POLÍTICA DE COMPRA E VENDA DE VALORES MOBILIÁRIOS POR GESTORES, EMPREGADOS E COLABORADORES

1. INTRODUÇÃO

A DG Administradora de Carteiras é uma gestora de recursos com sede na cidade de São Paulo cuja gestão estará permeada em fatores macroeconômicos baseado em análises fundamentalista e grafista.

Com o intuito de formalizar o processo de seleção e alocação de ativos da DG Administradora desenvolvemos o manual de Política de Decisão de Investimentos (“PDI”).

As aplicações diretas em ações, cotas de fundos, títulos ou outros valores mobiliários terão caráter de investimento e não simplesmente especulativo, sendo necessária, portanto, a manutenção de tais aplicações pelo prazo mínimo de 30 (trinta) dias.

2. COMITÊ DE INVESTIMENTO

Este comitê é composto pelos sócios e diretores da DG Administradora. O Compliance Officer fará a coordenação direta deste Comitê.

A principal atribuição desse comitê será assessorar o gestor da DG Administradora sobre a definição das metodologias de alocação de recursos bem como a avaliação da gestão.

O Comitê se reunirá, ordinariamente, em periodicidade quinzenal e, extraordinariamente, sempre que necessário para desempenhar todas as suas atribuições.

3. SELEÇÃO DE ATIVOS

Através das reuniões realizadas por meio do Comitê de Investimento serão definidas estratégias de alocação de ativos de acordo com o cenário macro atual.

Serão realizadas avaliações sobre as empresas já investidas e sobre aquelas que tenham potencial de rentabilidade.

Os portfólios serão sempre bem diversificados entre empresas e setores a fim de diluir possíveis perdas. Os múltiplos das empresas serão sempre analisados e comparados ao respectivo lucro, utilizaremos também projeções baseadas em fluxo de caixa descontado a partir dos balanços e demonstrativos publicados pelas empresas.

O valor intrínseco da ação será analisado por dois pontos de vista, o primeiro é altamente estatístico e envolve uma série de indicadores financeiros, e o segundo envolve a construção de uma estimativa específica da empresa, para esse segundo ponto serão considerados tanto a evolução dos fundamentos da empresa como também o impacto sobre estes das mudanças de mercado como taxa de juros, câmbio, cenário político, econômico, validando assim a estratégia principal de alocação adotada pela DG baseada em um horizonte de longo prazo.

Através das reuniões do Comitê de Investimento da DG serão repassadas e conferidas as posições atuais, novas projeções serão elaboradas adequando nossos portfólios sempre ao atual cenário dos mercados onde estivermos presentes.

Para seleção de ativos de renda variável serão utilizados indicadores de mercado, bem como research próprios e de terceiros. Para cotas de fundos faremos análises quantitativas e qualitativas, entrevista com gestores, análise histórica de desempenho, comparações com benchmark, entre outros.

Da mesma forma criteriosa utilizada na seleção de empresas para investimento, o desinvestimento também ocorrerá quando, após revisão de todos esses fatores descritos acima, identificarmos que o retorno projetado para cada ativo não for compatível com os riscos envolvidos.

4. METODOLOGIA DE GESTÃO DE RISCOS

Gerenciamos nossa exposição aos riscos de mercado através da diversificação de exposições, controlando o tamanho de nossas posições e estabelecendo hedges econômicos relativos a títulos ou derivativos, utilizando a metodologia do calculo do VAR (Value at Risk).

A Gestão de Riscos de Mercado está subordinada ao Compliance que tem a responsabilidade principal de avaliar, monitorar e gerir riscos de mercado. Em caso de alguma posição ficar fora dos parâmetros o comitê de compliance repassa a informação ao gestor que irá efetuar os devidos ajustes para o enquadramento de acordo com os preços de mercado e critérios pré-estabelecidos.

As métricas de risco utilizadas para horizontes tanto de curto prazo quanto longo prazo incluem VaR (Value at Risk) e métricas de sensibilidade. Para horizontes de longo prazo, nossas principais métricas de risco são os testes de estresse.

Os relatórios de risco incluem detalhes sobre os riscos principais, os impulsionadores e as mudanças para cada operação e para cada negócio. Nosso modelo de Risco Operacional foi elaborado a fim de eliminar os riscos de perdas geradas por sistemas e controles inadequados, falhas de gerenciamento e erros humanos, tais como:

1.Risco de Obsolescência;

2.Risco de Equipamento;

3.Risco de Tecnologia;

4.Risco de Erro Não Intencional ("erro humano");

5.Risco de Fraudes;

6.Risco da Qualificação de Pessoal;

7.Risco de Lavagem de Dinheiro; e

8.Risco de Acesso.

Em relação aos 3 (três) primeiros itens acima, estes serão controlados pelo Compliance Officer, contando com apoio de uma Área de Suporte de Tecnologia. Dentro da classificação Risco Operacional, o Compliance Officer controlará, diretamente, os 5 (cinco) últimos riscos supracitados.

5. PLANO DE CONTINUIDADE E CONTINGÊNCIA DE NEGÓCIOS

Para a manutenção da disponibilidade total dos sistemas utilizados pela DG foi necessária a elaboração de um Plano de Ação, denominado PCN (plano de continuidade de negócios). Para tanto, foram necessários um conjunto com outros três planos conforme segue;

5.1 PLANO DE GERENCIAMENTO DE CRISES

Essa é a primeira etapa em caso de alguma ocorrência. Definimos aqui a responsabilidade de cada membro das equipes envolvidas com o acionamento da contingência.

Participantes e suas Responsabilidades no Grupo de Gerenciamento de Crise

* Coordenador do Plano:

- ✓ *Nomear os Participantes do Plano;*
- ✓ *Garantir a documentação atualizada dos sistemas;*
- ✓ *Disponibilizar recursos para ação de resposta;*
- ✓ *Promover treinamento aos colaboradores;*
- ✓ *Promover exercícios simulados;*
- ✓ *Enviar relatório final de situação para o Comitê de Segurança da Informação*

* Grupo de Atuação Direta:

- ✓ *Planejamento das Ações de resposta relacionadas à sua área;*
- ✓ *Determinar as orientações para as equipes de atuação;*
- ✓ *Seguir os procedimentos descritos para determinado cenário;*
- ✓ *Elaborar situação final de situação;*

* Grupo de Apoio:

- ✓ *Planejamento das ações de resposta relacionadas à sua área;*
- ✓ *Seguir as orientações do Coordenador do Plano;*
- ✓ *Executar as atividades de infra-estrutura de engenharia e manutenção;*
- ✓ *Executar as atividades de provimento de recursos;*
- ✓ *Elaborar relatório final de situação;*

5.2 PLANO DE CONTINUIDADE OPERACIONAL

Tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade.

* Descrição dos Processos

- ✓ Cadastro de Clientes;
- ✓ Processos Administrativos;
- ✓ Produtos;
- ✓ Processos Financeiros;

* Do que proteger

- ✓ sabotagem de funcionários, ataques virtuais, vírus, perda repentina do serviço de internet, mal funcionamento do equipamento, etc;
- ✓ Desastres de causa Natural;

* Back Up

- ✓ Cada tipo de arquivo terá um tipo de cópia. Entretanto, serão segregados os arquivos de utilização pessoal dos arquivos de uso Corporativo;
- ✓ As cópias de todas as bases de dados corporativas serão realizadas com a frequência diária;
- ✓ O Backup será guardado em dois locais seguros;

* Estratégia de Continuidade

- ✓ O link de contingência irá funcionar com as mesmas especificações tecnológicas que a base principal;

- ✓ As duas cópias do Backup diários das bases de dados serão distribuídas da seguinte forma, uma ficará na sede da DG guardada no cofre, e a outra cópia irá para endereço onde estará toda estrutura de contingência, local distinto da sede.
- ✓ De acordo com qualquer necessidade teremos acessos aos terminais no local de contingência disponíveis para operação com cópia da última base salva que terá delay de no máximo 1 (um) dia.

5.3 PLANO DE RECUPERAÇÃO DE DESASTRES

Tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível.

Para perfeita funcionalidade do Plano de Recuperação de Desastres foi necessário desenvolver a nossa Análise de Impacto de Negócios – BIA, onde os processos são coletados para classificar cada processo por ordem de prioridade. O BIA inclui as seguintes informações;

- ✓ Uma descrição detalhada das funções e operações de cada departamento;
- ✓ Outras funções que tenham um impacto direto ou indireto sobre essa função;
- ✓ Quando a perda da função teria maior impacto;
- ✓ O tempo que a Asset levaria para perceber que a função falhou, tanto operacional quanto financeiramente;
- ✓ O equipamento de substituição necessário para se recuperar dessa perda de função, como telefones, PCs, software e estações de trabalho;
- ✓ Se a função pode ser realizada de casa, ou se ela pode ser deslocada para outra parte da empresa.

A equipe de planejamento de recuperação de desastre usa essas informações para classificar todas as funções segundo camadas de tempo. Por exemplo, a primeira camada inclui as funções que precisam estar online em poucos minutos em até 24 horas. A segunda camada inclui aquelas funções que precisam estar online em 24 a 36 horas, e assim por diante.

6. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da DG, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a DG, ou de qualquer natureza relativa às atividades da DG e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na DG, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo coordenador do Comitê de Ética.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da DG e circulem em ambientes externos à DG com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da DG. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da DG.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados semanalmente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, 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 na DG.

É proibida a conexão de equipamentos na rede da DG que não estejam previamente autorizados pela área de informática e pela área de compliance.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido,

conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da DG.

Em nenhuma hipótese um Colaborador pode emitir opinião por e-mail em nome da DG, salvo se expressamente autorizado para tanto.

Ainda, e-mails contendo palavras suspeitas, como código de ações, por exemplo, são automaticamente sinalizados para conferência na reunião quinzenal do Comitê de Ética, sendo que qualquer ocorrência mais suspeita será cuidadosamente analisada pelo referido comitê, que tomará as decisões cabíveis.

O Comitê de Ética também será avisado por e-mail em caso de tentativa de acesso aos diretórios e logins virtuais no servidor protegidos por senha. O comitê elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais devem obter autorização prévia do responsável pela área de informática. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao responsável pela Informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

As conversas telefônicas mantidas com a DG e seus profissionais, para tratar de quaisquer assuntos relativos às operações do cliente, poderão ser gravadas e seu conteúdo ser utilizado como prova no esclarecimento de questões relacionadas a sua conta e suas operações. As gravações poderão ser arquivadas pelo prazo de 180 (cento e oitenta) dias.

A DG se reserva no direito de gravar qualquer ligação telefônica dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela DG para a atividade profissional de cada Colaborador. Os integrantes do Comitê de Compliance são encarregados de, quinzenalmente, escutar, por amostragem, as ligações realizadas na mesa de operações, que serão gravadas. Qualquer informação suspeita encontrada será esclarecida imediatamente pelo Comitê de Compliance com registro em ata.

Todas as informações do servidor da DG, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com backup.

7. POLÍTICA DE COMPLIANCE E RISCO

O termo compliance é originário do verbo, em inglês, to comply, e significa “estar em conformidade com regras, normas e procedimentos”.

Visto isso, a DG adotou em sua estrutura as atividades de “Controles Internos” e “Compliance”. O responsável pelo compliance acumula estas duas funções e tem como foco principal garantir o cumprimento das normas regulamentares e processos internos, prevenindo e controlando os riscos envolvidos nas atividades da DG.

Por meio dos controles de compliance, qualquer desvio em relação às políticas da DG é observado e minimizado (ou evitado, quando se toma conhecimento prévio do risco inerente a determinada atividade).

O Compliance Officer tem como principais atribuições e responsabilidades o suporte a todas as áreas no que concerne a esclarecimentos de todos os controles e regulamentos internos (compliance), bem como no acompanhamento de conformidade das operações e atividades da DG com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação e monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (enforcement).

Não obstante, o Compliance Officer é, também, o responsável pela observância dos parâmetros e procedimentos relativos à precaução à lavagem de dinheiro.