sobre as corretoras de valores mobiliários, além dos critérios de contratação serem mais facilmente verificados pela área de Compliance graças a possibilidade de obtenção das informações reputacionais e regulatórias do órgão regulador e autorregulador, será feito um acompanhamento mensal sobre as alocações das ordens e a quantidade de ordens dada em cada corretora, alinhando com a qualidade do serviço oferecido, rapidez no atendimento e serviços análogos oferecidos como research, eventos com companhias abertas, etc.

G. Acompanhamento dos Prestadores de Serviço

Durante o prazo de duração dos contratos celebrados, a área de Compliance da MAR deverá realizar a manutenção periódica do contrato e do controle das contrapartes, realizando a

atualização da base de dados, assim como novas pesquisas sobre as informações obtidas durante o período de pré-contratação descrito no item A acima.

Adicionalmente, as áreas que usufruam dos serviços prestados pelos prestadores de serviço também deverão realizar a análise qualitativa dos serviços prestados, reportando imediatamente para o Diretor Jurídico e de Compliance caso algum serviço esteja sendo prestado de forma correta e adequada que deverá tomar as atitudes cabíveis do ponto de vista contratual e jurídico, podendo a decisão ser levada ao Comitê de Ética caso entenda ser necessário.

Em relação à classificação de risco estabelecida no item D. acima, a área de Compliance deverá realizar a revisão do cadastro e dos critérios respeitando os seguintes prazos:

(i) A cada 12 (doze) meses para as contrapartes classificadas como "Alto Risco";
(ii) A cada 24 (vinte e quatro) meses para as contrapartes classificadas como "Médio Risco"; e
(iii) A cada 36 (trinta e seis) meses para as contrapartes classificadas como "Baixo Risco".

Caso alguma notícia extraordinária surja ou a área de Compliance julgue necessária, poderá realizar a revisão das informações em um período menor do que o acima disposto.

Adicionalmente, tal área também poderá realizar mudanças para incluir novos critérios para a análise assim que surjam.

VI.3. Arquivo Interno:

Adicionalmente à política de arquivo na nuvem pelo Google Drive conforme disposto acima, a área de Compliance da MAR será responsável pela guarda dos documentos, tanto físicos, quanto eletrônicos, pelo prazo de 05 (cinco) anos na forma da legislação aplicável.

O prazo estabelecido de 05 (cinco) anos faz referência às melhores práticas de arquivos de documentos e também como atendimento à regulamentação vigente, principalmente em relação a arquivos de documentos tributários, quanto documentos trabalhistas, societários e comprovante de pagamentos.

O arquivo físico também deverá respeitar tal prazo e será mantido e organizado pela área de Compliance.

VII. Considerações Finais:

A atualização desta Política será realizada pelo Chief Compliance Officer dentro de um período de tempo razoável, logo após ocorram mudanças na regulamentação aplicável ou quando julgar apropriado. A versão atualizada será divulgada a todos os colaboradores e estará disponível no website da MAR: marinvestimentos.com.br.

Mediante a contratação/início do relacionamento e anualmente, todos os Colaboradores deverão aderir a esta Política através do preenchimento e assinatura do Formulário "Conheça seu Colaborador" que será disponibilizado por Compliance.

ANEXO 1 – Relatório da MAR elaborado pela empresa terceirizada Luckyb Informática Eireli

Rio de Janeiro, 22 de outubro de 2019.

Ref: Políticas e procedimentos de resiliência e continuidade de negócio - Versão: 1.0

1. **Licença de uso.**
   1.1. Esse documento foi criado pela **Luckyb TI** para **MAR Asset Management Gestora de Recursos Ltda (MAR)** que poderá usar e publicar sua totalidade ou parte.
   1.2. Não será permitido nenhum uso do presente documento para outro exceto a MAR Asset Management.

2. **Equipamentos, sistemas operacionais e aplicativos.**
   2.1. A MAR possui completa gerência em todos seus equipamentos. O ingresso de um novo equipamento necessita aprovação do departamento de compliance.
   2.2. Cada equipamento possui monitoramento periódico realizado pela Luckyb TI que permite identificar os potenciais riscos à segurança dos dados de propriedade da MAR.
   2.3. Mensalmente são aplicadas as atualizações propostas pelos fabricantes dos respectivos equipamentos. Nessa mesma rotina a atualização dos aplicativos, caso se aplique, também são verificadas as recomendações de seus fabricantes.

3. **Sistemas de backup.**
   3.1. Os arquivos compartilhados estão estocados e gerenciados na plataforma do Google GSuite. Essa plataforma garante backup e versionamento dos arquivos.
   3.2. Computadores mais importantes que possuem sistemas de trading, notícias e risco possuem seu próprio sistema de backup local para aumentar a capacidade de recuperação dos sistemas como um todo.

4. **Sistemas de Cyber-segurança**
   4.1. Um firewall de última geração controla os acessos entre os equipamentos operados pelos colaboradores e os serviços usados na internet. Cada serviço possui uma política de segurança gerenciada pelo firewall.

4.2. Além dos serviços na internet também são controlados os aplicativos que podem ser usados para acesso aos referidos serviços.
4.3. Serviços não cadastrados no firewall os colaboradores e seus equipamentos não terão acesso.
4.4. Todo o tráfego é monitorado, registrado, verificado existência de vírus detectado tentativas de intrusão ou negação de serviço.
4.5. O Firewall bloqueia automaticamente a conexão de origem caso seja detectado qualquer falta de conformidade com as regras e políticas. Além de detectar e bloquear o firewall alerta por email e registra cada ocorrência.
4.6. Na rede interna do escritório da MAR não há nenhum serviço publicado na internet.
4.7. Um sistema de antivírus de última geração protege as estações de trabalho dos colaboradores. Esse sistema detecta e bloqueia ameaças em tempo real nos computadores. Possui detecção de intrusão, alertas e relatórios aumentando o controle e a segurança contra cyber-ataques. A gerência é através de uma console personalizada e centralizada na internet e os alertas são enviados à Luckyb TI e ao departamento de compliance.

5. Gerenciamento de energia.

5.1. Um nobreak centralizado garante uma autonomia de 1 hora a todos os computadores e equipamentos de rede.
5.2. Um computador registra as ocorrências e gerencia o nobreak.

6. Plano de continuação de negócio.

6.1. O plano de continuidade de negócio da MAR é administrado pelo departamento de compliance.
6.2. O plano é iniciado se os colaboradores não conseguirem acesso aos computadores do escritório da MAR, seja por falta de energia elétrica, ataque cibernético, indisponibilidade de acesso ao prédio dentre outros eventos.
6.3. A premissa básica é garantir acesso dos colaboradores à um computador ou dispositivo móvel com acesso à internet. A MAR possui três notebooks fora do escritório que podem ser usados para acesso aos arquivos e sistemas.
6.4. Os dados estão na plataforma Gsuite Google Drive e disponíveis aos colaboradores por computador ou dispositivo móvel facilitando acesso aos sistemas baseados em arquivos, sem a necessidade de estar fisicamente dentro do escritório da MAR. Os colaboradores já usam diariamente os arquivos e sistemas tanto dentro como fora do escritório,
6.5. Bloomberg anywhere, sistema importante para as atividades da MAR possui a característica de conter o perfil de cada colaborador em nuvem. É usado diariamente tanto dentro como fora do escritório.

6.6. A MAR consegue operar com relativa normalidade apesar dos colaboradores não estarem concentrados em um mesmo local. Bastando um acesso à internet, móvel ou fixa, e um computador padrão. Os colaboradores são instruídos permanentemente a usarem a flexibilidade e mobilidade do Google drive e do Bloomberg Anywhere mantendo a empresa sempre pronta a exercer seu compromisso social.

7. Sumário.

7.1. O conjunto do sistema computacional da MAR possui uma moderna proteção contra cyber-ataques composta de um firewall e antivírus de última geração, sistemas operacionais atualizados e em sua última versão. Todos os equipamentos são controlados, monitorados e avaliados os riscos a eles inerentes.

7.2. Ótima resiliência contando com sistemas que funcionam em qualquer lugar ou dispositivo e capacidade de recuperação de dados.

7.3. Monitoramento e alertas fazem o tempo de resposta a paradas do sistema ser imediata acionando equipes de TI para devida mitigação.

MAR Asset_Poli□tica de Controles Internos_v1.2.pdf

Documento número #7d1c0568-d0c6-45f5-be13-9ec8f10f655b

Assinaturas

Igor Borde Gomes Galvão
Assinou como validador

Log

29 jun 2021, 15:57:56	Operador com email igalvao@marasset.com.br na Conta fc8fc3e5-171b-40d8-9864-b4ab781884a9 criou este documento número 7d1c0568-d0c6-45f5-be13-9ec8f10f655b. Data limite para assinatura do documento: 29 de julho de 2021 (15:34). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
29 jun 2021, 15:58:58	Operador com email igalvao@marasset.com.br na Conta fc8fc3e5-171b-40d8-9864-b4ab781884a9 adicionou à Lista de Assinatura: igalvao@marasset.com.br, para assinar como validador, com os pontos de autenticação: email (via token); Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Igor Borde Gomes Galvão e CPF 129.214.867-50.
29 jun 2021, 15:59:04	Operador com email igalvao@marasset.com.br na Conta fc8fc3e5-171b-40d8-9864-b4ab781884a9 alterou o processo de assinatura. Data limite para assinatura do documento: 29 de julho de 2021 (15:34).
29 jun 2021, 16:02:37	Igor Borde Gomes Galvão assinou como validador. Pontos de autenticação: email igalvao@marasset.com.br (via token). CPF informado: 129.214.867-50. IP: 179.218.29.83. Componente de assinatura versão 1.120.3 disponibilizado em https://app.clicksign.com.
29 jun 2021, 16:02:37	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 7d1c0568-d0c6-45f5-be13-9ec8f10f655b.

Hash do documento original (SHA256): 7150075c3ef9e03c8bbf40acb947340c2df2ed57bdbf9bf542879be2e2c12032