I. INTRODUÇÃO

1.1. Esta Política de Segurança e Sigilo de Informação, Privacidade de Dados e Segurança Cibernética ("Política") é parte integrante do conjunto de normas e políticas internas do DGF Investimentos Gestão de Fundos Ltda. ("DGF") e deve ser lido e interpretado em conjunto com o Código de Conduta e Ética, o Manual de Controles Internos e Compliance, a Política de Gestão de Risco, a Política de Prevenção a Lavagem de Dinheiro, a Política de Negociação de Valores Mobiliários e Aquisição e Acompanhamento de Ativos Imobiliários e Mobiliários, a Política de *Suitability*, o Manual de Precificação de Ativos e a Política de Rateio e Divisão de Ordens.

1.2. A presente Política do DGF tem como objetivo estabelecer as diretrizes, as regras e os procedimentos criados pelo DGF com o objetivo de atender às normas a ele impostas, atinentes às matérias aqui tratadas. A presente Política foi elaborada pelo Diretor responsável pela gestão do risco e pelo cumprimento de regras, políticas, procedimentos e controles internos do DGF ("Diretor de Compliance"), em conjunto com os demais Diretores do DGF, com assessoria de advogados externos.

1.3. Esta Política não tem o propósito de esgotar as matérias aqui tratadas, havendo a possibilidade de existirem situações que não estejam integralmente previstas e que demandem solução específica no caso concreto. Nessas situações, os Colaboradores (conforme abaixo definido), deverão se reportar ao Comitê de Ética e Compliance do DGF.

1.4. A Política aplica-se a todos os seus administradores, sócios, funcionários, prestadores de serviços, estagiários, trainees ou quaisquer outros colaboradores que, de alguma forma, venham a, direta ou indiretamente, prestar serviços em favor do DGF ("Colaborador" ou "Colaboradores"), por meio das quais os Colaboradores poderão ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

1.5. Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis ao DGF, bem como do completo conteúdo das Políticas.

1.6. Esta Política será revisada a cada dois anos, ou em periodicidade inferior, caso seja identificada necessidade, como, por exemplo, alterações legislativas ou regulamentares, identificação de melhorias a serem implementadas, implantação de novos sistemas e controles, ou outras ocorrências que indiquem possibilidade de aperfeiçoamento ou necessidade de alterações.

1.7. Quaisquer ocorrências relacionadas à presente Política deverão ser informadas ao

Comitê de Ética e Compliance do DGF, por meio do e-mail compliance@dgf.com.br ou outros canais diretos a serem disponibilizados, podendo tal comunicação ser feita de forma anônima

II. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

2.1. As medidas de segurança da informação têm por finalidade minimizar ameaças aos negócios do DGF. A presente seção objetiva preservar, melhorar e responder pelo sigilo, integridade e disponibilidade das informações do DGF, a fim de proteger tais informações de uma variedade de ameaças, tais como erro, fraude, violação de privacidade e interrupção de serviços.

2.2. Tais informações incluem, sem limitação, informações técnicas, como programas de computador e bases de dados, informações comerciais, tais como, objetivos do DGF e suas estratégias, segredos comerciais, processos, análises, gráficos, desenhos, relatórios, vendas, lucros, estatísticas, relações com clientes, estratégias de marketing, materiais de treinamento, remuneração de Colaboradores e registros, e outras informações de natureza semelhante.

2.3. A segurança das informações requer a participação e o apoio de todos os Colaboradores. Todos os Colaboradores do DGF receberão treinamento e materiais de referência de apoio os quais permitam aos mesmos protegerem e administrarem adequadamente os ativos de informação do DGF. Os materiais de treinamento comunicarão que a segurança da informação é parte integral dos negócios do DGF, devendo ser considerada tão vital quanto outras funções comerciais contínuas.

2.4. Ao término de seu vínculo empregatício com o DGF, o Colaborador deverá devolver todos os documentos a que teve acesso, decorrentes ou necessários para o desempenho de suas atividades, ao DGF.

2.5. O objetivo das medidas acima é: (i) assegurar e manter o sigilo, a integridade e a disponibilidade dos ativos de informação do DGF em uma medida condizente com a sensibilidade e o valor dos dados; (ii) proteger os ativos de informação do DGF contra uso indevido, abusivo e/ou não autorizado ou utilização de informações ou registros de clientes que possam resultar em danos, em uma medida condizente com a sua sensibilidade e o seu valor; (iii) garantir a segurança e a confidencialidade das informações e registros de clientes do DGF; e (iv) proteger o DGF contra quaisquer ameaças ou riscos à segurança ou integridade das informações e registros de clientes.

2.6. Visando a segurança das informações, os seguintes procedimentos devem ser observados:

- Os Colaboradores estão proibidos de fazer cópias, imprimir e/ou circular em ambientes externos ao DGF com os arquivos que sejam considerados confidenciais, utilizados, gerados ou disponíveis na rede da DGF;
- Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, uma vez que podem conter informações restritas e confidenciais mesmo no ambiente interno do DGF;
- Todos os arquivos digitalizados em pastas temporárias serão apagados semanalmente e, o descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação;
- Os Colaboradores devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade no DGF;
- A conexão de equipamentos na rede do DGF somente poderá ocorrer se for previamente autorizado pela área de informação e pelo responsável por Compliance;
- Cada Colaborador do DGF terá seus próprios equipamentos que, em nenhuma hipótese, poderão ser compartilhados, à exceção de impressoras. Cada Colaborador terá a senha de acesso individual à sua máquina e é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade; e
- O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam prejudicar a imagem e afetar a reputação do DGF e/ou de seus clientes.

2.7. Todo risco ou possível incidente (violação da segurança, ameaças, fragilidades ou mau funcionamento de recursos, divulgação indevida etc.) deve ser comunicado o mais breve possível ao Diretor de Compliance ou à equipe de Compliance para registro, análise da ocorrência e adoção de medidas cabíveis.

II.A. IDENTIFICAÇÃO DE USUÁRIO PARA RECURSOS DE INFORMÁTICA

2.8. A identificação de usuário para acessar os recursos de informática do DGF é um privilégio concedido a todos Colaboradores. Neste sentido, o acesso dos usuários aos arquivos eletrônicos é realizado por meio de um usuário próprio, ao qual são concedidos determinados privilégios de acesso a informações com base nas atribuições do respectivo Colaborador.

II.B. SENHAS E EXIGÊNCIAS DE HARDWARE/SOFTWARE

2.9. O acesso aos recursos de informática da Gestão será protegido por senha, a ser escolhida por cada Colaborador, com base nos critérios definidos pelo time de tecnologia da informação (quantidade mínima de caracteres, exigência de dificuldade mínima e de caracteres especiais etc.), e deverão ser atualizadas em periocidade mínima anual.

2.10. As senhas adotadas não deverão ser transcritas em nenhum local de fácil acesso, seja em meio físico ou eletrônico (por exemplo, arquivos salvos na rede, em blocos de notas nas estações de trabalho etc.). É expressamente proibido o compartilhamento de senhas com qualquer outro Colaborador e/ou terceiros.

2.11. O acesso remoto aos recursos de informática do DGF será limitado e deverá ser autorizados pela área de Compliance. Além das autorizações, o acesso remoto será permitido em casos de catástrofes ou situações de quarentena, de acordo com a Política de Crise e Continuidade dos Negócios do DGF.

II.C. PROCEDIMENTOS ADICIONAIS

2.12. Adicionalmente, todos os Colaboradores devem observar os seguintes procedimentos:

- As estações de trabalho devem ser fisicamente seguras e as sessões abertas devem ser trancadas quando deixadas sem supervisão;
- As senhas jamais devem ser armazenadas em um sistema de computação, aparelho, ou por escrito de forma desprotegida;
- Nenhum hardware ou software (incluindo hardwares e softwares pessoais) não autorizado deverá ser usado, carregado, instalado e/ou ativado em nenhuma estação de trabalho ou sistema de produção ou estágios sem análise e aprovação prévias; e
- Para evitar o acesso indevido por outros Colaboradores ou terceiros, todos os Colaboradores devem fechar os programas após sua utilização e efetuar o log-off de seus computadores quando ausentar-se do DGF por um período prolongado.

2.13. Além disso, quando da efetiva gestão de ativos pelo DGF, serão adotados os seguintes procedimentos para mitigar o risco de sistemas de informação:

- Registos de acesso dos usuários aos sistemas considerados críticos para a execução das atividades do DGF;
- Realização de cópias de segurança (backup) das informações, em periodicidade diária (com relação aos 10 dias antecedentes) e mensal (com relação aos 4

meses antecedentes), guardadas em local protegido e fisicamente distante de onde são armazenados os dados do DGF;

- Homologação de novos sistemas, ferramentas ou técnicas em ambiente distinto, antes de sua utilização pelo DGF de forma efetiva;
- Sincronização dos "relógios" de sistema pelo time de tecnologia da informação de forma periódica, de forma a garantir a sincronização dos servidores;
- Utilização de sistemas de segurança que controlam e restringem a conectividade e os serviços de internet por terceiros (firewall); e
- Utilização de programas antivírus em todas os equipamentos com atualizações e varreduras constantes.

II.D. RESTRIÇÕES AO USO DE RECURSOS DE INFORMÁTICA DO DGF

2.14. Os computadores e recursos de tecnologia do DGF existem com a finalidade exclusiva de conduzir os negócios do DGF. Todos os Colaboradores devem seguir políticas e procedimentos corporativos para a compra e uso de todos os equipamentos, hardwares e softwares.

II.E. AVALIAÇÃO DA POLÍTICA DE USO DA REDE

2.15. Para assegurar os procedimentos mencionados, o DGF reserva o direito de:

- Empregar softwares e sistemas capazes de monitorar e registrar todos os usos do e-mail corporativo e da Internet através da rede de estações de trabalho do DGF;
- Inspecionar qualquer arquivo armazenado na rede, no hard drive do computador ou em áreas privadas da rede a fim de assegurar o cumprimento rigoroso deste Manual de Compliance; e
- Manter um conjunto de softwares e hardwares instalados para proteger a rede interna e a integridade de dados e programas.

II.F. REALIZAÇÃO DE TESTES PERIÓDICOS DE SEGURANÇA PARA SISTEMAS DE INFORMAÇÃO

2.16. O DGF realiza análise e testes periódicos que objetivam a identificação de eventuais vulnerabilidades técnicas e processuais que porventura venham a apresentar risco às informações e seus sistemas críticos de negócios, que incluem:

- Teste mensais de vulnerabilidade da rede do DGF por terceiro no mercado;
- Avaliação de todas as tentativas de acesso não autorizadas, com a finalidade de se apurar eventuais novas fragilidades do sistema;

- Revisão periódica de usuários ativos nos sistemas, de forma a assegurar que os acessos de funcionários desligados foram efetivamente eliminados após o desligamento.

2.17. Todos os testes com novas tecnologias a serem implementadas pelo DGF serão realizados em ambiente de homologação segregado. Este procedimento visa evitar a contaminação dos sistemas em aplicação, o que poderia prejudicar o curso normal dos negócios e colocar em risco os dados dos clientes, principalmente daqueles mantidos em meio eletrônico.

2.18. O DGF busca realizar a troca e atualização de seus sistemas de informação de forma constante, de modo a preservar a integridade de seus dados e prevenir a ocorrência de quaisquer violações de segurança.

2.19. Ainda, o DGF também atualiza os testes acima descritos de forma periódica, além de contratar terceiros especializados para verificar a adequação das tecnologias de segurança da informação, conforme aplicável.

III. POLÍTICA DE PRIVACIDADE DE DADOS

3.1. É responsabilidade de todos os Colaboradores do DGF zelar pela privacidade e pelos dados coletados pelo DGF nas atividades regulares, adotando os procedimentos que garantam, de forma ampla, as boas práticas relativas à privacidade e à proteção de dados pessoais.

3.2. Ademais, o DGF e seus Colaboradores devem adotar todas as medidas possíveis para mitigar riscos de incidentes de segurança e devem agir de forma transparente com todos os titulares de dados.

3.3. O DGF e seu Diretor de Compliance serão responsáveis, ainda, pelo tratamento dos dados coletados legitimamente e deverão, sempre que solicitado pelo titular do dado, informar o uso que estiver sendo feito do mesmo, e/ou realizar a exclusão de todas as informações da base de dados do DGF, de acordo com termos legais.

3.4. Esta Política se rege pelos princípios e obrigações seguintes:

- Toda a pessoa natural tem assegurada a titularidade de seus dados pessoais e a garantia dos seus direitos fundamentais de liberdade;
- A Lei Geral de Proteção de Dados aplica-se independentemente dos meios e/ou formas de tratamento de dados coletados ou recebidos;
- O titular dos dados possui o direito de acesso às informações sobre o tratamento

de seus dados, com a finalidade de terminar quais dados foram tratados, quais estão sendo compartilhados e qual a finalidade do tratamento;

- O DGF manterá registros escritos que demonstrem a adoção de medidas de tratamento aos princípios estabelecidos na LGPD;
- A Lei Geral de Proteção de Dados impõe que os dados dos titulares só poderão ser tratados se fundamentados nos seguintes princípios:
  - Finalidade – o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias;
  - Adequação – o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
  - Necessidade – o tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
  - Livre acesso – é garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
  - Qualidade dos dados – é garantido aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
  - Transparência – é garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observado os segredos comerciais e industriais;
  - Segurança – devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
  - Prevenção – devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
  - Não discriminação – impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e
  - Responsabilização e prestação de contas – demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas;
- A LGPD estabelece, ainda, que o tratamento de dados pessoais pode ocorrer se:
  - Houver o consentimento do titular;
  - Existir a necessidade de cumprir uma obrigação legal ou regulatória do

controlador de dados e/ou do DGF;

- A administração pública necessitar dos dados tratados e compartilhados para a execução de políticas públicas previstas em leis e regulamentos;
- For necessário para a realização de estudos por órgão de pesquisa, garantidas, sempre que possível, a anonimização dos dados pessoais;
- Necessário para a execução de contrato ou de procedimentos contratuais preliminares;
- Necessário para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Necessário para o exercício regular de direito em processo judicial, administrativo ou arbitral;
- Necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Indispensáveis para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- Para a proteção do crédito, inclusive, quanto disposto em legislação vigente.

- O DGF poderá, mediante requisição expressa do titular, solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto
- Nos casos em que o DGF tratar dados em sistemas de decisões automatizadas, o titular dos dados terá o direito de solicitar a revisão de tal tratamento por uma pessoa natural;
- Em caso de descumprimento da LGPD, o titular dos dados poderá ser opor ao tratamento de seus dados, desde que o tratamento tenha ocorrido sem consentimento expresso e com base em outros finalidades da lei;
- Os titulares de dados poderão, a qualquer tempo, revogar o consentimento dado anteriormente bastando, apenas, que seja realizado o preenchimento de uma solicitação de próprio punho; e
- O DGF deverá, a qualquer tempo e desde que expressamente solicitado pelo titular dos dados, excluir todos os dados recebidos e tratados, salvo em condições que houver necessidade de manutenção de registros para fins legais.

III.A. COOKIES

3.5. Cookies são informações geradas a partir do acesso do usuário ao site e que geralmente ficam armazenadas para "memorizar" preferências do usuário e informações de navegação; dessa forma, os cookies identificam posteriores visitas do usuário a fim de melhorar a experiência daquele usuário.

3.6. O website do DGF poderá fazer o uso de cookies.

3.7. Antes de o website ativar qualquer cookie no computador do visitante, lhe será solicitada autorização clara e explícita para o fim a que o cookie se destina.

IV. POLÍTICA DE SIGILO E CONFIDENCIALIDADE

4.1. Nenhuma Informação Confidencial (conforme definido abaixo) deve, em qualquer hipótese, ser divulgada fora do DGF. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em consonância com as normas legais e de Compliance do DGF.

4.2. Os dados pessoais sensíveis, nos termos da Lei Geral de Proteção de Dados, são protegidos e não deverão ser compartilhados pelos Colaboradores do DGF. Além disso, eles serão, sempre que solicitado, disponibilizados aos seus titulares ou excluídos das bases de dados do DGF, nos termos da referida Lei.

4.3. Todos os Colaboradores são responsáveis por manter o sigilo de informações confiadas aos mesmos em razão de suas funções no DGF.

4.4. Cada Colaborador deve manter-se continuamente sensível à natureza confidencial e privilegiada das informações às quais tem acesso com relação às atividades do DGF, principalmente no que diz respeito às Informações Confidenciais (conforme definido abaixo), devendo exercer a maior discrição ao discutir quaisquer assuntos relacionados a trabalho com quaisquer pessoas ou terceiros. As proibições aqui estabelecidas deverão ser aplicáveis, inclusive, após eventual desligamento do Colaborador com o DGF, durante todo tempo em que a Informação Confidencial continuar como sigilosa.

4.5. São consideradas informações confidenciais (“Informações Confidenciais”), para os fins deste Manual de Compliance e das demais Políticas, independentemente do formato em que se encontram, podendo estar armazenadas em discos, pen-drives, mídias diversas, documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre o DGF, seus sócios e clientes, incluindo:

- Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador e todo material intelectual e técnico desenvolvido na e para o DGF;
- Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais, incluindo saldos, extratos e posições de clientes dos clubes, fundos de investimento e carteiras geridos e/ou administrados pelo DGF;
- Operações estruturadas, demais operações e seus respectivos valores

analisados ou realizados pelos clubes de investimento, fundos de investimento e carteiras geridos e/ou administrados pelo DGF;

- Relatórios, estudos, opiniões internas sobre ativos financeiros, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades do DGF e a seus sócios ou clientes;
- Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimento geridos e/ou administrados pelo DGF;
- Transações realizadas e que ainda não tenham sido divulgadas publicamente;
- Outras informações obtidas junto aos Colaboradores, sócios ou demais entidades relacionadas ao DGF ou, ainda, junto aos seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

4.6. Salvo descrição abaixo ou regras procedimentais a serem criadas pelo DGF, nenhum Colaborador deverá, com relação às Informações Confidenciais, divulgar ou conferir acesso a pessoas ou terceiros estranhos ao DGF, incluindo membros de sua família, ou à qualquer Colaborador que não esteja autorizado a receber as informações, durante ou após o período de trabalho, ou, ainda, conferir acesso a qualquer arquivo ou banco de dados que contenha Informações Confidenciais.

4.7. A divulgação de Informações Confidenciais será limitada aos Colaboradores que tenham necessidade válida de conhecer tais informações, sendo proibida divulgação de Informações Confidenciais, exceto quando necessário para fins regulatórios ou em razão de obrigação legal.

4.8. Todos os Colaboradores que violarem a presente norma de confidencialidade estarão sujeitos a medidas disciplinares, nos termos da legislação e regulamentação aplicável, não importando se tenha sido auferido ou não qualquer benefício com a divulgação da Informação Confidencial.

4.9. Colaboradores que entrarem em contato com as Informações Confidenciais ou tiverem alguma dúvida quanto à confidencialidade da informação deverão entrar em contato por meio dos canais indicados no presente Manual de Compliance, para orientação. De qualquer forma, quaisquer dúvidas sobre a proteção e confidencialidade das informações deverão ser resolvidas em favor da proteção e do sigilo de tais informações.

4.10. Todas as negociações envolvendo o DGF, tais como (i) avaliação de oportunidades, (ii) contratação de terceiros, (iii) parcerias, (iv) co-investimentos, dentre outras em que faça necessário o intercâmbio de Informações Confidenciais, deverão ser precedidas da

assinatura de um contrato de confidencialidade padrão, previamente aprovado pelo Diretor de Compliance ou pelo Comitê de Ética e Compliance do DGF.

IV.A. DIVULGAÇÃO PARA OUTROS COLABORADORES

4.11. As Informações Confidenciais poderão ser compartilhadas com outros Colaboradores do DGF sempre que houve um justo motivo para o compartilhamento e a necessidade de acesso às informações em razão das atividades do DGF para com os seus clientes.

IV.B. DIVULGAÇÃO PARA TERCEIROS

4.12. Os Colaboradores concordam expressamente em manter em estrita confidencialidade e guardar sigilo absoluto sobre todas as Informações Confidenciais, não as revelando para quaisquer terceiros, com exceção de daqueles que devam, necessariamente, tomar conhecimento das Informações Confidenciais para fins de análise e consumação de quaisquer negócios de interesse do DGF.

4.13. O DGF deverá exigir que qualquer intermediário financeiro, agente ou prestador de serviço contratado pelo DGF cumpra as normas de confidencialidade referentes às Informações Confidenciais e utilize as informações fornecidas pelo DGF apenas e exclusivamente para a execução do serviço específico solicitado pelo DGF.

4.14. No caso de as Informações Confidenciais serem informações pessoais sensíveis, o compartilhamento só será permitido com a expressa autorização do cliente e caso o prestador de serviço possua Política de Confidencialidade em consonância com a Lei Geral de Proteção de Dados.

IV.C. DIVULGAÇÃO POR DETERMINAÇÃO LEGAL

4.15. Informações Confidenciais também poderão ser compartilhadas nos casos de cumprimento de ordens legais, administrativas ou judiciais sendo que, nestes casos, o DGF deverá divulgar apenas a informação requerida pela autoridade pública (inclusive, no caso de autoridades reguladoras e autorreguladoras).

IV.D. INFORMAÇÃO PRIVILEGIADA, INSIDER TRADING E “DICAS”

4.16. Os Colaboradores são proibidos, sob qualquer hipótese, de realizar ou recomendar investimentos ou desinvestimentos, em benefício próprio, de clientes ou de quaisquer outros terceiros, em descumprimento aos procedimentos descritos neste Manual de Compliance e/ou motivados pelo conhecimento de Informações Privilegiadas.

4.17. Os Colaboradores devem estar cientes de que qualquer utilização indevida de informação privilegiada terminantemente proibida e representa descumprimento legal grave e pode ter como consequência a aplicação de sanções administrativas, especialmente pela Comissão de Valores Mobiliários ("CVM"), além de responsabilização civil e criminal aplicável.

4.18. O disposto nos itens de "Informação Privilegiada" e "Insider Trading e "Dicas'" abaixo deve ser analisado não só durante a vigência de seu relacionamento profissional com o DGF, mas, também, após o seu término

Informação Privilegiada

4.19. Para fins deste Manual de Compliance, "Informação Privilegiada" significa qualquer informação relevante a respeito de qualquer companhia que não tenha sido divulgada publicamente e que tenha sido 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.

4.20. Exemplos de Informações Privilegiadas incluem 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) ou qualquer outro fato que seja objeto de um acordo de confidencialidade firmado por uma empresa com o DGF ou com terceiros.

4.21. As Informações Privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

Insider Trading e "Dicas"

4.22. Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Privilegiada, com o objetivo de conseguir benefício próprio, de terceiros ou de Colaboradores do DGF.

4.23. "Dica" é a transmissão, a qualquer terceiro, estranho às atividades do DGF, de Informação Privilegiada que possa ser usada como benefício na compra e venda de títulos ou valores mobiliários.