SQUALO CAPITAL GESTORA DE RECURSOS

MANUAL DE CONTROLES INTERNOS E *COMPLIANCE*

Março de 2022

www.squalocapital.com.br

1. INTRODUÇÃO

A **SQUALO CAPITAL GESTORA DE RECURSOS LTDA.** ("Sociedade") é uma sociedade limitada dedicada à prestação de serviço de administração de carteiras de valores mobiliários, na categoria "gestor de recursos".

No exercício de tais atividades, a Sociedade está sujeita às regras que regem o funcionamento do mercado de capitais brasileiro, especialmente às normas editadas pela Comissão de Valores Mobiliários ("CVM"), que atualmente regula o exercício da atividade de administração de carteiras por meio da Resolução CVM nº 21, de 25 de fevereiro de 2021 ("Resolução CVM nº 21"), bem como aos código de regulação e melhores práticas da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("Anbima"), notadamente o Código de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros ("Código de Administração de Recursos de Terceiros").

Este Manual de Controles Internos e *Compliance* ("Manual") tem por objetivo estabelecer as regras, procedimentos e controles internos exigidos pela Resolução CVM nº 21 e pelo Código de Administração de Recursos de Terceiros da Anbima.

Este Manual aplica-se a todos os sócios, administradores e funcionários da Sociedade ("Colaboradores"), de modo que, previamente ao início do exercício de suas funções perante a Sociedade, os Colaboradores deverão receber uma cópia deste Manual e firmar um Termo de Adesão (**Anexo I**). O Diretor de Risco e *Compliance* manterá em arquivo, na sede da Sociedade, pelo prazo mínimo de 5 (cinco) anos, uma via original do Termo de Adesão devidamente assinado por cada Colaborador.

Adicionalmente, a Sociedade disponibilizará uma cópia deste Manual em sua sede para consulta. Em caso de dúvidas acerca da interpretação das regras contidas neste Manual, ou havendo necessidade de aconselhamento, o Colaborador deverá buscar auxílio junto ao Diretor de Risco e *Compliance*.

O descumprimento das regras previstas neste Manual será considerado infração contratual e ensejará a imposição de penalidades, sem prejuízo das eventuais medidas legais cabíveis.

2. ESTRUTURA DO *COMPLIANCE*

A área de *compliance* da Sociedade é de responsabilidade do Diretor de Risco e *Compliance*, incluindo entre suas atribuições o controle e a supervisão das práticas profissionais de todos os Colaboradores para atendimento das regras previstas no presente Manual, na regulamentação e na legislação vigente.

Tendo isso em vista, a área de *compliance* atua com o objetivo de:

a) assegurar a conformidade das operações e atividades desenvolvidas pela Sociedade com as disposições legais e regulamentares aplicáveis, bem como às políticas internas e instrumentos de autorregulação adotados;

b) monitorar e supervisionar, com independência e eficiência, as operações e atividades desenvolvidas pela Sociedade e o cumprimento das normas aplicáveis, especialmente as regras contidas neste Manual;

c) implementar os Programas de Treinamento dos Colaboradores e demais procedimentos operacionais que deem cumprimento às normas previstas neste Manual; e

d) esclarecer eventuais dúvidas dos Colaboradores a respeito da legislação e regulamentação aplicável, assim como sobre as disposições deste Manual.

O Diretor de Risco e *Compliance*, nos termos do artigo 4º, parágrafo 3º, da Resolução CVM nº 21 (i) exerce suas funções com independência em relação às demais áreas da Sociedade; e (ii) não atua em funções relacionadas à administração de carteiras de valores mobiliários, à intermediação e distribuição de cotas de fundos de investimentos, ou em qualquer atividade que limite a sua independência, na instituição ou fora dela.

O Diretor de Risco e *Compliance*, visando a assegurar que a Sociedade opere em conformidade com as regras, normas e orientações aos quais está sujeita, deverá, ao menos uma vez por ano, avaliar e revisar os seus procedimentos relativos a controles internos e *compliance*, de modo a implementar eventuais atualizações ou aprimoramentos. Adicionalmente, o Diretor de Risco e *Compliance*, em conjunto a empresa Sociedade, especializada na prestação de serviços de tecnologia da informação, realizará testes periódicos de segurança para os sistemas de informação,

a fim de minimizar preventivamente eventuais riscos operacionais e de descumprimento do disposto no Código de Administração de Recursos de Terceiros, na Resolução CVM nº 21 e neste Manual.

3. COMITÊS INTERNOS

A Sociedade possui 2 (dois) comitês internos: (i) o Comitê de Investimento; e (ii) o Comitê de Risco.

(i) Comitê de Investimento:

Compete ao Comitê de Investimento, discutir, em última instancia, novas oportunidades de investimentos, teses, estratégias, bem como fazer uma revisão da composição dos atuais portfólios e analisar as estratégias implementadas.

O Comitê de Investimento será composto por 3 (três) membros, sendo um deles, necessariamente o diretor responsável pela administração de carteiras de valores mobiliários.

As reuniões do Comitê de Investimento acontecerão, pelo menos, semestralmente, podendo reunir-se de forma extraordinária sempre quando necessário. Fica dispensada a elaboração de atas, devendo, no entanto, os estudos, as análises, os relatórios e *research* que embasaram as decisões de investimento serem arquivados eletronicamente no sistema interno utilizado pela Sociedade.

(ii) Comitê de Risco:

Cabe ao Comitê de Risco o gerenciamento dos riscos inerentes às atividades desenvolvidas pela Sociedade. Caberá também ao Comitê de Risco receber os *reports*, na periodicidade prevista na Política de Gestão de Risco da Sociedade, elaborados pelo Diretor de Risco e *Compliance* referentes aos riscos de mercado, liquidez, operacional, de contraparte e concentração.

O Comitê de Risco será composto por, no mínimo, 2 (dois) membros, sendo um deles obrigatoriamente o Diretor de Risco e *Compliance*.

As reuniões acontecerão, pelo menos, semestralmente de forma ordinária ou de forma extraordinária quando o contexto assim demandar. As reuniões serão obrigatoriamente formalizadas em atas, subscritas pelos presentes e arquivadas pelo Diretor de Risco e *Compliance*.

4. PROGRAMAS DE TREINAMENTO

PROGRAMAS DE TREINAMENTO

Todos os Colaboradores da Sociedade, inclusive seus sócios e administradores, deverão obrigatoriamente participar dos programas de treinamento descritos neste capítulo ("Programas de Treinamento").

Os Programas de Treinamento serão de dois tipos: (i) o programa de treinamento inicial ("Programa de Treinamento Inicial") e (ii) os programas de reciclagem contínua ("Programas de Reciclagem Contínua").

Os Programas de Treinamento serão conduzidos pelo Diretor de Risco e *Compliance*, responsável por supervisionar os Colaboradores quanto à sua assiduidade e dedicação.

Os Colaboradores deverão obrigar-se, por meio do "Termo de Adesão" (**Anexo I**), a participar dos Programas de Reciclagem Contínua eventualmente realizados pela Sociedade, em conformidade com as orientações do Diretor de Risco e *Compliance*.

PROGRAMA DE TREINAMENTO INICIAL

O Programa de Treinamento Inicial será realizado ao tempo da contratação de novos Colaboradores, antes do início efetivo de suas funções na Sociedade.

O Programa de Treinamento Inicial terá por objetivo principal apresentar aos novos Colaboradores a atividade desenvolvida pela Sociedade e sua filosofia de investimento, bem como prestar esclarecimentos sobre as disposições constantes deste Manual e das demais normas internas adotadas pela sociedade, inclusive no que diz respeito às funções exercidas pelo Diretor de Risco e *Compliance*.

Ademais, o Programa de Treinamento Inicial visa a assegurar a completa informação e esclarecimento dos novos Colaboradores acerca dos procedimentos e controles a serem adotados para garantir o bom uso das instalações, equipamentos e arquivos da Sociedade, bem como para o devido cumprimento das normas deste Manual.

PROGRAMAS DE RECICLAGEM CONTÍNUA

Os Programas de Reciclagem Contínua serão realizados periodicamente, no mínimo uma vez por ano, e envolverão a participação dos Colaboradores em cursos, palestras e treinamentos sobre temas relacionados à atividade desenvolvida pela Sociedade, objetivando promover a constante atualização do conhecimento dos Colaboradores sobre a legislação, regulamentação e auto-regulamentação aplicável e sobre quaisquer outros temas relevantes ao exercício de suas funções e às atividades da sociedade.

Nesse sentido, a Sociedade incentivará a participação de todos os seus Colaboradores em eventos pertinentes ao mercado financeiro e cursos específicos para determinadas necessidades.

A Sociedade poderá, por deliberação dos seus diretores, financiar cursos de aprimoramento profissional, desde que julgue viável e interessante o conteúdo a ser lecionado. Caberá ao Diretor de Risco e *Compliance* da Sociedade a aprovação de participação em cursos, eventos ou palestras pelo Colaborador solicitante.

5. POLÍTICAS INTERNAS DA SOCIEDADE

O presente Manual contém as seguintes políticas internas da Sociedade:

(i) Política de Segregação Física de Atividades;
(ii) Política de *Know Your Client*;
(iii) Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo;
(iv) Política de Contratação de Prestadores de Serviços;
(v) Política de Segurança das Informações; e
(vi) Política de Segurança Cibernética.

Além das políticas mencionadas anteriormente, a Sociedade também possui as seguintes políticas em documentos apartados:

(i) Política de Gestão de Risco;
(ii) Política de Exercício de Direito de Voto;
(iii) Política de Rateio e Divisão de Ordens;
(iv) Política de Aquisição e Monitoramento de Ativos de Crédito Privado;
(v) Política de Seleção e Alocação de Ativos;
(vi) Manual de Certificação;
(vii) Política de Compra e Venda de Valores Mobiliários;
(viii) Código de Ética e Conduta; e
(ix) Plano de Continuidade de Negócios.

6. POLÍTICA DE SEGREGAÇÃO FÍSICA DE ATIVIDADES

A Política de Segregação Física de Atividades tem como objetivo estabelecer as regras que orientam a segregação física das instalações entre áreas responsáveis pelas atividades prestadas pela Sociedade, em particular, as atividades de administração de ativos e carteiras de valores mobiliários das demais atividades, que, eventualmente, venham a ser desenvolvidas pela sociedade. Atualmente, a Sociedade exerce apenas a atividade de gestão de recursos de terceiros, não atuando na distribuição de cotas de fundos de investimento sob sua gestão.

Nesse sentido, a presente política é adotada tendo como premissa o desenvolvimento exclusivo da atividade de administração de carteiras de valores mobiliários, notadamente a gestão de recursos de terceiros.

A Política de Segregação Física de Atividades deve ser revista e ajustada antes de qualquer ampliação do escopo das atividades da Sociedade, referidas no parágrafo acima, a fim de atualizar as regras e condições para o desenvolvimento das novas atividades nas suas instalações, sem que haja o descumprimento da presente política. Nesse sentido, caso a Sociedade venha a exercer outras atividades que exijam a segregação física com a atividade de administração de carteiras de valores mobiliários, a Sociedade assegurará, por meio de acesso controlado, que apenas os Colaboradores diretamente envolvidos na gestão de recursos de terceiros tenham acesso ao ambiente segregado.

Adicionalmente, são disponibilizados linhas telefônicas específicas e diretórios de rede privativos e restritos aos Colaboradores diretamente envolvidos na gestão de recursos de terceiros, devidamente segregados dos equipamentos dos demais Colaboradores.

O Diretor de Risco e *Compliance* é responsável por promover a aplicação das regras aqui contidas, de forma a assegurar a segregação física das instalações entre áreas responsáveis pelas atividades prestadas pela Sociedade quando aplicável.

CONFLITO DE INTERESSES

A Sociedade tem como objetivo conduzir seus negócios buscando sempre identificar, administrar e eliminar a existência de potencial conflitos de interesses. Há potencial

conflito de interesses quando há indício de que o interesse pessoal dos Colaboradores (ou grupo de Colaboradores) e/ou da própria Sociedade sobrepõe-se, direta ou indiretamente, aos interesses dos clientes da Sociedade.

Qualquer circunstância que represente conflito de interesses real ou potencial deve sempre ser resolvida priorizando-se o cliente em detrimento da Sociedade e/ou seus Colaboradores. Todos os Colaboradores devem evitar engajar-se em negócios externos que possam representar potenciais ou reais conflitos de interesses, que possam prejudicar a imagem da Sociedade.

Os Colaboradores compreendem que o conflito de interesses se estende também aos seus familiares, cônjuges e relacionados devendo observar as regras estabelecidas neste Manual, também como forma de prevenir conflitos de interesses.

Os Colaboradores não poderão manter relações comerciais privadas com clientes, prestadores de serviços, parceiros e concorrentes nas quais venham a obter privilégios pessoais em razão de cargo ou função ocupada.

Os Colaboradores que forem investidores de fundos geridos pela Sociedade deverão atuar sempre de forma imparcial e independente, não podendo influenciar ou direcionar a tomada de decisões por motivos pessoais, devendo sempre pautar-se pelas regras de mercado e pelo profissionalismo exigido pela Sociedade, estando ciente de que a eles serão aplicáveis as mesmas regras de mercado e do investimento, em paridade, imputáveis aos demais investidores.

Entendendo ser difícil prever toda e qualquer situação de conflito, os profissionais devem ser sensíveis a potenciais conflitos e trazer dúvidas à atenção do Diretor de Risco e *Compliance*. Se um conflito não puder ser evitado, o mesmo deve ser gerido de forma ética e responsável, sempre priorizando os interesses dos clientes.

7. POLÍTICA DE *KNOW YOUR CLIENT* (“KYC”)

A Sociedade, como gestora de recursos de terceiros, empenha seus melhores esforços para a identificação de seus clientes, o que é realizado previamente ao efetivo cadastramento das operações.

Os procedimentos de KYC adotados pela Sociedade incluem a obtenção de informações precisas sobre a atuação profissional dos clientes, o seu ramo de atividade e a sua situação financeira patrimonial.

Os procedimentos de KYC serão formalizados por meio do preenchimento de formulários específicos para todos os clientes, pessoas físicas ou jurídicas. A Sociedade, por meio dos seus Colaboradores, deverá assegurar que todos os campos do referido formulário sejam preenchidos com veracidade, seriedade e clareza.

Sempre que possível, os responsáveis pelo preenchimento dos formulários devem realizar visitas aos clientes e, quando aplicável, aos seus estabelecimentos comerciais. Tais visitas devem ser periodicamente refeitas e visitas especiais deverão ser efetuadas em qualquer situação de anormalidade ou mudança no comportamento operacional do cliente. Adicionalmente, também serão realizadas pesquisas independentes em relação às informações fornecidas.

O formulário poderá ser arquivado eletronicamente, quando assim preenchido, ou fisicamente juntamente com a documentação cadastral do cliente.

Avaliação Interna de Risco

Com base nestas informações, a Sociedade classificará seus clientes como baixo, médio ou alto risco. Os clientes classificados como de alto risco, bem como aqueles que se recusem ou dificultem o fornecimento das informações requeridas, não serão aceitos pela Sociedade para cadastramento como cliente

8. POLÍTICA DE PREVENÇÃO A LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO ("PLDFT")

A presente política de PLDFT tem por objetivo estabelecer as normas, procedimentos e controles internos relacionados à prevenção de utilização indevida da Sociedade como intermediária para a prática dos crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores de que trata a Lei nº 9.613, de 3 de março de 1998, alterada pela Lei nº 12.683, de 9 de julho de 2012 ("Lei n° 9.613/98"), a Resolução CVM nº 50, de 31 de agosto de 2021 ("Resolução CVM nº 50"), bem como a Resolução nº 21, expedida pelo Conselho de Controle de Atividades Financeiras ("COAF") em 20 de dezembro de 2012.

Neste sentido, a Sociedade pretende, ao instituir a presente política de PLDFT, estabelecer e implementar procedimentos e controles destinados a:

(i) Identificar a qualificação e perfil dos clientes, contrapartes e demais envolvidos nas atividades desenvolvidas pela Sociedade;
(ii) Identificar o propósito e a natureza das relações de negócios, assim como os beneficiários finais das operações;
(iii) Reduzir os riscos de que os negócios, atividades e serviços prestados pela Sociedade sejam destinados à lavagem de dinheiro ou ao financiamento ao terrorismo;
(iv) Enquadrar e classificar as operações e clientes da Sociedade em categorias de risco, para maior controle; e
(v) Identificar as operações suspeitas do ponto de vista da lavagem de dinheiro e financiamento ao terrorismo e aquelas de comunicação obrigatória ao COAF.

LAVAGEM DE DINHEIRO

O crime de lavagem de dinheiro caracteriza-se pela realização de um conjunto de operações comerciais ou financeiras com o objetivo de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedades de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

Geralmente, o processo de lavagem de dinheiro é composto por 3 (três) fases independentes que, com frequência, ocorrem de forma simultânea, quais sejam:

(i) Colocação: ingresso no sistema financeiro de recursos provenientes de atividade ilícitas, por meio de depósitos, compra de instrumentos financeiros ou compra de bens. Nesta fase, é comum a utilização de instituições financeiras para a introdução de recursos obtidos ilicitamente;

(ii) Ocultação: execução de múltiplas operações financeiras com os recursos já ingressados no sistema financeiro, visando a ocultação dos recursos ilegais, por meio de transações complexas e em grande número para dificultar o rastreamento, monitoramento e identificação da fonte ilegal do dinheiro; e

(iii) Integração: incorporação formal do dinheiro no sistema econômico, por meio de investimento no mercado de capitais, imobiliário, obras de arte, dentre outros.

FINANCIAMENTO AO TERRORISMO

O delito de financiamento ao terrorismo caracteriza-se pela promoção ou recebimento de fundos com a intenção de emprega-los, ou ciente de que os mesmos serão empregados, no todo ou em parte, para levar a cabo: (i) um ato que constitua delito, nos termos da legislação aplicável; ou (ii) qualquer outro ato com intenção de causar a morte ou lesões corporais graves a um civil, ou a qualquer outra pessoa que não participe ativamente das hostilidades em situação de conflito armado, quando o propósito do referido ato, por sua natureza e contexto, for intimidar uma população, ou compelir um governo ou uma organização internacional a agir ou abster-se de agir.

CLASSIFICAÇÃO DOS CLIENTES – AVALIAÇÃO INTERNA DE RISCO

O cadastro de clientes é elemento essencial da prevenção e combate ao crime de lavagem de dinheiro e financiamento ao terrorismo e, portanto, os Colaboradores da Sociedade deverão manter cadastro atualizado de seus clientes.

Os Colaboradores deverão efetuar o cadastro de seus clientes contendo, no mínimo, as informações e os documentos indicados no Anexo B da Resolução CVM n° 50, e deverão atualizar o cadastro dos clientes ativos em intervalos não superiores a 12 (doze) meses. De acordo com a Resolução CVM nº 50, considera-se ativo o cliente que, nos últimos 12 (doze) meses tenha efetuado movimentação, em sua conta corrente ou em sua posição de custódia, tenha realizado operações no mercado de valores mobiliários ou apresentado saldo em sua posição de custódia.

É obrigatória a obtenção e análise dos dados cadastrais e da documentação exigida para abertura do relacionamento com os clientes, de modo que é vedada a realização de transações comerciais em nome de clientes que deixarem de apresentar comprovação de sua identidade e as demais informações e os demais documentos exigidos pela legislação aplicável.

Toda a informação e documentação deve ser cuidadosamente analisada para fins de confirmação do cadastro. Neste sentido, as informações prestadas deverão ser acompanhadas dos documentos de identificação da empresa contratante, seus sócios, administradores e procuradores (se houver), e de toda a documentação que comprove a veracidade das informações prestadas. Os Colaboradores responsáveis pela análise dos clientes deverão diligenciar para que todas as informações prestadas sejam verificadas, de modo a mitigar o risco do recebimento de informações falsas e/ou equivocadas, o que pode comprometer a análise e a classificação de risco dos clientes.

Após a análise, os Colaboradores deverão classificar seus clientes entre as seguintes categorias de Risco de Lavagem de Dinheiro e Financiamento ao Terrorismo: (i) Baixo Risco; (ii) Risco Moderado; e (iii) Alto Risco.

Deverão ser classificados na categoria “Alto Risco” os clientes (i) classificados como pessoa politicamente exposta, conforme definido a seguir; (ii) que não puderem ser identificados; (iii) cuja diligência não puder ser comprovada; (iv) que forem representados costumeiramente por terceiros; (v) que forem representados por, ou de cuja composição societária participe, pessoa domiciliada em jurisdições com deficiências estratégicas de prevenção a lavagem de dinheiro e ao financiamento ao terrorismo ou de região considerada de tributação favorecida; (vi) com ocupações profissionais e ramos de atividades considerados como de alto risco por serem incompatíveis com determinadas operações realizadas no mercado financeiro, ou serem mais suscetíveis de envolvimento em crimes de lavagem de dinheiro; e (vii) que forem, de qualquer forma, relacionados a pessoas que mantenham ou já tenham mantido relações com pessoas ou grupos terroristas, conforme definido na Resolução COAF n° 15, de 28 de março de 2007.

A Sociedade adotará o conceito de pessoa exposta politicamente determinado no Anexo A da Resolução CVM n° 50. Para a verificação dessa condição, os Colaboradores deverão adotar as seguintes providências: (i) solicitar declaração expressa do cliente a respeito da sua classificação; (ii) consultar informações publicamente disponíveis; e (iii)

consultar as bases de dados eletrônicos comerciais sobre pessoas politicamente expostas.

PROCEDIMENTOS DE KYC

Conforme exposto anteriormente, a Sociedade adota procedimentos de KYC, os quais têm por objetivo a exata identificação do perfil dos clientes, por meio da obtenção de informações precisas sobre a sua atuação profissional, o seu ramo de atividade e a sua situação financeira patrimonial.

PROCEDIMENTOS DE CONHEÇA SEU COLABORADOR (KNOW YOUR EMPLOYEE - KYE)

Os procedimentos de "Conheça seu Colaborador" têm por objetivo fornecer à Sociedade informações detalhadas sobre seus Colaboradores, os quais incluem critérios para a sua contratação e verificação de suas condutas.

A Sociedade adota uma postura rígida e transparente na contratação de seus Colaboradores e, portanto, além dos requisitos técnicos e profissionais, serão avaliados os requisitos ligados à reputação dos Colaboradores no mercado e ao perfil profissional, bem como os antecedentes profissionais do candidato.

Para este fim, a Sociedade obterá, junto aos meios legais aplicáveis, as informações relativas à situação econômico-financeira de seus Colaboradores.

PROCEDIMENTOS DE CONHEÇA SEU PARCEIRO (KNOW YOUR PARTNER - KYP)

Os procedimentos de "Conheça seu Parceiro" abrangem todos os parceiros de negócios da Sociedade, no Brasil ou no exterior, bem como todos os seus fornecedores e prestadores de serviços.

Os procedimentos de "Conheça seu Parceiro" têm como objetivo a prevenção do envolvimento da Sociedade em situações que possam acarretar a riscos legais e à sua reputação perante o mercado. A Sociedade tem como princípio sempre que realizar contratações, operações diretas, negociar ativos ilíquidos ou realizar transações em mercados ilíquidos, identificar a contraparte com o intuito de prevenir que a contraparte utilize a instituição gestora e/ou os fundos de investimento ou carteiras geridas para atividades ilegais ou impróprias.

O processo de análise de contrapartes da Sociedade está inserido dentro do âmbito das obrigações da gestora, devendo ser averiguada as seguintes questões:

- Estabelecer a identidade de cada contraparte;
- Conhecer a atividade da contraparte;
- Conhecer a origem do patrimônio da contraparte; e
- Averiguar a origem e destino dos recursos movimentados pela contraparte.

A Sociedade entende que para prevenir de maneira eficaz a lavagem de dinheiro é necessária a avaliação do risco oferecido por suas contrapartes, antes da efetiva transação do negócio. No auxílio a essa averiguação, a Sociedade poderá se utilizar de um Questionário de *Due Diligence* próprio, ou até mesmo efetuar visitas de diligência, de forma a assegurar que os parceiros comerciais possuam práticas adequadas de prevenção à lavagem de dinheiro.

Ainda, a Sociedade e seus Colaboradores farão pesquisas, através dos meios públicos disponíveis, sobre a reputação de potenciais parceiros e sobre seu histórico econômico-financeiro, por meio das informações disponíveis nos serviços de proteção ao crédito, nos órgãos judiciais, em mecanismos de busca online e demais fontes de informação pública.

No sentido de cooperar, conforme previsto acima, a Sociedade irá rever periodicamente as políticas de PLDFT dos prestadores de serviços dos fundos de investimento sob responsabilidade da Sociedade para verificar se adotam regras e controles internacionalmente aceitos e recomendados pela GAFI.

Por fim, a Sociedade conta com uma Política de Contratação de Prestadores de Serviços, prevista neste Manual de Controles Internos, que traz processos e requisitos para contratação de terceiros, o que auxilia o processo de KYP.

PROCEDIMENTOS RELACIONADOS AOS INVESTIMENTOS REALIZADOS PELAS CARTEIRAS

A negociação de valores mobiliários nos fundos de investimento também deve ser analisada e monitorada para fins de PLDFT, sobretudo no que diz respeito às Contrapartes envolvidas. Para os fins desta Política, entende-se como “Contraparte” a

pessoa natural ou jurídica, fundo de investimento, clube de investimento ou o investidor não residente que atua como contraparte nas operações da carteira do fundo realizadas pelos fundos de investimento quando da aquisição de ativos.

Na indústria de gestão de recursos de terceiros, o gestor do fundo de investimento é o responsável pela análise para fins de PLDFT das Contrapartes quando da aquisição de ativos.

Dessa forma, a Sociedade realizará o cadastro e monitoramento das Contrapartes, conforme mencionado acima, com o objetivo de prevenir que Contrapartes utilizem os fundos de investimento sob sua gestão para atividades ilegais ou impróprias.

MONITORAMENTO DE OPERAÇÕES

A Sociedade adotará procedimentos para controlar e monitorar a faixa de preços dos ativos e valores mobiliários negociados para os fundos de investimento, 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, comunicadas aos órgãos competentes.

Os registros de todas as operações que a Sociedade realizar em nome de seus clientes ficarão arquivados na sede da Sociedade e à disposição dos órgãos reguladores por, no mínimo, 5 (cinco) anos contados do encerramento da relação contratual com o cliente, podendo ser descartados após este prazo.

Ainda, a Sociedade também realizará o monitoramento de notícias e eventos negativos ou relacionados à lavagem de dinheiro com seus parceiros comerciais/contrapartes, que permite a Sociedade cessar o vínculo imediato com a eventual instituição, bem como apurar o cometimento de algum ilícito que possa afetar a Sociedade.

COMUNICAÇÃO AO COAF

Caso o Colaborador responsável pela análise da operação se depare com alguma operação em que se configurem as hipóteses listadas abaixo ou qualquer outra que possa configurar indício de ocorrência dos crimes de lavagem de dinheiro previstos na Lei nº 9.613/98 ou de financiamento ao terrorismo, a operação deverá ser analisada com especial atenção e, se consideradas suspeitas, comunicadas ao COAF:

(a) Operação que aparente não ser resultante de atividades ou negócios usuais do cliente ou do seu ramo de negócio;

(b) Operação cuja origem ou fundamentação econômica ou legal não sejam claramente aferíveis;

(c) Operação incompatível com o patrimônio, a capacidade econômico-financeira, ou a capacidade de geração dos recebíveis do cliente;

(d) Operação com cliente cujo beneficiário final não é possível identificar;

(e) Operação envolvendo pessoa jurídica domiciliada em jurisdições consideradas pelo Grupo de Ação contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI) de alto risco ou com deficiências estratégicas de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo ou países ou dependências considerados pela Secretaria da Receita Federal do Brasil (RFB) de tributação favorecida e/ou regime fiscal privilegiado;

(f) Operação envolvendo pessoa jurídica cujos beneficiários finais, sócios, acionistas, procuradores ou representantes legais mantenham domicílio em jurisdições consideradas pelo GAFI de alto risco ou com deficiências estratégicas de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo ou países ou dependências considerados pela RFB de tributação favorecida e/ou regime fiscal privilegiado;

(g) Resistência, por parte do cliente ou demais envolvidos, ao fornecimento de informações ou prestação de informação falsa ou de difícil ou onerosa verificação, para a formalização do cadastro ou o registro da operação;

(h) Atuação do cliente ou demais envolvidos, inclusive sócios e acionistas, no sentido de induzir a não realização dos registros exigidos pela legislação de prevenção à lavagem de dinheiro e ao financiamento do terrorismo;

(i) Operação da qual decorra pagamento que, por solicitação do cliente ou demais envolvidos, não seja por meio de Transferência Eletrônica Disponível – TED, Documento de Crédito – DOC, transferência entre contas ou cheque nominativo;

(j) Operação envolvendo pagamento a terceiro, mesmo quando autorizado pelo cliente, desde que não destinado, comprovadamente, a fornecedor de bens ou serviços do cliente, ou recebimento oriundo de terceiro que não o sacado;

(k) Pagamento distribuído entre várias pessoas ou utilizando diferentes meios;

(l) Operação lastreada em títulos ou recebíveis falsos ou negócios simulados;

(m) Operação em que o cliente dispense vantagens, prerrogativas ou condições especiais normalmente consideradas valiosas para qualquer cliente;

(n) Quaisquer tentativas de burlar os controles e registros exigidos pela legislação de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, inclusive mediante:

(i) Fracionamento;

(ii) Pagamento em espécie;

(iii) Pagamento por meio de cheque emitido ao portador; ou

(iv) Outros meios;

(o) Quaisquer outras operações que, considerando as partes e demais envolvidos, os valores, modo de realização e meio e forma de pagamento, ou a falta de fundamento econômico ou legal, possam configurar sérios indícios da ocorrência dos crimes previstos na Lei nº 9.613/98, ou com eles relacionar-se.

Os Colaboradores da Sociedade comunicarão o COAF sempre que as operações possuírem as seguintes características, independentemente de qualquer análise ou juízo de valor feito pelo Colaborador:

(a) Caso a operação envolva o pagamento ou recebimento de valor igual ou superior a R$ 50.000,00 (cinquenta mil reais), ou equivalente em outra moeda, em espécie ou por meio de cheque ao portador; e

(b) Em qualquer das hipóteses de envolvimento do cliente com grupos terroristas, conforme previsto na Resolução COAF nº 15, de 28 de março de 2007.

RESPONSÁVEL

O Diretor de Compliance e Risco da Sociedade é o responsável pelo cumprimento das regras relacionadas à PLD e KYC.

9. POLÍTICA DE CONTRATAÇÃO DE PRESTADORES DE SERVIÇOS

A Sociedade, na condução e no melhor exercício de suas atividades e responsabilidade como administrador de carteiras de valores mobiliários, poderá contratar terceiros, conforme suas especialidades e de acordo com a necessidade, para prestação dos serviços permitidos pela regulação em vigor.

Esta Política de Contratação de Prestadores de Serviços tem por objetivo estabelecer as regras e procedimentos que deverão ser observados pela Sociedade na seleção e contratação de prestadores de serviços, nos termos da Resolução CVM nº 21.

CONTRATAÇÃO DE CORRETORAS DE VALORES MOBILIÁRIOS

A área de gestão da Sociedade tem o dever para com os clientes de buscar a melhor execução para todas as operações realizadas pelos fundos de investimento sob sua gestão.

Não só os fatores quantitativos (comissões e taxas), mas também fatores qualitativos devem ser observados ao se buscar uma corretora de valores mobiliários. Ao se avaliar a melhor execução, o gestor deve considerar toda a oferta de serviços da corretora avaliada, incluindo, entre outras coisas, a capacidade de execução da ordem, a qualidade do *research*, a corretagem cobrada e a solidez financeira da instituição.

Alguns requisitos são fundamentais para a aprovação das corretoras, dentre os quais se destacam:

(i) Experiência

- Número de operações executadas com sucesso;
- Velocidade de execução das operações;
- Agilidade durante períodos de volatilidade elevada;
- Capacidade de executar estratégias diferenciadas como casar ativos diferentes, vencimentos distintos, estratégias com opções, etc.;
- Capacidade de buscar liquidez para minimizar o custo da operação em mercados com condições adversas;
- Busca de oportunidades para executar melhor a ordem;

- Competência para executar com eficiência diferentes tipos de ordens;
- Caso ocorram erros de execução, a corretora deve corrigir estes erros de maneira satisfatória e ressarcir os prejuízos; e
- Facilidade para operar em mercado *after-market*.

(ii) Infraestrutura

- Telefonia adequada; e
- Relatórios de confirmação das operações precisos e disponibilizados em arquivos formatados de acordo com as exigências dos administradores e custodiantes dos fundos de investimento e carteiras administradas.

(iii) Habilidade para prover as seguintes informações

- *Research* proprietário ou de terceiros;
- Acesso aos analistas de empresas, econômicos ou políticos;
- Condições financeiras da corretora.

(iv) Financeiro e Societário

- Checagem da solidez financeira do prestador de serviços, incluindo a análise de cadastros restritivos de crédito;
- Autorizações necessária para a prestação dos serviços contratados;
- Adesão a códigos da Anbima;
- Reputação ilibada; e
- Demonstrações Financeiras.

(v) Procedimentos

- Desenvolvimento de uma lista de corretoras aprovadas e corretoras alternativas que respeitem as características listadas acima; e
- Reavaliação sistemática e periódica das corretoras utilizadas.

Ao final da análise, o Diretor de Risco e *Compliance* elaborará um relatório com o resultado da análise com a decisão sobre a contratação da referida corretora.

CONTRATAÇÃO DE PRESTADORES DE SERVIÇOS

A contratação de outros prestadores de serviços (ex. consultoria especializada) observará os procedimentos mencionados anteriormente. A análise das informações referentes aos prestadores de serviços incluirá, além daquelas previstas acima, conforme aplicável, a análise do Questionário Anbima de *Due Diligence* específico para a atividade que será exercida pelo prestador de serviço.

Os prestadores de serviços que tiverem suas atividades autorreguladas pela Anbima e não forem associados ou aderentes aos Códigos Anbima de Regulação e Melhores Práticas devem, obrigatoriamente, ser classificados como de alto risco e ser supervisionados, no mínimo, a cada 12 (doze) meses.

Adicionalmente, para a contratação de terceiros para atividades que não possuam questionário Anbima de *Due Diligence*, deverão ser analisadas as competências técnicas dos profissionais, a qualidade dos produtos e serviços oferecidos, a agilidade e flexibilidade dos Colaboradores, o cumprimento de prazos, estabilidade financeira do prestador de serviço pessoa jurídica, e, por fim, o custo-benefício.

SUPERVISÃO E MONITORAMENTO DE PRESTADORES DE SERVIÇOS

Anualmente o Diretor de Risco e *Compliance* irá realizar uma revisão dos documentos, processos e informações apresentadas pelos prestadores de serviços quando da contratação, incluindo informações sobre a sua estrutura e capacidade operacional, nos termos da regulamentação vigente.

O Diretor de Risco e *Compliance* deve rever periodicamente 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.

A Sociedade deverá comunicar aos seus clientes sobre eventuais recebimentos de serviços adicionais fornecidos pelos prestadores de serviços em razão de sua contratação e relacionamento.

10. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INFORMAÇÕES CONFIDENCIAIS

Os Colaboradores da Sociedade, no desempenho de suas funções, poderão vir a ter acesso a diversas informações classificadas como confidenciais.

Para fins da presente Política de Segurança da Informação, serão consideradas informações confidenciais todas e quaisquer informações e/ou dados de natureza sigilosa (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Sociedade, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de administração de ativos e carteiras de valores mobiliários desenvolvida pela Sociedade, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui contempladas ("Informação Confidencial").

Não são consideradas informações confidenciais aquelas informações que: (a) sejam ou venham a se tornar de domínio público sem violação do disposto nesta Política de Segurança da Informação; (b) tenham sido recebidas de boa-fé pelo Colaborador, de terceiros que tenham o direito de divulgá-las, sem obrigação de confidencialidade; (c) em virtude de lei, decisão judicial ou administrativa, devam ser divulgadas a qualquer pessoa; ou (d) cuja divulgação tenha sido aprovada pelo Diretor de Risco e *Compliance*.

Nesse sentido, todos os Colaboradores, ao firmar o Termo de Adesão anexo ao presente Manual na forma do "**Anexo I**", deverão tomar conhecimento e expressamente anuir com o quanto segue:

(i) Os Colaboradores expressamente obrigam-se a manter o sigilo das Informações Confidenciais que lhes tenham sido transmitidas, fornecidas e/ou divulgadas sob ou em função de seu vínculo com a Sociedade ou de relacionamento com clientes da Sociedade, se comprometendo a não utilizar, reproduzir ou divulgar as referidas Informações Confidenciais, inclusive à pessoas não habilitadas ou que possam vir a utilizá-las indevidamente em processo de decisão de investimento próprio ou de terceiros, exceto mediante autorização expressa e

escrita do respectivo titular e na medida do estritamente necessário para o desempenho de suas atividades e/ou obrigações;

(ii) Todos os negócios, técnicas, materiais, planilhas, formulários, projetos, desenvolvimentos de estratégias, produtos ou serviços elaborados, desenvolvidos e/ou utilizados pela Sociedade e/ou por seus clientes, mesmo que tenham significativa participação de qualquer Sociedade, sempre serão de propriedade da Sociedade, sendo vedado a qualquer Colaborador divulgá-los, utilizá-los para si ou terceiros, cedê-los ou aliená-los, seja a que título for;

(iii) Os Colaboradores expressamente reconhecem ser de propriedade da Sociedade todos os direitos autorais e/ou intelectuais existentes e advindos de projetos, técnicas, estratégias, materiais, planilhas, formulários, desenvolvimentos de contratos ou serviços, métodos e/ou sistemas atualmente existentes ou que vierem a ser desenvolvidos durante seus respectivos vínculos com a Sociedade, nada podendo vir a reclamar a esse título;

(iv) Caso qualquer Colaborador seja obrigado a divulgar Informações Confidenciais por determinação judicial ou de autoridade competente, o Colaborador deverá comunicar a Sociedade da existência de tal determinação previamente à divulgação e se limitar estritamente à divulgação da Informação Confidencial requisitada;

(v) Para os propósitos do disposto nesta política, caberá ao Colaborador o ônus de provar o caráter não confidencial de qualquer informação; e

(vi) O acesso às Informações Confidenciais será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Sociedade, a critério do responsável de cada área e com anuência do Diretor de Risco e *Compliance*. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, conforme exposto aqui, seguirá o critério definido pelo responsável de cada área, a empresa contratada pela gestora especializada na prestação de serviços de tecnologia da informação, juntamente com o Diretor de Risco e *Compliance*, respeitando uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa.

Caso tenham conhecimento de que qualquer Colaborador tenha infringido a presente política, os demais Colaboradores obrigam-se a reportar tal falta ao Diretor de Risco e *Compliance*, sob pena de ser considerado corresponsável com o infrator.

O Diretor de Risco e *Compliance* visa a promover a aplicação da presente política, bem como o controle, a supervisão e a aprovação de exceções em relação à mesma, sendo responsabilidade deste Diretor assegurar a implementação de mecanismos eficientes capazes de resguardar o sigilo das Informações Confidenciais, bem como a identificação de quaisquer infrações às regras aprovadas na forma da presente política.

SEGURANÇA DA INFORMAÇÃO

Todos os Colaboradores da Sociedade têm a obrigação de zelar pelo sigilo das Informações Confidenciais, devendo observar as seguintes regras para tanto:

(i) Em nenhuma hipótese o profissional deverá, durante a vigência de sua prestação de serviços à Sociedade e mesmo após o término de seu contrato, transmitir ou revelar a qualquer pessoa, empresa, sociedade ou negócio, nem usar por sua própria conta, sem a aprovação escrita da Sociedade, qualquer informação relativa aos negócios e clientes recebida durante seu vínculo com a Sociedade, ou recebida de qualquer empresa direta ou indiretamente a ela relacionada;

(ii) Todos os dados recebidos serão tratados como Informações Confidenciais, devendo manter sigilo sobre as operações realizadas e os nomes de clientes;

(iii) Todas as listas de clientes, orientações e dados sobre vendas e serviços, operações e negócios, bem como todos os demais papéis, registros e documentos elaborados seja pela empresa, pelo profissional, ou que estejam em poder desse durante seu vínculo empregatício ou de alguma forma a ele pertinente, deverão ser devolvidos a Sociedade por ocasião do término do contrato de trabalho ou em qualquer tempo, sendo vedada a reprodução de cópias ou de arquivos eletrônicos com tais conteúdos;

(iv) O profissional é responsável pela guarda e boa conservação de todos e quaisquer documentos que estiverem sob sua responsabilidade durante a

execução de seu trabalho. O profissional será pessoalmente responsável no caso de quebra de sigilo a pessoas não autorizadas;

(v) O profissional reconhece que a violação, no todo ou em parte, de qualquer dos itens acima, constitui-se motivo para a rescisão por justa causa de seu contrato de trabalho com a Sociedade e caso ainda vigente, em conformidade com o Artigo 482, letra "g" da Consolidação das Leis do Trabalho e com os dispositivos aplicáveis contidos na legislação civil e criminal;

(vi) A Sociedade mantém arquivos separados eletronicamente, para cada área. Os diretórios de cada área são acessados conforme a configuração de acesso de cada Colaborador, sendo que os Colaboradores de uma área não têm permissão para criar, editar, alterar ou salvar arquivos armazenados nos diretórios de outras áreas;

(vii) A senha fornecida para acesso às redes de dados institucionais, incluindo os diretórios de acesso restrito, é pessoal e intransferível, sendo vedada a sua divulgação a outras Colaboradores ou terceiros;

(viii) Tendo em vista a alta especialização da atividade desenvolvida pela Sociedade, assim como os princípios que regem o mercado de valores mobiliários, é absolutamente vedada a revelação de carteiras e estratégias de investimento de todo e qualquer produto administrado e/ou gerido pela sociedade a qualquer não integrante da Sociedade, seja da Imprensa, de círculo pessoal de convívio, de ligação imediata de parentesco ou de estado civil, exceto nas formas da lei e com autorização da diretoria;

(ix) É também vedada a utilização de informações privilegiadas ("*Inside Information*"), assim entendidas informações não públicas a respeito de empresas de capital aberto e negociadas em bolsas de valores, e que façam parte do universo potencial de investimentos das estratégias da Sociedade. Todo Colaborador que, mesmo que involuntariamente, obtiver acesso a informações privilegiadas, deverá comunicá-las imediatamente à Diretoria, que poderá restringir a negociação com ativos relacionados à informação obtida até que sejam confirmadas publicamente ou desmentidas;

(x) Os profissionais devem proteger os ativos da empresa e assegurar o seu uso eficiente. Os ativos serão utilizados prioritariamente para fins do negócio. Qualquer suspeita de fraude ou roubo de ativos deve ser reportado à Diretoria imediatamente. Ativos da Sociedade incluem o seu capital, suas instalações, seus equipamentos, informação proprietária e intelectual, tecnologia, seu "*business plan*", ideias de novos produtos ou negócios, material e lista de clientes entre outros;

(xi) Os equipamentos e computadores disponibilizados aos Colaboradores da Sociedade devem ser utilizados com a finalidade prioritária de atender aos interesses comerciais legítimos da Sociedade;

(xii) A obtenção de cópias de arquivos de qualquer extensão, de forma gratuita ou remunerada, em computadores da Sociedade, originados em máquina remota ("*Download*") deverá observar os direitos de propriedade intelectual pertinentes tais como *copyright*, licenças e patentes. Arquivos eletrônicos, programas ou quaisquer outros materiais mantidos na rede são considerados ativos da sociedade e estão sujeitos a revisões periódicas, monitoramento ou vigilância por parte da empresa; e

(xiii) A Sociedade só autoriza o acesso à internet através de conexões aprovadas, não podendo o profissional fazer uso de conexões dial-up ou outros meios não aprovados. O profissional deve usar o bom senso e julgamento quando fizer uso de internet durante o horário de trabalho, quando o mesmo não for por interesse da sociedade.

Ao Colaborador, é vedado:

(i) Transmitir, copiar ou fazer download de quaisquer materiais, incluindo imagens, com conotações sexuais explícitas ou não, ou mensagens ou materiais que tragam conteúdo racista ou sexista, que possam embaraçar, ofender, ameaçar ou prejudicar um profissional, um cliente ou o público em geral;

(ii) Transmitir, postar, copiar, ou fazer download de "*copyright*" sem o devido consentimento do proprietário do material;

(iii) Transmitir ou postar informações não públicas sobre a Sociedade;

(iv) Tentar conseguir acesso a qualquer computador, base de dados ou rede sem a devida autorização;

(v) Transmitir vírus de forma intencional ou outros programas não autorizados;

(vi) Distribuir mensagens de e-mails que configurem correntes, spam, propagandas, etc.;

(vii) Criar um endereço de e-mail ou um domínio que seja derivado ou similar ao nome da Sociedade;

(viii) O uso de senhas é confidencial e as mesmas, não devem ser distribuídas ou comunicadas a terceiros sob nenhuma hipótese;

(ix) Uso de e-mail da Sociedade deve ser feito com bom senso e julgamento; e

(x) Toda comunicação eletrônica relacionada ao negócio deve ser feita através da rede de comunicação da Sociedade, não sendo permitido o envio de documentos, programas ou outros arquivos através de “hotmails” ou outros servidores que possam ser acessados através da Internet.

O correio eletrônico disponibilizado pela Sociedade caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo de utilização preferencial para alcançar os fins comerciais aos quais se destina. É permitida a utilização pessoal de forma moderada, desde que tais comunicações estejam de acordo com as regras descritas neste documento.

Não obstante, mensagens enviadas ou recebidas através do correio eletrônico corporativo, seus respectivos anexos, e a navegação na internet através de equipamentos da Sociedade poderão ser monitoradas sem qualquer aviso ao profissional.

Nenhum profissional está autorizado a falar com o público, dar entrevistas, prestar informações ou afins, seja a Imprensa, escrita ou falada, reguladores, fiscais, ficando essa função de responsabilidade exclusiva da Diretoria ou por alguém explicitamente aprovado pela Diretoria.

As regras dispostas nesta política visam a estabelecer regras que orientem o controle de acesso a Informações Confidenciais pelos Colaboradores, inclusive através do estabelecimento de regras para a utilização de equipamentos e e-mails da empresa, para gravação de cópias de arquivos, para *download* e instalação de programas nos computadores da empresa dentre outras.

11. POLÍTICA DE SEGURANÇA CIBERNÉTICA

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação da Sociedade, permitindo agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas da Sociedade.

Tendo isso em vista, esta Política de Segurança Cibernética tem por objetivo mitigar os riscos de uma ameaça cibernética por meio da implementação de um programa de segurança cibernética que contempla os seguintes aspectos: (i) identificação e avaliação dos riscos internos e externos aos quais a Sociedade está sujeita, os ativos de hardware e software e os processos que precisam de proteção; (ii) estabelecimento de ações de prevenção e proteção; (iii) monitoramento das ameaças em tempo hábil; (iv) criação de um plano de resposta; e (v) reciclagem e revisão do programa de segurança cibernética.

O Diretor de Risco e *Compliance* será o responsável para tratar e responder questões relacionadas à segurança cibernética.

Qualquer processo ou ativo classificado como Informação Confidencial será considerado vulnerável para fins de segurança cibernética, sendo classificado internamente com alto grau de ameaça institucional em caso de eventual ataque cibernético.

Nesse sentido, a área de *compliance*, juntamente com a empresa, contratada pela gestora, especializada na prestação de serviços de tecnologia da informação realiza ações de prevenção e proteção de tais ativos, por meio dos procedimentos elencados na Política de Segurança de Sigilo das Informações. Adicionalmente, ressalta-se que a Sociedade trabalha com (i) backup dos seus arquivos; (ii) sistema de firewall e antivírus; (iii) restrição de instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos; e (iv) acesso restrito a páginas na rede mundial de computadores.

Para fins de monitoramento, a empresa Sociedade da gestora realiza, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades.

Adicionalmente, a Sociedade (i) mantém inventários atualizados de hardware e software por ela detidos; (ii) mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizados; (iii) monitora diariamente as rotinas de backup, executando testes regulares de restauração dos dados; e (iv) analisa regularmente os logs e trilhas de auditoria criadas, de forma a permitir a rápida identificação de ataques, sejam internos, sejam externos.

No caso concreto de um ataque cibernético amplo nas redes da Sociedade, a área de *compliance* e a empresa Sociedade deverão contatar imediatamente os Colaboradores chaves da Sociedade, no menor tempo possível. Neste cenário, os Colaboradores da Sociedade deverão utilizar instalações de contingência até a normalização dos serviços, as quais obedecerão às regras de controle de acesso previstas na Política de Segurança e Sigilo de Informações.

Em se tratando de um ataque individual a um determinado Colaborador, a Sociedade deverá disponibilizar novos equipamentos para a continuidade da prestação dos serviços por parte daquele Colaborador.

Todo e eventual incidente cibernético deverá ser documentado por escrito em relatório elaborado pela área de *compliance*, no qual constarão as descrições do incidente e as medidas tomadas pela Sociedade para resolver tal incidente, e deverá ser arquivado na sede da Sociedade para fins de evidência em eventuais questionamentos.

Os procedimentos previstos nesta Política de Segurança Cibernética, conforme mencionados anteriormente, serão revisados anualmente pela Sociedade, ou quando houver alteração na regulação referente à segurança cibernética. Em tais revisões, serão atualizadas as avaliações de riscos, vulnerabilidades e ameaças identificadas originalmente.

12. DEMAIS CONSIDERAÇÕES

Quaisquer dúvidas ou solicitação de esclarecimento relacionados a este Manual ou a quaisquer outras políticas internas da Sociedade, podem ser endereçadas ao Diretor de Risco e *Compliance*.

ANEXO I

TERMO DE ADESÃO AO MANUAL DE CONTROLES INTERNOS E *COMPLIANCE* E DEMAIS POLÍTICAS INTERNAS DA SQUALO CAPITAL GESTORA DE RECURSOS LTDA.

Eu, [●], portador da Cédula de Identidade nº [●], inscrito no CPF sob o n° [●], declaro para os devidos fins que:

(i) Recebi uma versão atualizada do Manual de Controles Internos e *Compliance* e das demais políticas internas ("Políticas") da SQUALO CAPITAL GESTORA DE RECURSOS LTDA. ("Gestora"), cujas regras e políticas me foram previamente explicadas e em relação às quais tive oportunidade de tirar todas as dúvidas existentes, tendo ainda lido e compreendido todas as diretrizes estabelecidas em tais documentos, me comprometendo a observar integralmente seus termos no desempenho de minhas funções;

(ii) Estou ciente de que as Políticas passam a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras de conduta adotadas pela Gestora;

(iii) Tenho absoluto conhecimento sobre a Política de Segurança da Informação e autorizo expressamente a Gestora a realizar gravação de todas as conversas pelas linhas telefônicas da sociedade, bem como a monitorar todas as comunicações realizadas via e-mail corporativo, internet, chat, etc.;

(iv) Sei que, a partir desta data, a não observância dos termos estabelecidos nas Políticas poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão por justa causa;

(v) As regras estabelecidas nas Políticas da Gestora não invalidam nenhuma disposição relativa a qualquer norma interna estabelecida pela Gestora, mas apenas servem de complemento e esclarecem como lidar com determinadas situações na execução de minhas atividades profissionais;

(vi) Em [●] de [●] de [●], participei do treinamento específico realizado em consonância com disposto no Manual de Controles Internos e *Compliance*,

sendo que compreendi perfeitamente as regras estabelecidas nas Políticas, bem como na legislação e regulamentação em vigor, comprometendo-me a observar integralmente os termos e condições que me foram apresentados.

São Paulo/SP, [●] de [●] de [●].

_____

[●]