MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS DA SABRA CAPITAL GESTÃO DE RECURSOS LTDA.

("Sociedade")

Versão Março/2018

CAPÍTULO I
DO OBJETIVO

1.1. A Sociedade deve garantir, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissional. Os controles internos devem ser efetivos e consistentes com a natureza, complexidade e risco das operações realizadas.

1.2. O presente instrumento tem como objetivo a definição de regras e princípios norteadores das condutas dos colaboradores da Sociedade, assim entendidos seus (i) sócios; (ii) funcionários; ou (iii) de quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Sociedade, tenham acesso a informações relevantes sobre a Sociedade ou sobre suas estratégias de investimento, em especial no que concerne ao devido tratamento de informações confidenciais, investimentos próprios, conflitos de interesse, contingência e segurança da informação.

1.3. Tais princípios deverão ser compulsoriamente observados pelos colaboradores da Sociedade, declarando estarem cientes de todas as regras e políticas aqui expostas, que lhes foram previamente apresentadas pelo responsável pelo compliance da Sociedade e em relação às quais não existe qualquer dúvida, comprometendo-se a observá-las a todo tempo no desempenho de suas atividades.

CAPÍTULO II
DOS PRINCÍPIOS NORTEADORES DAS CONDUTAS

2.1. Todos os colaboradores da Sociedade deverão pautar suas condutas em conformidade com os valores da boa-fé, lealdade e veracidade.

2.2. Todos os esforços em prol da eficiência na gestão dos fundos e carteiras devem visar à obtenção de melhor retorno aos investidores, com base na análise e interpretação de informações divulgadas ao mercado, e jamais no acesso a informações privilegiadas.

2.3. Os colaboradores da Sociedade devem estar conscientes de que a informação transparente, precisa e oportuna constitui o principal instrumento à disposição do público investidor para que lhes seja assegurado o indispensável tratamento equitativo.

2.4. O relacionamento dos colaboradores da Sociedade com os participantes do mercado e com os formadores de opinião deve dar-se de modo ético e transparente.

2.5. Todos os profissionais que desempenhem funções ligadas à administração de carteiras de valores mobiliários devem atuar com imparcialidade e conhecer o Código de Ética e as normas aplicáveis, bem como as políticas previstas pela Instrução CVM 558/2015 e as disposições relativas a controles internos.

CAPÍTULO III
DA SEGREGAÇÃO FÍSICA E VIRTUAL / ACESSO AOS ARQUIVOS

3.1. A equipe de gestão de recursos de terceiros localiza-se em sala devidamente segregada dos demais ambientes do imóvel da Sociedade, resguardando, assim, a privacidade e o sigilo de que os profissionais que compõem a citada equipe precisam para o desempenho das respectivas atividades.

3.2. Já no que tange à segregação virtual das informações com as quais a equipe de gestão profissional de recursos de terceiros tenha contato, vale ressaltar que todos os computadores da Sociedade são acessados mediante senhas pessoais e intransferíveis, impedindo o acesso de terceiros não autorizados aos arquivos armazenados digitalmente na Sociedade.

3.3. Neste sentido, foram implementados os seguintes cuidados nos sistemas operacionais da Sociedade:

PROTEÇÃO CONTRA ADULTERAÇÕES

Para a proteção dos recursos computacionais são adotadas as seguintes medidas:

(i) **Controle de Acesso -** tem como objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

(ii) **Lógico -** conjunto de procedimentos e medidas com o objetivo de proteger os dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou por outros programas de computador. São estes os controles implementados:

- **Identificação e Autenticação de usuário –** Os usuários dos sistemas computacionais são identificados e autenticados durante um processo, chamado logon. Os processos de logon são usados para conceder acesso aos dados e aplicativos em um sistema computacional e orientam os usuários durante sua identificação e autenticação. O processo de logon irá: (i) evitar identificar o sistema ou suas aplicações até que o processo de logon esteja completamente

concluído; (ii) limitar o número de tentativas de logon sem sucesso a três tentativas; (iii) registrar as tentativas de acesso inválidas; (iv) mostrar as seguintes informações, quando o procedimento de logon no sistema finalizar com êxito: data e hora do último logon com sucesso; e detalhes de qualquer tentativa de logon sem sucesso, desde o último procedimento realizado com sucesso.

- **Atribuição de Direitos** – São definidos direitos de acesso individualmente para cada usuário e objeto. A forma a ser adotada será a mais comumente definida como matriz de controle de acesso. Nessa matriz é possível fazer duas análises: uma em relação aos usuários; outra, em relação aos objetos. Na primeira abordagem, cada usuário recebe uma permissão (ou capacidade) que define todos os seus direitos de acesso. As permissões de acesso são, então, atributos que definem o que ele pode ou não fazer com outros objetos.

REGISTROS DE ALTERAÇÕES

O monitoramento dos sistemas de informação é feito normalmente pelos registros de log, trilhas de auditoria ou outros mecanismos capazes de detectar invasões. Esse monitoramento é essencial à segurança de informações, já que é praticamente impossível eliminar por completo todos os riscos de invasão por meio da identificação e autenticação de usuários.

Na ocorrência de uma invasão, falha do sistema ou atividade não autorizada, é imprescindível reunir evidências suficientes para que possam ser tomadas medidas corretivas necessárias ao restabelecimento do sistema às suas condições normais, assim como medidas administrativas e/ou judiciais para investigar e punir os invasores.

A forma mais simples de monitoramento é a coleta de informações, sobre determinados eventos, em arquivos históricos, mais conhecidos como logs. Com essas informações, a equipe de segurança deverá ser capaz de registrar eventos e de detectar tentativas de acesso e atividades não autorizadas após sua ocorrência.

Para este fim são utilizados: (i) Logs do Sistema Operacional do Servidor; (ii) Logs de Auditoria ativados no servidor de arquivos; (iii) Logs do Firewall; e (iv) Logs do Antivírus.

Para garantia de integridade de mensagens de e-mail são adotadas assinaturas eletrônicas de e-mail, garantindo a integridade e confiabilidade das mensagens enviadas pelos usuários da rede.

SISTEMAS DE BACKUP E SEGURANÇA DE DADOS

Todas as informações e arquivos da Sociedade, do banco de dados dos clientes e os modelos dos analistas são armazenados em servidor na nuvem.

O sistema de backup é composto por duas rotinas bem distintas:

a) Backup de Arquivos: Esta rotina destina-se a efetuar um backup completo do servidor em nível de arquivos e sistema operacional. Os backups são salvos em mídias removíveis, seguindo o modelo Avô/Pai/Filho modificado. Neste esquema têm-se backups completos e diferenciais. A cada semana, é feito um backup completo e, a cada dia, é feito um diferencial. É adotado um sistema com 18 rotinas, sendo 12 de backups completos mensais (rotação anual), 4 backups completos semanais (rotação mensal) e 4 backups diferenciais diários (rotação semanal). Com este cenário, consegue-se uma precisão de, no mínimo, um dia na última semana, uma semana no último mês e um mês nos últimos doze meses. Devido a sua eficiência e boa relação custo/benefício, este certamente é o método mais utilizado atualmente.

b) Backup de AD: Esta rotina destina-se a efetuar um backup semanal completo do Active Directory, em mídias removíveis junto com o backup de arquivos. Desta forma será possível recompor a segurança de acesso aos serviços de rede nele configurado.

As rotinas de backup seguirão as seguintes premissas:

- Os dados são removidos do site diariamente;

- Todos os backups serão criptografados garantindo a segurança dos mesmos contra furto de mídia; e

- Todos os dados dos usuários estarão no servidor e serão salvos em backup diariamente.

CAPÍTULO IV
DO TRATAMENTO DAS INFORMAÇÕES CONFIDENCIAIS

4.1. Os colaboradores da Sociedade deverão:

a) abster-se de utilizar informação privilegiada para obter, em benefício próprio ou de outrem, vantagem mediante negociação de títulos e/ou valores mobiliários;

b) abster-se de recomendar ou de qualquer forma sugerir que qualquer pessoa compre, venda ou retenha títulos e/ou valores mobiliários se a informação a que tenha acesso privilegiado puder, em tese, influenciar a tomada de qualquer uma dessas decisões;

c) advertir, de forma clara, àqueles em relação a quem se verificar a necessidade de revelar informação privilegiada, sobre a responsabilidade pelo cumprimento do

dever de sigilo e pela proibição legal de que se utilizem de tal informação para obter, em benefício próprio ou alheio, vantagem mediante negociação com tais títulos e/ou valores mobiliários; e

d) guardar sigilo sobre qualquer informação a que tenham acesso e que ainda não tenha sido divulgada ao público em geral, ressalvada a revelação da informação quando necessária para a Sociedade conduzir seus negócios de maneira eficaz e, ainda, somente se não houver motivos ou indícios para presumir que o receptor da informação a utilizará erroneamente.

4.2. Os colaboradores da Sociedade deverão guardar absoluto sigilo sobre toda e qualquer informação de natureza confidencial a que tenham acesso ou conhecimento no desempenho de suas funções, inclusive por meio dos sistemas e arquivos disponibilizados pela Sociedade para tanto. Tal determinação se aplica igualmente às informações obtidas/repassadas verbal ou informalmente, assim como às escritas ou impressas.

4.3. O fornecimento de informações confidenciais a pessoas externas à Sociedade será realizado somente nos casos estritamente necessários a fim de cumprir as normas atinentes à atividade desenvolvida pela Sociedade, proteção contra fraudes ou qualquer outra atividade ilegal suspeita, mediante contratos de confidencialidade, quando for o caso.

4.4. Sob nenhuma circunstância os colaboradores da Sociedade poderão utilizar informações confidenciais para obter vantagens pessoais, tampouco poderão fornecê-las para terceiros, inclusive familiares, parentes e amigos, ou mesmo a outros colaboradores da Sociedade que não necessitem de tais informações para executar suas tarefas.

4.5. Consideram-se informações de natureza confidencial todas as informações às quais os colaboradores da Sociedade venham a ter acesso em decorrência do desempenho de suas funções na Sociedade, inclusive por meio dos sistemas e arquivos disponibilizados pela Sociedade para tanto, que não sejam notória e comprovadamente de domínio público.

4.6. Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o colaborador deve, previamente à sua divulgação, procurar o responsável pelo compliance para obter orientação adequada, o qual deverá atribuir interpretação extensiva ao conceito de informação confidencial definido acima.

4.7. A revelação dessas informações a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada ao diretor responsável pela Sociedade para que este decida sobre a forma mais adequada para tal revelação.

4.8. Anualmente os colaboradores da Sociedade passarão por um programa de treinamento, de modo a esclarecer, dentre outras matérias, as suas obrigações quanto à manutenção da confidencialidade das informações.

4.9. A não observância da confidencialidade estará sujeita à apuração de responsabilidades nas esferas cível e criminal, sem prejuízo da sujeição às penalidades previstas neste Manual.

CAPÍTULO V
DOS TESTES PERIÓDICOS DE SEGURANÇA

5.1. As rotinas adotadas pelo compliance para fins de verificação da conduta dos colaboradores da Sociedade deverão ser realizadas conforme descrito abaixo:

DIARIAMENTE: (a) verificação de questões como o trancamento das estações de trabalho e backup de informações e, sempre que detectado algum desvio de conduta, o colaborador deve ser imediatamente reprimido pelo compliance, que volta a instruí-lo a respeito das boas práticas de conduta; (b) verificação do enquadramento das operações realizadas pela Sociedade no âmbito do mercado financeiro e de capitais às normas que as regem, avaliando, ainda, tais operações sob a ótica da Política de Combate e Prevenção à Lavagem de Dinheiro adotada pela Sociedade.

SEMANALMENTE: (a) checagem, sem aviso prévio, das mensagens eletrônicas enviadas e recebidas pelos colaboradores da Sociedade, assegurando a utilização adequada desta ferramenta.

MENSALMENTE: (a) verificação da adequação dos investimentos pessoais dos colaboradores à Política estabelecida neste Manual. Esta verificação será realizada através da análise de relatórios acerca dos investimentos pessoais dos colaboradores, recolhendo declaração dos mesmos nas quais atestam o cumprimento da Política de Investimentos Pessoais da Sociedade.

SEMESTRALMENTE: (a) validação de todos os regulamentos e normas de conduta interna, rotinas e procedimentos, adequando-os às normas e instruções dos órgãos reguladores da atividade desenvolvida pela Sociedade. Esta validação deverá ser realizada ainda sempre que o compliance julgar necessário, considerando eventuais alterações na legislação.

ANUALMENTE: (a) a elaboração, implementação e manutenção dos treinamentos com o objetivo de orientar seus colaboradores acerca das normas de conduta internas e da regulamentação vigente que rege a atividade de administração de títulos e valores mobiliários desenvolvida pela Sociedade; (b) envio das informações periódicas exigidas pela CVM, bem como a toda e qualquer entidade auto reguladora a qual a Sociedade esteja vinculada.

CAPÍTULO VI
DO TREINAMENTO

6.1. A Sociedade conta com um programa de treinamento dividido em 02 (duas) etapas distintas. A primeira etapa consiste na apresentação pelo responsável pelo compliance dos normativos internos ao colaborador no ato do seu ingresso na Sociedade, disponibilizando-se para prestar quaisquer esclarecimentos que se façam necessários.

6.2. Já a segunda etapa do treinamento ocorre anualmente quando o responsável pelo compliance, além de ratificar o conteúdo dos normativos internos e recolher a adesão dos colaboradores ao Código de Ética e as normas aplicáveis, bem como as políticas previstas pela Instrução CVM 558/2015 e as disposições relativas a controles internos, abordará as seguintes questões:

- Risco de imagem e risco legal (Descumprimento da legislação/regulamentação).
- Enforcement - Implicações da não observância das normas de conduta e ética.
- Boas práticas para manipulação da informação.
- Carreiras de informação e segregação de atividades de forma a evitar possíveis conflitos de interesses.
- Política de segurança e preservação da Informação, conceito "need to know".
- Registro das operações e das tomadas de decisão.
- Identificação e comunicação das operações atípicas/suspeitas.
- Utilização indevida de informações privilegiadas.
- Parâmetros para os relatórios internos de análise.
- Segregação entre a gestão de recursos próprios e de terceiros – política de investimentos próprios.
- Regras de compliance.
- Obrigações e responsabilidades dos demais prestadores de serviços correlatos: administrador fiduciário / distribuidores / custodiante / auditor independente.
- Limites operacionais e de risco e enquadramento às políticas de investimento das carteiras sob gestão.
- Metodologia adotada para a contabilização de ativos.
- Regras de aplicação, resgate, carência e conversão de cotas. Liquidez dos ativos X regras de movimentação previstas em regulamento.
- Política de voto em assembleias.

CAPÍTULO VII
CONFLITO DE INTERESSE

7.1. Os colaboradores da Sociedade devem evitar desempenhar outras funções fora da Sociedade que possam gerar conflitos de interesse, ou mesmo aparentar tais conflitos. Também devem evitar defender interesses de terceiros que possam gerar conflitos de

interesse na hora da tomada de decisão e implicar em algum tipo de prejuízo para a Sociedade ou seus investidores.

7.2. Ficam estritamente proibidas transações em nome da Sociedade com pessoas físicas ou jurídicas com as quais qualquer dos colaboradores da Sociedade ou pessoa a este ligada possua interesse financeiro.

7.3. Consideram-se conflitos de interesse, de forma genérica e não limitadamente, quaisquer interesses pessoais dos colaboradores, em benefício próprio ou de terceiros, contrários ou potencialmente contrários aos interesses da Sociedade, dos investidores dos fundos e demais veículos de investimento geridos pela Sociedade e dos demais clientes da Sociedade.

7.4. Caso o colaborador resolva exercer outras atividades, sejam elas com ou sem fins lucrativos, além da praticada junto à Sociedade, deve comunicar previamente ao responsável pelo compliance para a devida aprovação a fim de evitar potenciais conflitos de interesse.

CAPÍTULO VIII
INVESTIMENTOS PRÓPRIOS

8.1. Todo e qualquer investimento no âmbito do mercado financeiro e de capitais realizado em nome próprio do colaborador da Sociedade deverá se dar através de: (i) aplicação em fundos de investimento abertos e cujas cotas sejam disponíveis ao público em geral; (ii) títulos públicos negociados através do Tesouro Direto; ou (iii) aplicação em quaisquer outros ativos disponíveis para negociação no mercado, desde que não sejam o foco de atuação da Sociedade, devendo tais posições serem mantidas por um período mínimo de 30 (trinta) dias, com o objetivo de evitar investimentos de natureza especulativa.

8.2. Excepcionalmente, determinadas operações não enquadradas no item 8.1. acima poderão ser realizadas em nome próprio dos colaboradores, desde que prévia e expressamente aprovadas pelo responsável pelo compliance e não configurem situação de conflito com as carteiras administradas pela Sociedade.

8.3. Para fins de autorização das operações de que trata o item 8.2. acima, o compliance deverá analisar os seguintes aspectos:

(i) se a operação pretendida poderá implicar algum prejuízo para a Sociedade ou seus investidores;

(ii) se a operação pretendida poderá, de qualquer forma, limitar a discricionariedade dos colaboradores da Sociedade na análise dos títulos e valores mobiliários e na tomada de

decisão de investimentos. Caso esta operação limite o poder de análise e decisão dos colaboradores da Sociedade, o compliance não poderá autorizá-la; e

(iii) reais objetivos da operação pretendida, de modo a assegurar a boa-fé do colaborador da Sociedade e manter a estrita relação fiduciária entre a Sociedade e seus investidores.

CAPÍTULO IX
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

9.1. Os colaboradores da Sociedade que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

9.2. Todos os computadores da Sociedade possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores utilizados pela Sociedade permitem a identificação do seu remetente/receptor.

9.3. A troca de informações entre os colaboradores da Sociedade deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de compliance deve ser acionada previamente à revelação.

9.4. O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros.

9.5. A segregação virtual das informações confidenciais é garantida pela utilização de senhas de acesso, pessoais e intransferíveis, permitindo a identificação do seu usuário. Todos os documentos arquivados nos computadores da Sociedade são objeto de back-up diário com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

9.6. A base de dados eletrônicos utilizada pela Sociedade é segregada de modo que informações confidenciais são arquivadas em pastas de acesso restrito, através da utilização de senha, a pessoas previamente autorizadas pelo compliance da Sociedade.

9.7. O sistema eletrônico utilizado pela Sociedade está sujeito à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

CAPÍTULO X
DISPOSIÇÕES GERAIS E *ENFORCEMENT*

10.1. O presente Instrumento prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da Sociedade aos seus termos e condições.

10.2. A título de *enforcement*, vale notar que a não observância dos dispositivos do presente Manual resultará em advertência, suspensão ou demissão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.