

POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO AO TERRORISMO

GMG INTERNET SERVICE LTDA

I. INTRODUÇÃO

A presente Política de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo (“Política”) tem por objetivo estabelecer diretrizes, orientações, definições e procedimentos, em consonância com a legislação nacional e internacional, com o fim de prevenir e detectar operações ou transações que apresentem características atípicas, para combater os crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores, bem como identificar e acompanhar as operações suspeitas que indiquem a ocorrência de casos de lavagem de dinheiro e do financiamento ao terrorismo, em cumprimento à legislação aplicável, notadamente a Lei nº 9.613, de 3 de março de 1998, alterada pela Lei nº 12.683, de 9 de julho de 2012 (“Lei nº 9.613/98”) e a Instrução CVM 301, de 16 de abril de 1999 (“Instrução CVM 301”).

Neste sentido, a Gmg Internet Service Ltda pretende, ao instituir a presente Política, estabelecer e implementar procedimentos e controles destinados a:

- (i) Identificar a qualificação e perfil dos clientes e demais envolvidos nas operações e atividades desenvolvidas pela Gmg Internet Service;
- (ii) Identificar o propósito e a natureza das relações de negócios, assim como os beneficiários finais das operações;
- (iii) Treinar e capacitar Colaboradores (conforme definido abaixo), no que se refere a prevenção e identificação de crimes relacionados com a lavagem de dinheiro;
- (iv) Reduzir os riscos de que os negócios, atividades e serviços prestados pela empresa sejam destinados a lavagem de dinheiro e/ou ao financiamento ao terrorismo;
- (v) Assegurar que o desenvolvimento da atividade financeira cumpra a legislação e a regulamentação contra os crimes de lavagem de dinheiro;
- (vi) Garantir a observância da política de cadastramento de clientes e os procedimentos de “conheça seu cliente” (“Know Your Client”), relacionando a origem de recursos, capacidade financeira e condição patrimonial;
- (vii) Delimitar os critérios para o monitoramento das transações e a identificação de situações atípicas ao perfil do cliente e estipular os procedimentos necessários para avaliação das situações identificadas e para a constatação de indícios de lavagem de dinheiro;
- (viii) Enquadrar e classificar as operações e clientes da Gmg Internet Service Ltda em categorias de risco, para maior controle; e
- (ix) Identificar as operações suspeitas do ponto de vista da lavagem de dinheiro e financiamento ao terrorismo e aquelas de comunicação obrigatória ao COAF.

II. APLICAÇÃO E RESPONSABILIDADE

O Diretor Responsável pela Prevenção à Lavagem de Dinheiro será o responsável por verificar o cumprimento desta Política por parte dos Colaboradores, bem como fornecer a estes os treinamentos necessários.

O Diretor Responsável pela Prevenção à Lavagem de Dinheiro cumulará as funções de Diretor de Compliance e Riscos, de modo que os reportes exigidos por força desta Política deverão ser comunicados ao *compliance officer*.

Previamente ao início do exercício de suas funções na Gmg Internet Service , os seus Colaboradores deverão receber uma cópia desta Política e firmar um Termo de Adesão. O *compliance officer* manterá em arquivo, na sede da empresa, pelo prazo mínimo de 5 (cinco) anos, uma via original do Termo de Adesão devidamente assinado por cada Colaborador.

Em caso de dúvidas acerca da interpretação das regras contidas nesta Política, ou havendo necessidade de aconselhamento, o Colaborador deverá buscar auxílio junto ao *compliance officer*.

O conhecimento de algum indício de lavagem de dinheiro ou ato corrupto deverá ser comunicado ao *compliance officer*, sendo este responsável por averiguar as informações reportadas e, caso aplicável, comunicar aos órgãos reguladores.

Nos termos do artigo 2º da Instrução CVM 301 e do Ofício Circular 5/2015/SIN/CVM, independentemente das responsabilidades relacionadas aos administradores dos fundos de investimento eventualmente geridos pela Gmg Internet Service , esta é igualmente obrigada a seguir os procedimentos relacionados à Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo previstos na Lei 9.613/98 e na Instrução CVM 301.

O descumprimento das regras previstas nesta Política será considerado infração contratual e ensejará a imposição de penalidades, conforme abaixo definidas, sem prejuízo das eventuais medidas legais cabíveis.

III. CONCEITO

I. CONCEITO DE PLDFT

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.

O delito de financiamento ao terrorismo caracteriza-se pela promoção ou recebimento de fundos com a intenção de empregá-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.

II. IDENTIFICAÇÃO DE CLIENTES, COLABORADORES E PARCEIROS

A) Identificação e Cadastro de Clientes

O cadastro de clientes é elemento essencial na prevenção e combate ao crime de lavagem de dinheiro e financiamento ao terrorismo e, portanto, os Colaboradores da Gmg Internet Service Ltda deverão manter cadastro atualizado dos seus clientes.

Os Colaboradores deverão efetuar o cadastro de seus clientes contendo, no mínimo, as informações e os documentos indicados no Anexo I da Instrução CVM 301, e deverão atualizar o cadastro dos clientes ativos em intervalos não superiores a 24 (vinte e quatro) meses. De acordo com a Instrução CVM 301, considera-se ativo o cliente que tenha efetuado movimentação ou tenha apresentado saldo em sua conta no período de 24 (vinte e quatro) meses posteriores à data da última atualização.

É obrigatório 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 documentação deve ser cuidadosamente analisada para fins de confirmação do cadastro.

Considerando as principais diretrizes e regras existentes no mercado financeiro e a análise dos principais casos de lavagem de dinheiro é possível relacionar perfis de investidores mais propensos ao envolvimento com o crime de lavagem de dinheiro, os quais serão classificados como “Especial Atenção”.

Serão considerados clientes Especial Atenção:

- (i) aquelas pessoas que desempenhem ou tenham desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiras, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo (“Pessoas Politicamente Expostas”);
- (ii) aquelas pessoas com ocupações profissionais e ramos de atividades consideradas 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;
- (iii) aquelas pessoas residentes em locais perto de fronteiras;
- (iv) os clientes maiores de 80 (oitenta) e menores de 18 (dezoito) anos;

- (v) os clientes que, no momento do cadastramento, indicarem procurador ou representante; e
- (vi) as pessoas físicas ou jurídicas já envolvidas em crimes de lavagem de dinheiro ou quaisquer outros crimes relacionados ao mercado financeiro, bem como aqueles que receberam qualquer tipo de publicidade negativa.

B) Procedimentos de Conheça seu Cliente (Know Your Client)

A Gmg Internet Service Ltda adotará procedimentos de “Conheça seu Cliente”, 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.

Os procedimentos de “Conheça seu Cliente” serão formalizados por meio do preenchimento de formulários específicos para todos os clientes, pessoas físicas ou jurídicas.

A Gmg Internet Service Ltda, 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.

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

Nos termos do artigo 2º da Instrução CVM 301 e do Ofício Circular 5/2015/SIN/CVM, independente das responsabilidades relacionadas aos administradores dos eventuais fundos de investimento geridos pela Gmg Internet Service Ltda, esta é igualmente obrigada a seguir os procedimentos relacionados à Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo previstos na Lei 9.613/98 e na Instrução CVM 301.

C) Procedimentos de Conheça seu Colaborador (Know Your Employee – KYE)

Os procedimentos de “Conheça seu Colaborador” têm por objetivo fornecer à Gmg Internet Service Ltda informações detalhadas sobre seus Colaboradores, os quais incluem critérios para a sua contratação e verificação de suas condutas.

A Gmg Internet Service Ltda 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 Gmg Internet Service Ltda obterá, junto aos meios legais aplicáveis, as informações relativas à situação econômico-financeira de seus Colaboradores.

D) Procedimentos de Conheça seu Parceiro (Know Your Partner – KYP)

Os procedimentos de “Conheça seu Parceiro” abrangem todos os parceiros de negócios da Gmg Internet Service Ltda, 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 Gmg Internet Service Ltda em situações que possam acarretar a riscos legais e à sua reputação perante o mercado.

Antes do início do relacionamento com parceiros de negócios, a Gmg Internet Service Ltda 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.

São exemplos de sites para a realização das pesquisas mencionadas no parágrafo anterior:

(i) Sites de busca de informações relevantes:

- (a) The Financial Conduct Authority (FCA UK) – www.fca.org.uk
- (b) Prudential Regulation Authority – www.bankofengland.co.uk
- (c) Google – www.google.com
- (d) Justiça Federal – www.cjf.jus.br
- (e) OCC – www.occ.treasury.gov
- (f) Ofac – www.treas.gov
- (g) Press Complaints Commission (PCC) – www.pcc.org.uk
- (h) UK Gov – www.direct.gov.uk
- (i) Unauthorized Banks – http://occ.treas.gov/ftp/alert/2008_28a.pdf<http://occ.treas.gov/ftp/alert/2008-28a.pdf>
- (j) US Oregon Gov – www.oregon.gov

(ii) Sites de órgãos reguladores e autorreguladores:

- (a) Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – (“ANBIMA”) www.anbima.com.br
- (b) BACEN – www.bcb.gov.br
- (c) Bolsa de Valores, Mercadorias e Futuros (“BM&FBovespasp”) – www.bmfbovespa.com.br
- (d) Câmara de Custódia e Liquidação (“CETIP”) – www.cetip.com.br
- (e) CVM – www.cvm.org.br
- (f) COAF – www.coaf.fazenda.gov.br/ www.fazenda.gov.br/
- (g) Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (“ENCCLA”) – <http://enccla.camara.leg.br/>

- (h) Grupo de Ação Financeira contra Lavagem de Dinheiro e o Financiamento do Terrorismo Grupo de Ação Financeira Internacional (“GafiGAFI/FATF”) – www.fatf-gafi.org
- (i) Ministério da Previdência Social (“PREVIC”) – www.previdencia.gov.br/previc/
- (j) Presidência da República – www.presidencia.gov.br
- (k) Secretaria da Receita Federal do Brasil (“RFB”) – www.fazenda.gov.br
- (l) Superintendência de Seguros Privados (“SUSEP”) – www.susep.gov.br
- (m) Wolfsberg Group – www.wolfsberggroup.com

E) Procedimento para Investimentos realizados pelos Fundos de Investimento sob gestão (Contrapartes)

A negociação de ativos e valores mobiliários financeiros nos Fundos de Investimento sob gestão da Gmg Internet Service Ltda também deve ser analisada e monitorada para fins de prevenção e combate à lavagem de dinheiro, do ponto de vista da contraparte de cada operação.

É necessária a análise, quando da aquisição de ativos para fins de prevenção à lavagem de dinheiro, das contrapartes através da realização de cadastro, além da realização de pesquisas, através dos meios públicos disponíveis, sobre a reputação das contrapartes 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, devendo ser utilizados os sites acima indicados, para fins de exemplo de locais de busca pelos colaboradores.

E levando-se em conta a razoabilidade e proporcionalidade dos controles internos, qualquer atuação suspeita em relação à contraparte deve ser comunicada ao COAF, mesmo que já tenha passado pelo processo de prevenção e combate à lavagem de dinheiro.

Nos termos do artigo 2º da Instrução CVM 301 e do Ofício Circular 5/2015/SIN/CVM, independente das responsabilidades relacionadas aos administradores dos fundos de investimento geridos pela Gmg Internet Service Ltda, esta é igualmente obrigada a seguir os procedimentos relacionados à Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo previstos na Lei 9.613/98 e na Instrução CVM 301.

IV. PROCEDIMENTOS GERAIS

I- Identificação de Indícios de Lavagem de Dinheiro

Os Colaboradores devem monitorar continuamente as seguintes operações ou situações envolvendo títulos ou valores mobiliários:

- (i) Realização de aplicações ou resgates em fundos que apresentem atipicidade em relação à capacidade econômico-financeira do cliente;
- (ii) Abertura, movimentação de contas de fundos de investimento ou realização de aplicações ou resgates por detentor de procuração ou de qualquer outro tipo de mandato;

- (iii) Apresentação de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente, seguidas ou não do encerramento do relacionamento comercial;
- (iv) Realização de várias aplicações em contas de investimento em fundos, em uma mesma data ou em curto período, com depósitos de valores idênticos ou aproximados;
- (v) Informação de mesmo endereço comercial por diferentes pessoas jurídicas ou organizações, sem justificativa razoável para tal ocorrência;
- (vi) Representação de diferentes pessoas jurídicas ou organizações pelos mesmos procuradores ou representantes legais, sem justificativa razoável para tal ocorrência;
- (vii) Informação de mesmo endereço residencial ou comercial por pessoas naturais, sem demonstração da existência de relação familiar ou comercial;
- (viii) Manutenção de numerosas contas de investimento em fundos, destinadas ao acolhimento de aplicações de um mesmo cliente, incompatíveis com o patrimônio, a atividade econômica ou a ocupação profissional e a capacidade financeira do cliente;
- (ix) Incompatibilidade entre a atividade econômica e o faturamento informados pelo cliente com o padrão apresentado por clientes com o mesmo perfil de risco;
- (x) Movimentação de quantia significativa, por meio de contas de fundos, até então pouco movimentada;
- (xi) Ausência repentina de movimentação financeira em conta de fundo que anteriormente apresentava grande movimentação;
- (xii) Realização de aplicações em contas de fundos que, por sua habitualidade, valor e forma, configurem artifício para burla da identificação da origem, do destino, dos responsáveis ou dos beneficiários finais;
- (xiii) Manutenção de contas de fundos, qualquer que seja o valor da aplicação, por pessoas que reconhecidamente tenham cometido ou tentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento;
- (xiv) Existência de recursos em contas de fundos pertencentes ou controlados, direta ou indiretamente, por pessoas que reconhecidamente tenham cometido ou tentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento;
- (xv) Movimentações (aplicações ou resgates em contas de investimento em fundos) com indícios de financiamento de terrorismo;
- (xvi) Solicitação de não observância ou atuação no sentido de induzir funcionários da instituição a não seguirem os procedimentos regulamentares ou formais para a realização de uma aplicação ou resgate em contas de fundos;
- (xvii) Operações cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional, os rendimentos ou a situação patrimonial ou financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais dos clientes;
- (xviii) Operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;
- (xix) Operações que evidenciem oscilação significativa em relação ao volume ou frequência de negócios de qualquer das partes envolvidas;
- (xx) Operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos ou beneficiários respectivos;
- (xxi) Operações cujas características ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;
- (xxii) Operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);

- (xxiii) Operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;
- (xxiv) Operações com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;
- (xxv) Operações liquidadas em espécie, se e quando permitido;
- (xxvi) Transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;
- (xxvii) Operações e situações em que não seja possível identificar o beneficiário final;
- (xxviii) Aplicações cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do cliente ou de seu representante;
- (xxix) Depósitos ou transferências realizadas por terceiros, para liquidação de operações de cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;
- (xxx) Pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do cliente;
- (xxxi) Resistência ao fornecimento de informações necessárias para o início de relacionamento ou para a atualização cadastral, oferecimento de informação falsa ou prestação de informação de difícil ou onerosa verificação;
- (xxxii) Declarar diversas contas bancárias ou modificá-las com habitualidade; e
- (xxxiii) Autorizar procurador que não apresente vínculo aparente.

Caso qualquer um dos Colaboradores identifique situações suspeitas que possam caracterizar indícios de lavagem de dinheiro ou financiamento ao terrorismo, estes deverão reportá-las imediatamente ao *compliance officer* que será o responsável por respeitar o sigilo do reporte e proporcionar a devida averiguação dos fatos.

Caso o *compliance officer* verifique tratar-se de indícios de lavagem de dinheiro ou financiamento ao terrorismo, este deverá comunicar imediatamente tal fato ao COAF, nos termos da Instrução CVM 301, da Lei 9.613/98.

II - Comunicação de Indícios de Lavagem de Dinheiro

O *compliance officer* é o responsável pelas rotinas de monitoramento das operações para identificação de indícios de lavagem de dinheiro e financiamento ao terrorismo.

Para isto, a Gmg Internet Service possui capacidade para gerar ocorrências relacionadas às operações e informações cadastrais declaradas pelos clientes. As atipicidades identificadas pelo sistema gerarão alertas identificando quais filtros cadastrados foram acionados.

Uma vez gerada a ocorrência, caberá ao *compliance officer* analisar o cliente e suas operações para confirmar ou não os indícios de lavagem de dinheiro de financiamento ao terrorismo.

Para este fim, o *compliance officer* poderá (i) exigir a atualização cadastral do cliente; (ii) solicitar esclarecimentos ao assessor comercial do cliente ou ao próprio

cliente; e (iii) realizar análise com o viés de determinação de riscos referente ao caso, dadas as inconsistências de movimentação.

Após a análise pelo *compliance officer*, este deverá (i) arquivar a ocorrência, caso verifique não se tratar de indício de lavagem de dinheiro ou financiamento ao terrorismo; ou (ii) comunicar o fato ao COAF, nos termos da Instrução CVM 301 e da Lei 9.613/98 e da Carta Circular nº 3.542/2012 do BACEN, caso confirme tratar-se de indício de lavagem de dinheiro ou financiamento ao terrorismo.

Na hipótese de comunicação ao COAF, os Colaboradores deverão abster-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela a qual se refira a informação, no prazo de 24 (vinte e quatro) horas a contar da ocorrência. Neste sentido, a comunicação possui caráter confidencial e, portanto, deve ser restrita aos Colaboradores envolvidos no processo de análise.

Cabe ressaltar que a comunicação ao COAF não acarreta suspensão automática das operações ou propostas de operações, salvo quando solicitada pelas autoridades competentes.

Desde que não tenha sido prestada nenhuma comunicação ao COAF, os Colaboradores devem comunicar à CVM, anualmente, até o último dia útil do mês de janeiro, por meio de sistema eletrônico disponível na página da CVM na rede mundial de computadores, a não ocorrência no ano civil anterior das transações ou propostas de transações passíveis de serem comunicadas.

Todos os registros das conclusões de suas análises acerca de operações ou propostas que fundamentaram a decisão de efetuar, ou não, a comunicação ao COAF devem ser arquivados e mantidos pelo prazo de 5 (cinco) anos.

III - Comunicação de Operações decorrentes de decisões tomadas pela Gmg Internet Service Ltda como Gestora.

Caso qualquer dos colaboradores entenda que alguma decisão tomada pela Gmg Internet Service Ltda enquanto gestora de fundos de investimento esteja em desacordo com o previsto nesta Política e na legislação aplicável, notadamente a Instrução CVM 301 e da Lei 9.613/98, este deverá informar este fato ao Diretor de Compliance, que tomará as providências necessárias para a efetiva apuração de tal operação suspeita, com a conseqüente comunicação ao COAF, se for o caso.

VI. TREINAMENTO

I - Programas de Treinamento

Todos os Colaboradores da Gmg Internet Service Ltda, inclusive seus sócios e administradores, deverão obrigatoriamente participar dos programas de treinamento descritos abaixo (“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 Responsável pela Prevenção à Lavagem

de Dinheiro, responsável por supervisionar os Colaboradores quanto à sua assiduidade e dedicação.

Os Colaboradores deverão obrigar-se, por meio do “Termo de Adesão” a participar dos Programas de Reciclagem Contínua eventualmente realizados pela Gmg Internet Service Ltda, em conformidade com as orientações do Diretor Responsável pela Prevenção à Lavagem de Dinheiro.

A) 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 Gmg Internet Service Ltda.

O Programa de Treinamento Inicial terá por objetivo principal apresentar aos novos Colaboradores a atividade desenvolvida pela Gmg Internet Service Ltda e sua filosofia de investimento, bem como prestar esclarecimentos sobre as disposições constantes desta Política e das demais normas internas adotadas pela sociedade, inclusive no que diz respeito às funções exercidas pelo Diretor Responsável pela Prevenção à Lavagem de Dinheiro.

B) Programa de Treinamento Inicial

Os Programas de Reciclagem Contínua serão realizados periodicamente e envolverão a participação dos Colaboradores em cursos, palestras e treinamentos sobre temas relacionados à atividade desenvolvida pela Gmg Internet Service Ltda, objetivando promover 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.

VII. PENALIDADES

O descumprimento total ou parcial das regras contidas nesta Política e na legislação vigente constitui violação dos padrões éticos, técnicos e operacionais, conforme o caso, que regem o funcionamento da Gmg Internet Service Ltda.

A verificação de descumprimento das normas contidas nesta Política ensejará a aplicação de penalidades pelo Diretor Responsável pela Prevenção à Lavagem de Dinheiro, nos termos do art. 10 da Instrução CVM 301. Tais penalidades podem variar entre advertência, multas (em espécie ou em perda direta de benefícios ou de pontos de avaliação para fins de remuneração variável), suspensão, destituição ou demissão por justa causa do Colaborador infrator sem prejuízo das demais consequência legais.

Os Colaboradores reconhecem o direito da Gmg Internet Service Ltda de exercer direito de regresso caso venha a ser responsabilizada, sofra prejuízo ou venha a arcar com ônus de qualquer espécie em decorrência de atos ilícitos ou infrações cometidas por seus Colaboradores no exercício de suas funções.

VIII. AUDITORIA

A presente Política deverá ser submetida periodicamente a auditorias internas, realizadas pelo *compliance office*, e eventualmente por auditorias externas, realizadas por meio de instituições contratadas.

Neste sentido, deverá ser realizada análise e correção das eventuais deficiências apontadas nos relatórios dos auditores, como forma de melhoria contínua e de garantia do cumprimento das normas vigentes.

São José do Rio Preto/SP, 30 de maio de 2023.

GMG INTERNET SERVICE LTDA

Diretoria: Marcelo Ferraz Rodrigues