POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Esta Política de Confidencialidade e Segurança da Informação ("Política"), elaborada em conformidade com a Instrução CVM n.º 558, de 26 de março de 2015, conforme alterada ("ICVM 558"), tem por objetivo estabelecer regras e procedimentos de sigilo e procedimentos de conduta para garantia da confidencialidade das informações obtidas no exercício de atividades profissionais por todos os sócios, administradores, empregados e estagiários da Trigger Gestora de Recursos Ltda. ("Trigger Gestora" e "Colaboradores").

Todos os Colaboradores devem respeitar as regras e procedimentos dispostos nesta Política na condução de suas atividades profissionais, seja em caráter temporário ou permanente, no relacionamento com clientes, agentes de mercado, fornecedores, parceiros, contrapartes e quaisquer terceiros.

Nos termos da ICVM 558, a Trigger Gestora deverá manter versão atualizada desta Política em seu website '*trigger.com.br*' juntamente com outros documentos obrigatórios, conforme definido na ICVM 558.

Esta Política deverá ser obedecida em conjunto com a Política de Segregação de Atividades.

2. OBJETIVO

Definir regras e procedimentos de sigilo e conduta e de segurança da informação, assegurando o controle de informações confidenciais a que tenham acesso os Colaboradores no desempenho de suas atividades na Trigger Gestora.

3. ABRANGÊNCIA

Esta Política se aplica a todos os Colaboradores da Trigger Gestora. Todos os Colaboradores devem se assegurar do pleno conhecimento e atendimento da legislação e regulamentação aplicáveis à Trigger Gestora, bem como do conteúdo integral desta Política.

Para manifestar a ciência e a obrigação de cumprimento das regras e procedimentos dispostos a seguir, todos os Colaboradores devem assinar o Termo de Adesão anexo a esta Política ("Termo de Adesão").

4. INFORMAÇÕES CONFIDENCIAIS

Por "Informação Confidencial" entende-se toda e qualquer informação resguardada contra a revelação pública, seja transmitida por meio eletrônico, escrito ou verbal a qual os Colaboradores

tiverem acesso no exercício de suas atividades profissionais, independentemente de estarem ou não classificadas como informações confidenciais, incluindo:

- dados da Trigger Gestora, de seus Colaboradores, investidores, fundos de investimento e/ou ativos alvo dos fundos de investimento por ela administrados;
- informações e documentos de natureza negocial, estratégica, técnica, operacional, financeira, administrativa, patrimonial, legal, contábil, comercial;
- dados de clientes de fato ou potenciais;
- propostas, projetos, relatórios, planejamento, métodos operacionais;
- dados cadastrais, de qualquer natureza;
- relatórios de órgãos reguladores, autorreguladores e do poder público;
- informações e documentos de inspeções e fiscalizações;
- materiais de *marketing*.

5. REGRAS PARA MANUTENÇÃO DE SIGILO DE INFORMAÇÕES CONFIDENCIAIS

Em virtude do desempenho de suas funções, os Colaboradores podem vir a ter acesso a Informações Confidenciais, as quais, nos termos desta Política, das demais políticas e regras da Trigger Gestora, da legislação e regulamentação aplicáveis e em consonância com as melhores práticas, não poderão ser reveladas a terceiros não autorizados, nem usadas com propósito diverso do qual foram confiadas.

Dessa forma, os Colaboradores devem orientar suas ações no sentido de:

- manter o controle sobre a segurança e empregar os melhores esforços para salvaguardar as informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade;
- somente passar Informações Confidenciais para outro Colaborador caso ele precise desta informação para exercer suas funções no curso normal das atividades da Trigger Gestora;
- evitar a discussão de questões confidenciais em lugares públicos e evitar circular em ambientes externos à Trigger Gestora com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao curso normal das atividades da Trigger Gestora, devendo essas cópias, quando estiverem em dispositivos eletrônicos (como *pen drives*) serem criptografadas ou mantidas protegidas com senha de acesso;

- manter documentos que contenham Informações Confidenciais em local seguro e cuidar para que as minutas ou cópias desses documentos sejam sempre destruídas antes do descarte. Quando apropriado, nomes codificados devem ser utilizados para prevenir a identificação das partes envolvidas;

- empregar os melhores esforços para evitar a materialização de eventos externos que possam comprometer o sigilo das Informações Confidenciais, como por exemplo vírus de computador, fraudes, etc., ou mitigar os efeitos advindos de uma inevitável materialização desses eventos;

- manter todas as senhas de acesso aos sistemas da Trigger Gestora, as quais são pessoais e intransferíveis, em boa guarda;

- assegurar que contratos firmados com consultores ou terceiros contenham, quando veicularem Informações Confidenciais, cláusula de confidencialidade; e

- informar ao Diretor de Compliance e Gestão de Riscos qualquer situação suspeita de violação desta Política.

Aos Colaboradores é vedado, mesmo após o término do seu vínculo com a Trigger Gestora, direta ou indiretamente, usar ou divulgar Informações Confidenciais a que tenham tido acesso, exceto se tal divulgação for autorizada pelo Diretor de Compliance e Gestão de Riscos ou decorrer de decisão judicial ou ordem de autoridades governamentais, sendo que, neste caso, a Trigger Gestora deverá ser notificada imediatamente sobre a solicitação de divulgação de tais Informações Confidenciais.

6. PROCEDIMENTO PARA GUARDA E DESTRUIÇÃO DE INFORMAÇÕES CONFIDENCIAIS

Documentos impressos ou digitais

Os Colaboradores devem evitar fazer cópias ou impressão de documentos que contenham Informações Confidenciais para uso externo à Trigger Gestora, exceto nos casos em que tais documentos tenham que ser apresentados em reuniões externas.

O Colaborador que fizer a cópia/impressão, uso de armazenamento externo ou transmissão de documentos que contenham Informações Confidenciais será responsabilizada por qualquer uso indevido destes por terceiros.

Cada Colaborador terá acesso apenas ao conjunto de Informações Confidenciais relativas ao projeto de constituição ou aos dados do FIP no qual este estiver trabalhando. Colaboradores dedicados a projetos ou áreas específicas não terão acesso às informações de outras equipes de trabalho da Trigger

Gestora para evitar o acesso indevido a Informações Confidenciais. Apenas o Gestor de Risco e de Compliance terá acesso a todos os documentos da Trigger Gestora.

Comunicação de perda

Em caso de perda de qualquer equipamento de armazenamento externo ou documento impresso que contenham Informações Confidenciais, o Colaborador que tomar conhecimento desse fato imediatamente comunica-lo ao Diretor de Compliance e Gestão de Riscos para a tomada das providências necessárias à mitigação do risco de divulgação e utilização indevida das Informações Confidenciais contidas no arquivo (eletrônico ou impresso) objeto de perda, bem como para eventual responsabilização de Colaboradores envolvidos.

A não comunicação de perda de arquivos (eletrônicos ou físicos) que contenham Informações Confidenciais ensejará a aplicação de sanção ao Colaborador responsável ainda que não sejam materializadas perdas pelo uso indevido das informações.

Destruição de documentos confidenciais

Todos os documentos que contenham Informações Confidenciais deverão ser destruídos tão logo deixem de ser utilizados pelos Colaboradores, respeitada a obrigação de guarda de determinados documentos e informações por períodos superiores, nos termos da legislação e regulamentação aplicáveis e demais políticas da Trigger Gestora.

Os arquivos físicos serão destruídos por meio de fragmentadora de papel. Os arquivos digitais serão destruídos por meio que impeça a sua recuperação. Já os arquivos digitalizados em pastas temporárias serão apagados periodicamente, quando deixarem de ser utilizados pelos Colaboradores no desempenho de suas funções.

A guarda de documentos que contenham Informações Confidenciais para fins de cumprimento de normas legais e regulamentares será supervisionada pelo Diretor de Compliance e Gestão de Riscos, de como a assegurar que o acesso a esses documentos seja franqueado somente aos Colaboradores que o necessitem para o desempenho de suas atividades profissionais.

Treinamento e Aperfeiçoamento

A Trigger Gestora exige que seus Colaboradores sejam adequadamente treinados no que se refere a todos os aspectos dos requisitos desta política e no uso de Informações Confidenciais de forma a evitar principalmente o acesso indevido A Informações Confidenciais. Todos os Colaboradores deverão passar por programas de treinamento voltados a conhecer e compreender as regras do mercado de capitais pertinentes às atividades desenvolvidas pela Trigger Gestora. Os programas de treinamento têm como finalidade principal garantir que todos os Colaboradores da Trigger Gestora tenham pleno conhecimento de seus deveres e obrigações, bem como de suas limitações. Novos Colaboradores da Trigger Gestora deverão obrigatoriamente participar de um programa de treinamento específico antes do início do

exercício de suas funções.

7. SANÇÕES

Sem prejuízo da aplicação das sanções previstas na legislação e regulamentação aplicáveis, os Colaboradores que descumprirem as regras previstas nesta Política estarão sujeitos às seguintes sanções:

- advertência;
- suspensão;
- demissão de Colaborador empregado ou estagiário;
- destituição de Colaborador diretor; ou
- exclusão de Colaborador sócio, nessa hipótese, desde que respeitado o quórum de aprovação e procedimento previstos no contrato social da Trigger Gestora.

Nas hipóteses em que a Trigger Gestora venha a ser responsabilizada por infrações legais ou regulamentares eventualmente praticadas por seus Colaboradores, a Trigger Gestora se reserva o direito de pleitear indenização pelos danos eventualmente incorridos, incluindo, mas não se limitando aos danos de imagem.

* * *