POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS

IRIDIUM GESTÃO DE RECURSOS LTDA.

ÍNDICE

POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS

Razão Social: Iridium Gestão de Recursos Ltda. ("Iridium" ou, simplesmente, "Gestora")
CNPJ/MF nº 27.028.424/0001-10
Site: http://www.iridiumgestao.com.br

PARTE A - ASPECTOS GERAIS

1. INTRODUÇÃO

A Diretoria de Compliance da Iridium é responsável pela elaboração, implementação e manutenção do programa de compliance ("Programa de Compliance") da Gestora. O Programa de Compliance inclui regras, políticas e procedimentos ("Políticas"), que atendem a regulamentações vigentes, processos referentes à revisão e atualização periódica das políticas e códigos constantes deste manual ("Revisão Periódica"), implementação de controles internos e testes de aderência ("Controles") para monitorar a efetividade das Políticas, e condições de realização de treinamentos aos sócios e colaboradores ("Treinamento").

O Programa de Compliance da Iridium foi desenvolvido a fim de cumprir as obrigações estabelecidas nas normas da Comissão de Valores Mobiliários ("CVM"), especialmente a Instrução CVM nº 301/1999, a Instrução CVM nº 555/2015 e a Instrução CVM nº 558/2015, e nas normas da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") às quais a Iridium seja aderente, especialmente o Código de Regulação e Melhores Práticas de Fundos de Investimento ("Código de Fundos").

2. GOVERNANÇA

A. Comitê de Compliance

A Iridium conta com um Comitê de Compliance com autonomia sobre as questões de compliance da mesma. Seguem abaixo as características deste comitê:

Competência: Análise e revisão dos limites e o enquadramento das carteiras de valores mobiliários sob administração (gestão); criação, revisão e cumprimento de regras, políticas, procedimentos e controles internos; e o acompanhamento de questões regulatórias, autorregulatórias e legislações do mercado de capitais. Adicionalmente, o Comitê visa a apurar e tomar determinadas decisões e aprovações de compliance, quanto à Prevenção à Lavagem de Dinheiro e ao Combate ao Financiamento do Terrorismo ("PLD"). Por fim, o Comitê também pode tratar a respeito de assuntos sobre Cibersegurança.

Composição: Gestor, Diretor de PLD e Compliance, Equipes de gestão e Analista de RI.

Frequência: Mensal ou quando for necessário.

Decisões: As decisões do Comitê de Compliance são tomadas pelo voto da maioria dos seus membros e deverão ter o voto favorável do Diretor de PLD e Compliance, a quem sempre será garantido o poder final de decisão em matérias de gestão de compliance. Em relação a medidas corretivas e medidas emergenciais, o Diretor de Compliance poderá decidir monocraticamente, sujeito à ratificação do Comitê.

Forma de registro das decisões: Registro em ata, as quais deverão ser assinadas pelos membros presentes à reunião, devendo permanecer arquivadas na sede da Gestora.

B. Diretoria de Compliance

Competência: A Diretoria de Compliance da Iridium tem competência para:

- Assegurar que os colaboradores, sócios e prestadores de serviços, ajam de acordo com os melhores interesses dos investidores e com integridade em relação ao mercado;

- Evitar a prática de condutas que possam afetar ou prejudicar a imagem da Iridium, dos seus sócios e colaboradores, e dos mercados financeiros e de capitais;

- Prestar ativamente assessoria aos sócios e colaboradores em relação a assuntos regulatórios e promover continuamente a cultura de ética e compliance; e

- Administrar o relacionamento com agentes fiscalizadores, reguladores e de autorregulação.

Garantia de independência: A Diretoria de Compliance da Iridium é independente, podendo empregar seus poderes com relação à qualquer sócio ou colaborador da Gestora. Não obstante, a Diretoria te Compliance transmite reportes periódicos ao Comitê Executivo.

Por fim, apesar da existência da área de Compliance, os sócios e colaboradores da Iridium devem sempre agir de forma diligente e de acordo com as melhores práticas.

C. Diretor responsável pela diretoria de compliance ("Diretor de Compliance")

Antonio Carlos da Rocha Conceição é o diretor responsável pela Diretoria de Compliance na Iridium, o que inclui a responsabilidade pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos no Artigo 22 da Instrução CVM nº 558/2015. Por fim, ele também acumula a função de diretor

responsável pelo risco (“Diretor de Risco”) e controles internos que visam o combate e a prevenção a Lavagem de Dinheiro (PLD) (“Diretor de PLD”).

Na execução das atividades sob sua responsabilidade estabelecidas nesta política, o Diretor da Diretoria de Compliance poderá se utilizar de sistemas eletrônicos e/ou serviços de advogados ou firmas de consultoria de compliance para suporte e auxílio em suas funções.

O Diretor de Compliance tem a responsabilidade pelo cumprimento desta Política. Nos casos em que entender que haja fundada suspeita em dissonância com o previsto nesta Política, deve submeter estes a apreciação do Comitê de Compliance, para que sejam tomadas as medidas cabíveis.

O Comitê de Compliance e a Diretoria de Compliance são independentes das outras áreas da empresa e poderão exercer seus poderes em relação a qualquer sócio ou colaborador.

3. CRIAÇÃO, REVISÃO E CUMPRIMENTO DE REGRAS, POLÍTICAS, PROCEDIMENTOS E CONTROLES INTERNOS

Para que a Iridium mantenha as melhores práticas e cumpra os requisitos legais e regulatórios, é de responsabilidade da Diretoria de Compliance a criação de um Programa de Compliance (“Programa”) que compreenda as seguintes regras, políticas, procedimentos e controles internos:

- Política de Compliance e Controles Internos, incluindo:
    - Política de prevenção de conflitos de interesse;
    - Política de negociações da gestora;
    - Política de segregação de atividades e/ou de áreas;
    - Política de confidencialidade e segurança de informações;
    - Política de contratação de terceiros; e
    - Política de treinamento de colaboradores.
- Código de Ética e Padrões de Conduta Profissional;
- Política de Combate ao Suborno e Corrupção;
- Política de Investimentos Pessoais;
- Política de Prevenção à Lavagem de Dinheiro (PLD); e

- Política Operacionais, incluindo:
    - Política de voto;
    - Política de rateio de ordens; e
    - Política de certificação.

É de responsabilidade da Diretoria de Compliance a supervisão do cumprimento deste Programa pelos sócios, colaboradores e prestadores de serviços contratados da Iridium. Adicionalmente, a Diretoria de Compliance também é responsável pela elaboração do relatório de conclusão de controles internos de que trata o Artigo 22 da Instrução CVM nº 558/2015 ("Relatório Anual de Compliance"), o qual deverá ser entregue à administração da Gestora até 31 de março de cada ano, referente aos processos de compliance verificados no ano-civil imediatamente anterior. O Relatório Anual de Compliance deverá ser arquivado na sede da Iridium, permanecendo disponível para eventual consulta pela CVM.

Ao menos uma vez por ano, a Diretoria de Compliance deverá conduzir uma revisão completa de todo o Programa de Compliance.

4. DISPONIBILIZAÇÃO DA POLÍTICA

Em cumprimento ao Inciso III do Artigo 14 da Instrução CVM nº 558/2015, a presente Política de Compliance e Controles Internos está disponível no seguinte endereço eletrônico:

http://www.iridiumgestao.com.br

Adicionalmente, a mesma Política também está disponível na intranet da Gestora através do endereço abaixo para o acesso de todos os seus sócios e colaboradores.

Z:\Manuais & Políticas\Vigentes

5. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, e será alterada quando necessário e sem aviso prévio. As alterações serão divulgadas a todos os sócios e colaboradores da Iridium pela Diretoria de Compliance e ficarão disponíveis para consulta de qualquer sócio e colaborador na intranet e no website da Iridium acima indicados.

PARTE B - CONFLITOS DE INTERESSES

É de responsabilidade da Diretoria de Compliance o cumprimento do que está disposto no Código de Ética e Padrões de Conduta Profissional da Iridium, no que tange a administração de eventuais conflitos de interesses, reais e potenciais.

Deste modo é de responsabilidade da Diretoria de Compliance deliberar e recomendar eventuais sanções aos sócios e colaboradores da Iridium sobre situações que possam ser caracterizadas como de conflitos de interesses, tanto pessoais como profissionais. Esses conflitos podem acontecer, inclusive, mas não se limitando, às seguintes situações endereçadas em políticas próprias: investimentos pessoais, atividades externas, presentes e entretenimentos, contribuições políticas, transações com partes relacionadas, contratação de fornecedores ou prestadores de serviços que tenham vínculo com partes relacionadas, alocações de oportunidades e despesas entre veículos geridos, dentre outros exemplos.

1. ASPECTOS GERAIS

A. Definição

Conflitos de interesses são todas as circunstâncias em que relacionamentos ou fatos relacionados aos interesses pessoais puderem interferir na objetividade e isenção necessária na forma de atuação Gestora, tornando os negócios incompatíveis.

B. Exemplos

São exemplos de conflitos de interesses as situações ou fatos em que há:

- Influência quanto ao julgamento do colaborador atuando em nome da Gestora;
- Desvio de oportunidades de negócios da Gestora;
- Concorrência com a atividade/negócio da Gestora;
- Ocupação significativa do tempo ou da atenção dispensada pelo colaborador, diminuindo sua eficiência e produtividade em relação às suas tarefas profissionais;
- Prejuízo à reputação do colaborador ou à imagem da Gestora; e
- Caracterização de benefícios exclusivos ao colaborador às expensas da Gestora.

C. Dever de prevenir

O colaborador deve evitar a existência de conflitos de interesse, além de atentar cuidadosamente para situações envolvendo familiares ou parentes.

D. Dever de informar

A Gestora preocupa-se em evitar circunstâncias que possam produzir conflito de interesses, seja em situação de colisão de interesses da Gestora com os dos colaboradores, seja com os dos clientes. Em caso de dúvida, o potencial conflito de interesse deverá ser levado ao conhecimento do Comitê, que definirá a linha de ação a ser tomada.

Por fim, a Iridium entende necessário também acompanhar e evitar eventuais conflitos de interesses entre o desempenho da atividade de administração de carteiras e atividades desenvolvidas por outras empresas pertencentes a seu grupo. Desta forma, com a preocupação de manter o maior nível de isenção na condução de seus negócios, na hipótese de originação de oportunidades de negócio à Iridium por qualquer empresa a ela relacionada, o cliente deverá ser informado sobre o relacionamento entre as duas empresas, bem como sobre possível situação de conflito de interesses no caso, respeitadas as previsões normativas específicas.

2. PRESENTES E DIVERSÕES

A. Definições

- "Diversões": refeições de negócios, os eventos esportivos, musicais, culturais, e as recepções privadas, viagens e outros convites ou vantagens econômicas do mesmo gênero; e

- "Presentes": quaisquer gratuidades, favores, descontos, hospitalidade, empréstimos, ou qualquer de valor monetário, assim como treinamento, transporte, viagens domésticas ou internacionais, alojamento e refeições, objetos como brindes, objetos de valor, vantagens econômicas, e descontos.

B. Regra geral

Sócio e colaboradores podem dar e receber Presentes e Diversões desde que não excedam USD 250,00 (duzentos e cinquenta dólares norte-americanos) e não sejam excessivos ou luxuriosos. Tampouco podem os presentes aceitos com a aparência de terem sido ofertados para aumentar a influência sobre quem os recebe. Por fim, os Presentes e Diversões devem ser encarados como cortesia ou parte da estratégia de marketing e divulgação.

Estão vedadas vantagens econômicas quaisquer que forem oferecidas ou recebidas de partes com que a Gestora estiver com negociações pendentes ou em aberto.

C. Dever de informar

Quaisquer Presentes ou Diversões deverão ser sempre informados à Diretoria de Compliance em formulário específicos, inclusive os excessivos ou luxuriosos que estejam abaixo do valor informado acima.

D. Situações específicas

i. Receber diversões em situações de negócios

Sócios e colaboradores podem ser convidados a jantares de negócios, eventos esportivos, e outras Diversões às expensas de prestadores de serviços e parceiros comerciais. Todavia, quaisquer Diversões cujo valor seja superior a USD 250,00 (duzentos e cinquenta dólares norte-americanos) devem ser objeto de consulta prévia e autorização. Em caso de shows e eventos de grande procura em que houver sobrepreço, desconsiderar-se-á o valor de face da atração, e o valor com ágio deve ser utilizado para verificação do limite indicado acima. Caso a Diretoria de Compliance não autorize dentro de sua discricionariedade, ou caso o valor das Diversões ultrapasse USD 250,00 (duzentos e cinquenta dólares norte-americanos), o sócio ou colaborador fica proibido de aceitá-las.

ii. Receber presentes de fornecedores e parceiros comerciais

Sócios e colaboradores podem receber Presentes de fornecedores que não sejam excessivos ou luxuriosos. Todavia, quaisquer Presentes cujo valor agregado anual seja superior a USD 250,00 (duzentos e cinquenta dólares norte-americanos) devem ser objeto de consulta prévia e autorização da Diretoria de Compliance. Para o caso em que o mesmo ofertante presenteie o colaborador com vários Presentes ao longo do ano, o limite indicado acima deve ser calculado como a soma anual dos valores de cada um dos Presentes oferecidos. Caso a Diretoria de Compliance não autorize, ou caso o valor agregado do Presente ultrapasse USD 250,00 (duzentos e cinquenta dólares norte-americanos), o sócio ou colaborador fica proibido de aceitá-lo.

iii. Oferecer presentes ou diversões em situações de negócio

Sócios e colaboradores estão proibidos de oferecer ou custear Diversões e Presentes para clientes e parceiros comerciais. Excepcionalmente a Diretoria de Compliance pode autorizar que (i) refeições de valor inferior a USD 250,00 (duzentos e cinquenta dólares norte-americanos) per capita sejam oferecidos a clientes e parceiros comerciais; (ii) passagens aéreas ou despesas de viagem de valor inferior a USD 250,00 (duzentos e cinquenta dólares norte-americanos), desde que oferecidas em conexão com processos de *due diligence*, ou como reembolso de despesas feitas no estrito curso do trabalho;

ou (iii) brindes de valor inferior a USD 50,00 (cinquenta dólares norte-americanos) sejam oferecidos a clientes como produto de ações de marketing institucional. Neste último caso, todavia, o valor agregado anual de presentes oferecidos a um mesmo cliente não pode ser superior a USD 250,00 (duzentos e cinquenta dólares norte-americanos). Quaisquer outros tipos de Diversões ou Presentes são proibidos.

3. INFORMAÇÃO PRIVILEGIADA

A. Definição

Informação privilegiada ("*insider information*") é definida como aquela que não é de domínio público e que tenha impacto material na avaliação dos ativos de um determinado emissor, ou conjunto de emissores ou do mercado em geral, e que foi obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros).

Exemplos de informações privilegiadas são informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO).

B. Vedações

É vedado aos sócios e colaboradores qualquer tipo de operação em mercado financeiro, que seja realizada de posse de informação privilegiada, seja esta operação para benefício dos fundos geridos, seja para investimentos pessoais. Além disso, é vedada a comunicação de informação privilegiada a terceiros.

C. Dever de comunicar

Caso os sócios e colaboradores tenham acesso, por qualquer meio, a informação privilegiada, deverão levar tal circunstância ao imediato conhecimento da Diretoria de Compliance, indicando, além disso, a fonte da informação privilegiada assim obtida. Tal dever de comunicação também será aplicável nos casos em que a informação privilegiada seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. A Gestora mantém registro de reuniões externas com *asset managers*.

4. MANIPULAÇÃO DE MERCADO

A. Definição

São definidas como "Manipulação de Mercado" as práticas ou dispositivos que, mesmo que potencialmente, interfiram no correto funcionamento do mercado de valores mobiliários. São proibidas, nos termos da Instrução CVM nº 8/79 quatro tipos principais de infrações:

- Criação de condições artificiais de demanda: condições criadas em decorrência de negociações pelas quais seus participantes ou intermediários, por ação ou omissão dolosa provocarem, direta ou indiretamente, alterações no fluxo de ordens de compra ou venda de valores mobiliários;

- Manipulação de preços no mercado de valores mobiliários: a utilização de qualquer processo ou artifício destinado, direta ou indiretamente, a elevar, manter ou baixar a cotação de um valor mobiliário, induzindo, terceiros à sua compra e venda;

- Operação fraudulenta no mercado de valores mobiliários: operação em que se utilize ardil ou artifício destinado a induzir ou manter terceiros em erro, com a finalidade de se obter vantagem ilícita de natureza patrimonial para as partes na operação, para o intermediário ou para terceiros; e

- Prática não equitativa no mercado de valores mobiliários: prática de que resulte, direta ou indiretamente, efetiva ou potencialmente, um tratamento para qualquer das partes, em negociações com valores mobiliários, que a coloque em uma indevida posição de desequilíbrio ou desigualdade em face dos demais participantes da operação.

B. Tipos

Entre as formas de Manipulação de Mercado catalogadas, encontram-se as seguintes práticas:

- "Zé-com-zé" ("*Wash Trades*"): comprar e vender a mesma ação de modo a mover os preços praticados nos mercados;

- "*Pools*": acordos dentro de um mesmo grupo de traders para delegar a um gestor os poderes para negociar uma ação específica por um período determinado de tempo;

- "*Churning*": entrar com ordens de compra e venda no mesmo preço;

- "*Stock Bashing*" ou "*Pump and Dump*": fabricar informações falsas ou enganosas sobre um ativo com o objetivo de aumentar ou deprimir o preço, e realizar uma venda ou uma compra após a mudança de preço;

- "*Bear Raid*": vender a descoberto uma ação ou utilizar informações negativas para conseguir ganhos de curto prazo;

- "*Lure and Squeeze*": vender ação de empresa em problemas com o conhecimento de que tal empresa utilizará ações para solucionar sua situação com credores.

C. Ações preventivas e integridade do processo de investimento

Como forma de proteção, a Gestora também busca preservar a integridade do processo de investimento de modo a garantir que decisões de compra e venda de ativos sejam baseadas em análises aprofundadas e que sejam devidamente registradas e documentadas por evidências. São dois os tipos de integridade:

- Integridade em investimentos de longo prazo, baseada na análise fundamentalista de ativos; e

- Integridade na análise, baseada em material original ou proprietário produzido pela própria Gestora, processo endógeno de obtenção de informações sobre ativos e companhias, e proteção de informações privilegiadas.

D. Mecanismos de proteção

A Gestora utiliza-se dos seguintes mecanismos específicos de prevenção de manipulação:

- Controle de fluxos de informações;

- Monitoramento de traders e centralização das ordens em nome da Iridium;

- Detecção de atividades suspeitas e atividades de risco;

- Treinamento e orientação de colaboradores; e

- Política de negociações pessoais restritivas, com disclosure mandatório de operações.

PARTE C - NEGOCIAÇÕES DA GESTORA

1. ASPECTOS GERAIS

A Gestora pode alocar recursos em fundos de investimento administrado (gerido) por terceiros e pode também negociar ativos em mercado, executando ordens e operando com corretoras.

Como agente dos fundos, destarte, tem responsabilidade fiduciária de agir para conseguir, nas circunstâncias de mercado, preços e condições de execução mais favoráveis para negócios com valores mobiliários em nome de clientes e carteiras administrada (geridas) por ela. Deve, deste modo, cultivar transparência e franqueza em relação a potenciais conflitos de interesse, práticas de remuneração, benefícios indiretos, e outros fatores que possam interferir na escolha de prestador de serviço. Por essa razão, mantém política de *best execution*, buscando os melhores interesses de seus clientes.

2. OBJETIVOS

Os objetivos da Política de Negociações da Gestora são os seguintes:

- Obter, nas circunstâncias existentes de mercado, best execution;
- Prevenir conflitos de interesse e o uso dos ativos dos clientes em benefício de terceiros;
- Prevenir e evitar o envolvimento de colaboradores em situações apresentando riscos de violações de deveres fiduciários;
- Permitir a detecção de riscos potenciais de violações da política;
- Reprimir ações que criem riscos para a ética, integridade e reputação;
- Reduzir o custo de enforcement interno; e
- Orientar e treinar colaboradores para identificar, prevenir, evitar e reprimir situações de risco e violações à política.

3. DEVERES

Os deveres principais da Gestora em relação à *best execution* são os seguintes:

- Dever de considerar preços, custos, velocidade, probabilidade de execução e liquidação, tamanho, natureza de ordens e quaisquer outros elementos relevantes para a estratégia;
- Dever de colocar os interesses dos clientes acima de seus próprios;

- Dever de minimizar o risco de conflito de interesse;

- Dever de ativamente evitar transações conflitadas, arranjos de soft-dollar, e negociações paralelas sem a necessária transparência e consentimento do interessado; e

- Dever de reverter todo e qualquer benefício direta ou indiretamente recebidos em relação à execução de ordens de clientes.

4. MECANISMOS ESPECÍFICOS

A política de *best execution* da Gestora é baseada em três mecanismos principais:

- Pré-autorização de corretoras baseada em critérios objetivos e rotinas de avaliação: a Gestora somente opera com corretoras pré-selecionadas com base nos seguintes critérios:

    - Capacidade de execução e habilidades da corretora (habilidade de executar trades de diferentes tamanhos, tipos e papel);

    - Confiabilidade dos sistemas de comunicação e negociação da corretora;

    - Comissões e descontos; e

    - Reputação e saúde financeira da corretora e de seu grupo financeiro.

- Revisão periódica de políticas: revisão periódica e sistemática das políticas de corretoras autorizadas; e

- Recusa de vantagens e serviços em troca de preferência de execução: A Gestora não aceita serviços que não sejam pesquisa (quaisquer serviços proibidos, "Serviços Proibidos").

5. COMITÊ DE BEST EXECUTION

Para estruturar sua política de *best execution*, a Gestora formou um comitê encarregado de realizar o direcionamento de fluxo de trade. O comitê tem poderes para: avaliar se há conflito de interesse entre a Gestora e uma contraparte, estabelecer critérios para avaliar a qualidade da execução de ordens, e realizar o acompanhamento, selecionar, avaliar e classificar corretoras e contrapartes em vista dos serviços de execução buscados e estabelecer balizas para o *trader* direcionar o fluxo de negócios. O comitê é formado pelo Gestor, Diretor de Compliance e equipe de análise. O comitê reunir-se-á ordinariamente, trimestralmente, e extraordinariamente, quando houver necessidade.

6. EXECUÇÃO DE ORDENS

A execução de ordens procura fazer com que as alterações de posição se dê de maneira eficiente, com minimização de custos e execução aos preços desejados. Hoje a gestora mantém uma lista de corretoras, da qual solicita três diferentes cotações, sendo escolhida a de taxas mais baratas e maior velocidade de execução. As ordens podem ser colocadas por telefone ou sistema eletrônico.

PARTE D - SEGREGAÇÃO DE ATIVIDADES E/OU DE ÁREAS

1. ASPECTOS GERAIS

A Iridium mantem a devida segregação entre as suas diversas áreas, bem como das demais empresas pertencentes ao mesmo grupo, e implementa controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

É de responsabilidade da Diretoria de Compliance garantir a segregação de atividades e/ou de áreas que contenham conflitos de interesses. Deste modo, é de responsabilidade da Diretoria de Compliance segregar áreas de negócio e/ou criar restrições de fluxo de informações confidenciais, que contenham potenciais conflitos de interesses. Esta segregação pode ser feita de forma física e/ou de processos.

2. SEGREGAÇÃO

A Iridium adota as seguintes formas de segregação de negócios e/ou de processos:

A. Segregação de atividades e funções

Implementou-se um sistema de segregação de atividades baseado nas diferenças funcionais de atuação e autoridades definidas para as posições de Gestor, Analistas, Relações com Investidor, Compliance, Risco e Administrativo. Perfis de acesso físico e eletrônico, e o controle são realizados com base nessas divisões. Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade ("*as-needed basis*") no Comitê de Compliance, sendo que os participantes se responsabilizam pelo sigilo das informações.

B. Segregação física

A segregação física é feita através do uso de controles de acesso entre as áreas de trabalho da Iridium. A liberação de acesso e o monitoramento destes são realizados pela

Diretoria de Compliance, que avalia quais as áreas cada sócio ou colaborador necessita ter acesso para o exercício de suas atividades. Por fim, apenas a Diretoria de Compliance tem acesso a área onde estão localizados os servidores de dados e comunicação da Iridium.

Áreas confidenciais e/ou com conflito de interesses separadas por função ou espaço. Por exemplo: uso de portas com controles de acessos para segregar espaços físicos. Segrega-se fundamentalmente a área de análise da área de relação com investidores. Além disso, as áreas comuns da Gestora também são segregadas, e o acesso a tais salas é permitido apenas com solicitação prévia e registro. O acesso de pessoas que não fazem parte do quadro de colaboradores será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração, e desde que acompanhadas de colaboradores. O atendimento a clientes nas dependências da Gestora deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

C. Segregação eletrônica

A Gestora implementou uma estrutura de rede que permite restrição de acesso a informação entre áreas confidenciais e/ou com conflito de interesses. A segregação virtual, que envolve a rede, sistemas e dados, é feita através do uso de controles de acesso entre as áreas de trabalho da Iridium. A liberação de acesso e o monitoramento destes são realizados pela Diretoria de Compliance, que avalia quais as áreas cada colaborador necessita ter acesso para o exercício de suas atividades. Apenas a Diretoria de Compliance tem acesso a criação de usuários e a rede localizada nos servidores de dados e comunicação da Iridium.

Cada colaborador tem seu perfil de utilização, que é controlado pela área de compliance em colaboração com a área de tecnologia da informação da Gestora. Além disso, usam-se redes de dados segregadas para os computadores dessas áreas. Há restrição de acesso a sistemas entre áreas confidenciais e/ou com conflito de interesses, exemplo, uso de redes com sistemas segregadas para os computadores dessas áreas.

PARTE E - POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DE INFORMAÇÕES

1. ASPECTOS GERAIS

A. OBJETO

Esta política tem por escopo proteger as informações sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme o Parágrafo 8º do Artigo 4º da Instrução CVM nº 558/2015.

Confidencialidade é um princípio fundamental e aplica-se a quaisquer informações não-públicas referentes aos negócios da Iridium, como também a informações recebidas de seus clientes, contrapartes ou fornecedores da Iridium durante o processo natural de condução de negócios. Os colaboradores não devem transmitir nenhuma informação não-pública a terceiros.

Deste modo, nenhuma informação considerada sigilosa deve ser divulgada, dentro ou fora da Iridium, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais. Adicionalmente, qualquer informação sobre a Iridium, ou de qualquer natureza relativa as suas atividades ou a de seus sócios, colaboradores e clientes só poderá ser fornecida ao público, mídia ou a demais órgãos, caso autorizado pela Diretoria de Compliance.

B. RESPONSABILIDADE

É de responsabilidade da Diretoria de Compliance o controle da disseminação de informações confidenciais. Informações confidenciais e/ou privilegiadas só podem ser repassadas a outras áreas e terceiros, que não tinham acesso a tais, com a prévia autorização da Diretoria de Compliance. Adicionalmente é de responsabilidade da Diretoria de Compliance supervisionar o cumprimento das regras de disseminação de informações confidenciais por meio do monitoramento dos sócios e colaboradores quanto aos meios de comunicação.

A Diretoria de Compliance tem a responsabilidade pela implementação e monitoramento desta política. Todos os colaboradores da Iridium têm o dever de:

- Obedecer a política de segurança da informação;
- Proteger informações sigilosas contra o acesso, modificação, destruição ou divulgação não autorizada pela Iridium;
- Seguir as leis e normas que regulamentam os aspectos relacionados à propriedade intelectual no que se refere às informações sigilosas;
- Assegurar que os recursos da Iridium a sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela mesma;
- Buscar orientação do superior hierárquico em caso de dúvidas relacionadas a segurança das informações sigilosas; e
- Comunicar imediatamente a Diretoria de Compliance a respeito de qualquer descumprimento ou violação da política de segurança da informação.

2. DIRETRIZES

A. COMPORTAMENTO SEGURO

Os sócios e colaboradores da Iridium deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Os sócios e colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

O disposto no presente capítulo deve ser observado durante a vigência do relacionamento profissional do colaborador com a Iridium e também após seu término

Todos os sócios e colaboradores da Iridium têm o dever de adotar a postura de comportamento seguro, que consiste nos seguintes itens:

- Assumir atitude proativa e engajada a respeito da proteção de informações consideradas sigilosas;

- Compreender as ameaças externas que podem afetar a segurança das informações sigilosas, tais como ataques de vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos e etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e servidores;

- Não discutir assuntos relacionados à Iridium e ao desempenho de suas atividades em ambientes públicos ou áreas expostas;

- Não transferir, compartilhar ou divulgar a terceiros as senhas de acesso a sistemas da Iridium;

- Não anotar em papel ou em sistemas visíveis as senhas de acesso a sistemas da Iridium;

- Bloquear seus computadores sempre que ausentarem das estações de trabalho;

- Não instalar softwares nas estações de trabalho da Iridium que não foram homologados ou previamente aprovados pela Diretoria de Compliance;

- Não abrir arquivos eletrônicos ou mensagens de e-mail de origem desconhecida;

- Não reproduzir ou disseminar dados da rede de computadores da Iridium; e

- Utilizar o e-mail corporativo e aplicativos de mensagem exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades.

B. POLÍTICAS GERIAS

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da Iridium são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na Iridium e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os sócios e colaboradores tiverem com relação aos clientes da Iridium deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, salvo na hipótese de decisão judicial específica que determine à Iridium a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da CVM. Caso a Iridium ou qualquer dos sócios e colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser seguido de imediata e expressa comunicação aos clientes afetados, caso não haja norma dispondo de forma diversa.

Os sócios e colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Iridium, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Iridium. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração da Iridium, para que sejam tomadas as medidas cabíveis.

A Iridium exige que seus sócios e colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Iridium, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

Todo e qualquer material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Iridium, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do superior hierárquico do sócio ou colaborador. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo sócio e colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

A Iridium concederá autorização para acesso a informações e arquivos apenas que se refiram ao departamento no qual o colaborador atua. Aos sócios e colaboradores que

atuem diretamente na atividade de administração de recursos, haverá além da segregação de acesso por departamento, a concessão de acesso específico para as informações do cliente e/ou do projeto sob responsabilidade de referido sócio ou colaborador.

C. SEGURANÇA DA INFORMAÇÃO

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados, cujo acesso é permitido apenas aos administradores da Iridium, além dos membros do departamento de informática.

Todo software disponibilizado aos sócios e colaboradores deverá ser utilizado somente para os negócios da Iridium, em consonância com os acordos de licenciamento firmados.

É realizado de back up de todas as informações e armazenadas em nuvem, em um HD externo e no CPD com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

O acesso aos sistemas de informação da Iridium é feito por meio de um par "usuário/senha" que permite ao responsável pelo departamento de informática acompanhar, de forma precisa as atividades desenvolvidas por cada um dos colaboradores. O controle desses dados é de domínio da Iridium, uma vez que o armazenamento dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

Todos os acessos concedidos são avaliados conforme o envolvimento de cada colaborador com clientes e/ou projetos específicos. Desta forma, a concessão de acesso às informações obtidas para o exercício da atividade de administração observará dois critérios:

- Acesso restrito apenas aos colaboradores envolvidos com a atividade de administração de carteiras, sendo, portanto, inacessíveis aos colaboradores de áreas administrativas da Iridium; e

- Dentre os colaboradores atuantes na área de administração de recursos, o acesso às informações será limitado apenas aos colaboradores que efetivamente atuem com determinado cliente e/ou projeto, de forma que apenas terão acesso às informações os colaboradores estritamente necessários para o desempenho da atividade em questão.

Para tanto, serão criados nos servidores próprios ou na nuvem diretórios específicos, a partir dos quais será possível controlar a concessão de acessos de acordo com as regras estabelecidas.

Todo sócio ou colaborador que tiver acesso aos sistemas de informação da Iridium é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O sócio ou colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não divulgá-los a terceiros em qualquer hipótese.

A Iridium se reserva o direito de proibir o uso de telefones celulares na área de gestão e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Iridiumou utilizados em nome dela, a fim de assegurar o fiel cumprimento deste Manual, bem como da legislação em vigor.

D. TESTES PERIÓDICOS

Periodicamente, a Iridium realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

- Verificação do login dos colaboradores;
- Anualmente, altera-se a senha de acesso dos colaboradores;
- Testes no *firewall*;
- Testes nas restrições impostas aos diretórios;
- Manutenção trimestral de todo o *hardware* por empresa especializada em consultoria de tecnologia de informação;
- Manutenção trimestral com a atualização de todo o *software* pela empresa especializada em consultoria de tecnologia de informação; e
- Testes no *back-up* (salvamento de informações) diário, realizado na nuvem, HD externo e no próprio CPD da Iridium.

E. COMUNICAÇÕES

i. Internet

Todos os sócios e colaboradores da Iridium têm o dever de utilizar a internet exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades. O acesso a internet é monitorado permanentemente e os arquivos contendo os registros dos acessos e das tentativas de acesso são

armazenadas pela Iridium, sendo que a Diretoria de Compliance é informada sobre estes acessos e tentativas de acesso.

ii. Telefone

Todos os sócios e colaboradores da Iridium tem o dever de utilizar o sistema de telefonia exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades. O sistema de telefonia é monitorado e gravado pela Iridium, sendo que a Diretoria de Compliance tem acesso a estas gravações.

iii. Aplicativos de mensagem

Todos os sócios e colaboradores da Iridium tem o dever de utilizar os aplicativos de mensagem exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades. Os aplicativos de mensagem são monitorados e gravados pela Iridium, sendo que a Diretoria de Compliance tem acesso a estas gravações.

iv. Mídias externas e/ou portáteis

Todos os sócios e colaboradores da Iridium são proibidos de utilizar mídias externas e/ou portáteis para transferir dados, sistemas e arquivos da rede da Iridium.

Para utilização destes equipamentos, os sócios e colaboradores devem solicitar a Diretoria de Compliance para efetuar esta atividade, dado que apenas esta diretoria tem acesso a este tipo de equipamento. Adicionalmente, esta solicitação precisa ser relacionada aos negócios conduzidos pela Iridium ou para o desempenho das atividades do requisitante.

v. Acesso Remoto

Todos os sócios e colaboradores da Iridium são proibidos de utilizar programas ou aplicativos de acesso remoto.

Para utilização destes aplicativos/programas, os sócios e colaboradores devem solicitar a Diretoria de Compliance para efetuar esta atividade.

vi. Utilização de recursos

Todos os sócios e colaboradores da Iridium têm o dever de não utilizar os recursos disponibilizados pela Iridium como de uso pessoal.

Conforme mencionado neste capítulo, a utilização dos recursos disponibilizados pela Iridium está sujeita ao monitoramento periódico, sem frequência determinada ou aviso

prévio. Adicionalmente, os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto da política de segurança da informação e demais regras internas da Iridium, e, conforme o caso servir como evidência em processos administrativos e/ou legais.

PARTE F - POLÍTICA DE CIBERSEGURANÇA

1. ASPECTOS GERAIS

A. OBJETO

Esta política tem por escopo deliberar a Política de Cibersegurança da Iridium a fim de proteger as informações sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme o Parágrafo 8º do Artigo 4º da Instrução CVM nº 558/2015 e o Guia de Cibersegurança elaborado pela ANBIMA.

B. RESPONSABILIDADE

Como a Iridium se utiliza de um prestador de serviço contratado para administrar a sua área de Tecnologia da Informação - TI, é de responsabilidade da Diretoria de Compliance o gerenciamento e controle de qualidade do serviço prestado por este.

Sendo assim, a Diretoria de Compliance tem através do terceiro contratado a responsabilidade pela implementação e monitoramento desta política, considerando os assuntos abaixo:

- Identificação e avaliação de riscos;
- Ações de prevenção e proteção;
- Monitoramento e testes;
- Criação de um plano de resposta; e
- Reciclagem e revisão.

2. DIRETRIZES

A. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A Iridium, como uma gestora de recursos independente, conta com um servidor de processamento de dados, um servidor de armazenamento de dados e computadores individuais para todos os seus colaboradores para executar todas as suas funções. Adicionalmente, a Iridium conta com uma Intranet desenvolvida para armazenar programas e dados, acesso a internet para os seus computadores e servidores e telefones com um servidor dedicado para a gravação de dados para esses últimos aparelhos.

Dado o tamanho diminuto da Iridium, toda a informação e dado administrado por ela é considerado como confidencial e, logo, a Política de Confidencialidade e Segurança de Informações se aplica a todos esses.

Adicionalmente, com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, a Iridium tomou a decisão conservadora de restringir o uso de sua infraestrutura apenas ao exercício de sua função, o que auxilia na prevenção e diminuição de ataques e ameaças cibernéticas.

Em casos de identificação de ataques e ameaças por parte de seus sócios e colaboradores, a Iridium pede que esses sejam reportados conjuntamente para a Diretoria de Compliance e para a empresa tercerizada responsável por TI. Esses casos depois são reportados no Comitê de Compliance.

B. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Conforme descrito no item acima, toda a infraestrutura da Iridium é utilizada por seus sócios e colaboradores apenas para o exercício de suas funções:

i. Internet

Todos os sócios e colaboradores da Iridium têm o dever de utilizar a internet exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades. O acesso a internet é monitorado permanentemente e os arquivos contendo os registros dos acessos e das tentativas de acesso são armazenadas pela Iridium, sendo que a Diretoria de Compliance é informada sobre estes acessos e tentativas de acesso.

ii. Telefone

Todos os sócios e colaboradores da Iridium tem o dever de utilizar o sistema de telefonia exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades. O sistema de telefonia é monitorado e gravado pela Iridium, sendo que a Diretoria de Compliance tem acesso a estas gravações.

iii. Aplicativos de mensagem

Todos os sócios e colaboradores da Iridium tem o dever de utilizar os aplicativos de mensagem exclusivamente para assuntos relacionados aos negócios conduzidos pela Iridium ou para o desempenho de suas atividades. Os aplicativos de mensagem são monitorados e gravados pela Iridium, sendo que a Diretoria de Compliance tem acesso a estas gravações.

iv. Mídias externas e/ou portáteis

Todos os sócios e colaboradores da Iridium são proibidos de utilizar mídias externas e/ou portáteis para transferir dados, sistemas e arquivos da rede da Iridium.

Para utilização destes equipamentos, os sócios e colaboradores devem solicitar a Diretoria de Compliance para efetuar esta atividade, dado que apenas esta diretoria tem acesso a este tipo de equipamento. Adicionalmente, esta solicitação precisa ser relacionada aos negócios conduzidos pela Iridium ou para o desempenho das atividades do requisitante.

v. Acesso Remoto

Todos os sócios e colaboradores da Iridium são proibidos de utilizar programas ou aplicativos de acesso remoto.

Para utilização destes aplicativos/programas, os sócios e colaboradores devem solicitar a Diretoria de Compliance para efetuar esta atividade.

vi. Utilização de recursos

Todos os sócios e colaboradores da Iridium têm o dever de não utilizar os recursos disponibilizados pela Iridium como de uso pessoal.

Conforme mencionado neste capítulo, a utilização dos recursos disponibilizados pela Iridium está sujeita ao monitoramento periódico, sem frequência determinada ou aviso prévio. Adicionalmente, os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto da política de segurança da informação e demais regras internas da Iridium, e, conforme o caso servir como evidência em processos administrativos e/ou legais.

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados, cujo acesso é permitido apenas aos administradores da Iridium, além dos membros do departamento de informática.

Todo software disponibilizado aos sócios e colaboradores deverá ser utilizado somente para os negócios da Iridium, em consonância com os acordos de licenciamento firmados.

O processo de back-up é realizado da seguinte maneira com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência:

- Banco de Dados: O back-up do banco de dados dos sistemas utilizados pela Iridium é realizado diariamente por esta, com retenção de 30 dias nos servidores da própria Iridium. Adicionalmente, há um processo diário com retenção em nuvem dos últimos 5 anos e que pode ser acessado remotamente. Por fim, existe também um hard drive externo que realiza o back-up diário dos dados do servidor e fica localizado nos servidores da Iridium.

- E-mail: O back-up dos dados de e-mail utilizados pela Iridium é de responsabilidade da Microsoft, feito em nuvem e hospedado nos servidores desta.

- Telefonia: O back-up dos dados de telefonia utilizados pela Iridium é realizado diariamente, com retenção de 30 dias nos servidores da Iridium. Adicionalmente, há um processo diário com retenção em nuvem dos últimos 5 anos.É realizado de back up de todas as informações e armazenadas em nuvem, em um HD externo e no CPD com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

O acesso aos sistemas de informação da Iridium é feito por meio de um par "usuário/senha" que permite ao responsável pelo departamento de informática acompanhar, de forma precisa as atividades desenvolvidas por cada um dos colaboradores. O controle desses dados é de domínio da Iridium, uma vez que o armazenamento dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

Todos os acessos concedidos são avaliados conforme o envolvimento de cada colaborador com clientes e/ou projetos específicos. Desta forma, a concessão de acesso às informações obtidas para o exercício da atividade de administração observará dois critérios:

- Acesso restrito apenas aos colaboradores envolvidos com a atividade de administração de carteiras, sendo, portanto, inacessíveis aos colaboradores de áreas administrativas da Iridium; e

- Dentre os colaboradores atuantes na área de administração de recursos, o acesso às informações será limitado apenas aos colaboradores que efetivamente atuem com determinado cliente e/ou projeto, de forma que apenas terão acesso às informações os colaboradores estritamente necessários para o desempenho da atividade em questão.

Para tanto, são criados nos servidores próprios ou na nuvem diretórios específicos, a partir dos quais será possível controlar a concessão de acessos de acordo com as regras estabelecidas.

Todo sócio ou colaborador que tiver acesso aos sistemas de informação da Iridium é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O sócio ou colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não divulgá-los a terceiros em qualquer hipótese.

Adicionalmente, todos os servidores e computadores da Iridium possuem filtro de e-mail Exchange Online Protection do serviço Office 365 da Microsoft, Firewalls Sophos XG 135W com sistema Sophos Intercept-X operando de forma redundante e sistema antivirus Sophos Endpoint Protection Advanced.

A Iridium se reserva o direito de proibir o uso de telefones celulares na área de gestão e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Iridiumou utilizados em nome dela, a fim de assegurar o fiel cumprimento deste Manual, bem como da legislação em vigor.

C. MONITORAMENTO E TESTES

Periodicamente, a Iridium realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

- Verificação do login dos colaboradores;
- Anualmente, altera-se a senha de acesso dos colaboradores;
- Testes no *firewall*;
- Testes nas restrições impostas aos diretórios;
- Manutenção trimestral de todo o *hardware* pela empresa especializada em consultoria de tecnologia de informação;
- Manutenção trimestral com a atualização de todo o *software* pela empresa especializada em consultoria de tecnologia de informação; e
- Testes no *back-up* (salvamento de informações) diário, realizado na nuvem, HD externo e no próprio CPD da Iridium.

D. CRIAÇÃO DE UM PLANO DE RESPOSTA

No caso de um eventual ciberataque, o procedimento a ser adotado depende do grau de severidade do ataque sofrido:

- Utilização comprometida de um ou mais computadores: Os sócios e colaboradores afetados tem o dever de reportar o problema para a Diretoria de Compliance e conjunto com a empresa tercerizada responsável por TI. Nesse caso, a empresa de TI tem o dever de tentar reparrar o prejuízo causado e o sócio ou colaborador prejudicado, pode trabalhar de um computador notebook ou outro computador desktop sem utilização que a Iridium possui; e

- Utilização comprometida de toda a intranet e/ou de todos os computadores: Os sócios e colaboradores afetados tem o dever de reportar o problema para a Diretoria de Compliance e conjunto com a empresa tercerizada responsável por TI. Nesse caso, a empresa de TI tem o dever de tentar reparrar o prejuízo causado e a Política de Contingência e de Continuidade de Negócios é acionada.

E. RECICLAGEM E REVISÃO

A Diretoria de Compliance em conjunto com a empresa responsável por TI ficam incubidas de produzirem um relatório toda vez que cibersegurança da Iridium for comprometida. Esse relatório é apresentado no Comitê de Compliance e contempla os danos incorridos e as ações tomadas e sugestões para melhora com relação ao procedimento.

PARTE G - POLÍTICA DE CONTRATAÇÃO DE TERCEIROS

1. CRITÉRIOS DE CONTRATAÇÃO

A Gestora pode contratar terceiros para a prestação de determinados serviços relacionados ao objeto social da Gestora, sempre que permitido pela legislação ou regulamentação aplicáveis ao exercício de sua atividade.

Para fins da contratação de terceiros, a Gestora observa os critérios de qualificação técnica, capacidade operacional, licenças, preço e idoneidade do terceiro contratado. A aferição destas condições é realizada através da análise de documentação, e eventual realização de visitas, bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do terceiro contratado. A contratação de futuros prestadores pela Gestora considera a qualificação adequada para cada posição a ser ocupada, e avalia não somente a formação técnica dos candidatos, mas também suas experiências em trabalhos anteriores.

A Iridium, no limite da sua responsabilidade enquanto empregadora ou tomadora de serviços, a depender da situação fática, implementa todos os procedimentos necessários ao monitoramento das atividades prestadas por seus sócios, colaboradores

e prestadores de serviço contratados, sempre balizado no princípio da eficiência, transparência e boa-fé, nos termos da legislação e da regulamentação vigente.

2. DUE DILIGENCE & PROCESSO DE CONTRATAÇÃO

Quando da eventual contratação de prestadores de serviço pela Iridium, nas hipóteses em que a legislação e/ou a regulamentação permitir, o terceiro deve observar os critérios de qualificação técnica, capacidade operacional, licenças, preço e idoneidade. A aferição destas condições é realizada através da análise de documentação, e eventual realização de visitas (*due dilligence*), bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do prestador de serviços contratado. Quando for o caso, o potencial candidato também deve submeter a análise da Iridium o questionário ANBIMA de Due Diligence específico para a atividade contratada.

O processo de contratação e supervisão do terceito deve ser sempre efetuado visando o melhor interesse de seus clientes, especialmente em casos em que haja ligação direta ou indireta entre a Gestora e a empresa contratada ou em hipóteses de potenciais conflitos de interesse. Adicionalmente, é dever da Iridium sempre fornecer aos seus investidores total transparência com relação a eventuais recebimentos de serviços contratados ou relacionamento, como no caso da contratação de Corretoras.

É de responsabilidade da Diretoria de Compliance que esta esteja envolvida na diligência de potenciais fornecedores e prestadores de serviços, durante o processo de contratação desses. Sendo assim, durante esse procedimento, a Diretoria de Compliance deve procurar por processos, condenações e notícias desabonadoras sobre esses potenciais novos fornecedores e prestadores de serviços e seus sócios e administradores.

Adicionalmente, durante o processo de contratação, a Diretoria de Compliance tem o dever de classificar o risco potencial da atividade a ser delegada a um terceiro. A classificação deve utilizar os seguintes parâmetros:

- Baixo risco;
- Médio risco; e
- Alto risco.

Baseada nessa análise de risco, a Iridium deve descrever as supervisões necessárias para cada grau de risco diferente e nenhuma dessas pode ter uma periodicidade maior que 36 (trinta e seis) meses. Além do mais, na ocorrência de fatos relavantes envolvendo o contratado ou de alteração significativa a respeito do serviço prestado em termos de qualidade e/ou performance, a Iridium também se mantém o direito de reavaliação tempestiva destes. Todos esses processos, tem o intuito de garantir que as medidas de supervisão, prevenção e mitigação sejam proporcionais aos riscos identificados.

Por fim, é dever da Diretoria de Compliance supervisionar e formalizar em um relatório as suas análises e também manifestar a sua opinião/recomendação com relação a idoneidade do fornecedor e prestador de serviço contratado e a ser contratado.

PARTE H - POLÍTICA DE TREINAMENTO

A Política de Treinamentos da Iridium tem como objetivo estabelecer as regras que orientem o treinamento dos colaboradores, de forma a torná-los aptos a seguir todas as regras dispostas nas Políticas. Todos os sócios e colaboradores recebem o devido treinamento acerca de todas as políticas e procedimentos constantes deste Manual. Assim, são proporcionados aos sócios e colaboradores uma visão geral das Políticas adotadas, de forma que os mesmos se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.

A Iridium poderá financiar, total ou parcialmente, cursos de aprimoramento profissional aos colaboradores, principalmente aos membros da equipe técnica, desde que julgue viável e interessante o conteúdo a ser lecionado. O controle e a supervisão das práticas profissionais dos colaboradores em relação à política de treinamentos é responsabilidade do Diretor de Compliance, que visará promover a aplicação conjunta da referida Política com as normas estabelecidas nas demais Políticas aprovadas nos termos do presente Manual.

Poderão ser ministradas a todos os sócios e colaboradores da Iridium palestras internas, a fim de dar ciência sobre:

- As políticas adotadas pela Iridium;

- A regulamentação vigente e aplicável aos negócios da Iridium; e

- Eventuais problemas ocorridos, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela Iridium.

Referidas palestras serão de participação obrigatória, comprovada mediante assinatura do colaborador em lista de presença. Não sendo possível a participação do sócio ou colaborador, sua ausência deverá ser justificada ao Diretor de Compliance da Iridium, sendo certo que a ausência deverá ser reposta na data mais próxima possível.

Todo o treinamento interno proposto pela Iridium, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais da Iridium, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Com relação aos procedimentos de controle e de prevenção à lavagem de dinheiro, a Iridium tem por princípio capacitar seus integrantes a observá-los. Adicionalmente, é esperado que sócios e colaboradores das áreas de relações com investidores, *back office*, mesa de operações, risco e compliance tenham um embasamento sério sobre a identificação de operações para crimes de lavagem de dinheiro.

O treinamento será realizado a cada 12 (doze) meses, e obrigatório a todos os colaboradores. Quando do ingresso de um novo colaborador, a Diretora aplicará o devido treinamento de forma individual para o novo colaborador. A Diretora poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os colaboradores constantemente atualizados em relação às Políticas.

O treinamento para capacitação de todos os colaboradores com relação às regras de prevenção à lavagem de dinheiro será realizado conjuntamente com o treinamento interno aqui referido. Os procedimentos de combate e prevenção à lavagem de dinheiro serão supervisionados pela Diretoria de Compliance, o qual terá livre acesso aos dados cadastrais dos clientes e colaboradores e às operações por estes realizadas.