POLÍTICA DE SEGURANÇA E SIGILO DAS INFORMAÇÕES

Dg Administradora de Carteiras de Valores Mobiliários

INTRODUÇÃO

A Política de Segurança e Sigilo das Informações (“SSI”) da DG ADMINISTRADORA DE CARTEIRAS DE VALORES MOBILIÁRIOS LTDA (“DG”), tem como objetivo estabelecer mecanismos para garantir o controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso nossos sócios, diretores, administradores, profissionais e terceiros contratados (“Colaboradores”).

Assegurar a existência de testes periódicos de segurança para os sistemas de informação, em especial para os mantidos em meio eletrônico.

Implantar e manter treinamento para nossos sócios, diretores, alta administração e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas e participem do processo de decisão de investimento.

A informação alcançada em função da atividade profissional desempenhada na DG não pode ser transmitida de forma alguma a terceiros não colaboradores ou a colaboradores não autorizados. Incluem-se aqui, por exemplo, posições compradas ou vendidas, estratégias e conselhos de investimento ou de desinvestimento, relatórios, análises e opiniões sobre ativos financeiros, dados a respeito de resultados financeiros antes da publicação dos balanços e balancetes da DG e dos fundos geridos e transações efetuadas e que ainda não foram publicadas, informações oriundas de estudo efetuado pelas áreas de Research de Ações, Renda Fixa, Derivativos e Hedge Funds, mesmo que os ativos correspondentes não tenham sido contraídos na composição do portfólio da DG etc.

Os controles iniciais tratam dos seguintes tópicos;

I. Regras de acesso às informações confidenciais, reservadas ou privilegiadas, indicando como se dá o acesso e controle das pessoas autorizadas e não autorizadas a essas informações, inclusive nos casos de mudança de atividade dentro da mesma instituição ou desligamento do profissional;
II. Regras específicas sobre proteção da base de dados e procedimentos internos para tratar casos de vazamento de informações confidenciais, reservadas ou privilegiadas mesmo que oriundos de ações involuntárias; e
III. Regras de restrição ao uso de sistemas, acessos remotos e qualquer outro meio/veículo que contenha informações confidenciais, reservadas ou privilegiadas.

Pode-se considerar como informação privilegiada qualquer informação importante a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

São exemplos de informações privilegiadas: informações verbais ou documentadas referentes a resultados operacionais de empresa, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, e qualquer outro acontecimento que seja motivo de um acordo de confidencialidade fixado por uma empresa com a DG ou com terceiros.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Quem tiver acesso a uma informação privilegiada deverá transmiti-la rapidamente ao Comitê de Compliance, não podendo comunicá-la a ninguém, nem mesmo a outros membros da DG, profissionais de mercado, amigos e parentes, e nem a usar, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter

privilegiado da informação, deve-se rapidamente relatar o ocorrido ao Comitê de Compliance. Quem tiver acesso a uma informação privilegiada deverá reduzir ao máximo a circulação de documentos e arquivos com tal informação.

É proibida a prática dos casos mencionados neta política SSI por qualquer membro da DG, seja agindo em benefício próprio, da DG ou de terceiros.

O disposto nos itens de "Informação Privilegiada" deve ser analisado não só durante a vigência do relacionamento profissional do Colaborador com a DG, mas mesmo após o seu término.

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.

INFORMAÇÕES CONFIDENCIAS E PRIVILEGIADAS

Conforme disposto na presente Política de SSI da DG, todos os colaboradores deverão seguir as regras de confidencialidade com o intuito de preservar informações confidenciais, cujo conceito deve ser entendido como quaisquer informações que a DG ou seus clientes forneçam aos colaboradores que não sejam de domínio público, não tenham sido divulgadas ao mercado, ou que a DG não deseje que sejam divulgadas.

São exemplos de informações confidenciais, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, que não devem ser divulgadas a terceiros:

I. Os negócios da Gestora, seus clientes, investimentos, estruturas societárias, custos, preços, lucros, relatórios financeiros, produtos, serviços, equipamentos, sistemas, procedimentos, operações, planos de negócios, operações financeiras e contratos;

II. Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

III. Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais; incluindo saldos, extratos e posições de clientes dos fundos de investimento e carteiras administradas geridos pela Gestora;

IV. Operações estruturadas, demais operações e seus respectivos valores analisadas ou realizadas pelos fundos de investimento e carteiras administradas geridos pela DG;

V. Relatórios, estudos, opiniões internas sobre ativos financeiros;

VI. Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

VII. Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da DG e a seus sócios ou clientes;

VIII. Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimento geridos pela DG;

IX. Transações realizadas e que ainda não tenham sido divulgadas publicamente;

X. Outras informações obtidas junto a colaboradores ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Não é permitido o uso indevido ou a divulgação de informações confidenciais obtidas por qualquer meio, seja ele contratual, advindo do relacionamento com cliente ou referente a investimentos das carteiras ou fundos de investimento geridos pela DG.

Informações consideradas confidencias devem ser acessadas apenas por colaboradores que necessitem de tal acesso para a execução de suas atividades, de forma a preservar ao máximo o seu caráter restrito. Essas informações deverão ser utilizadas exclusivamente para o cumprimento das atividades na DG e os colaboradores obrigam-se a não compartilhar tal informação com terceiros.

É vedado aos colaboradores, mesmo após o fim do vínculo de trabalho deste com a DG, o uso ou divulgação de qualquer informação ou dado ao qual teve acesso em função de suas atividades, exceto caso, à época, tais dados já sejam de domínio público.

Caso seja determinada a revelação de alguma das informações delineadas nesta política de SSI por alguma autoridade governamental ou em virtude de decisões judiciais, arbitrais ou administrativas, a decisão deverá ser comunicada previamente ao Diretor de Compliance e Risco, para que este conduza as discussões no âmbito do Comitê de Compliance e Risco, para a deliberação da maneira mais adequada de proceder com a revelação.

DEFINIÇÕES

De acordo com a política de SSI da DG, considera-se informação privilegiada qualquer informação relevante a respeito de qualquer companhia, que não tenha sido divulgada publicamente e que seja 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).

Exemplos de informações privilegiadas são:

I. Informações verbais ou documentadas a respeito de resultados operacionais de empresas;

II. Alterações societárias (fusões, cisões e incorporações);

III. Informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO); e

IV. Qualquer outro fato que seja objeto de um acordo de confidencialidade firmado por uma empresa com a Gestora ou com terceiros.

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, DICAS E FRONT-RUNNING

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 ou de terceiros.

Dica é a transmissão, a qualquer terceiro, estranho às atividades da DG, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running significa a prática que envolve aproveitar alguma informação privilegiada para realizar ou concluir uma operação antes de outros.

O disposto nos itens de Informação Privilegiada, Insider Trading, Dicas e Front-running deve ser analisado não só durante a vigência de seu relacionamento profissional com a DG, mas também após o seu término. Os colaboradores deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Caso os colaborares tenham acesso, por qualquer meio, a informação privilegiada, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance e Risco, indicando, além disso, a fonte da informação privilegiada assim obtida.

Tal dever de comunicação também será aplicável nos casos em que a informação privilegiada seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo.

Os Colaboradores que, desta forma, acessem a informação privilegiada, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance e Risco anteriormente mencionada.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se

o Colaborador às penalidades descritas nesta política de SSI e na legislação aplicável, incluindo eventual demissão por justa causa.

PRINCÍPIOS GERAIS

Todas as informações produzidas e utilizadas internamente pelos Colaboradores devem ser consideradas como ativos que tem valor para a DG e se constituem em vantagem competitiva. A proteção dessas informações, através da adoção dos procedimentos delineados nesta política de SSI é responsabilidade e obrigação de todos os colaboradores, e uma prioridade para a DG.

Os Princípios Gerais de SSI valorizados pela DG são a ***Integridade***, a ***Disponibilidade*** e a ***Proteção***. Em primeiro lugar, é de suma importância que as informações produzidas e utilizadas internamente tenham veracidade, precisão e relevância, pois representam ferramentas para a tomada de decisões estratégicas de alocação de recurso, e que não sejam modificadas sem expressa autorização.

Além disso, as informações devem estar prontamente disponíveis quando solicitado ou necessário, somente para colaboradores devidamente autorizados e para uso estritamente profissional.

Por fim, as informações devem ser gerenciadas de forma apropriada para evitar a ocorrência de fraude, roubo, perda não intencional, falhas operacionais e outras ameaças e riscos.

Ademais, a utilização dos ativos e sistemas da DG, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional, para tanto a DG adota os seguintes procedimentos:

I. Os colaboradores que atuam em Mesa de Operações estão impedidos de utilizar telefone celular no ambiente de trabalho;

II. Os Colaboradores estão impedidos de utilizar sistemas de mensagens instantâneas alternativos aos sistemas corporativos e ao e-mail corporativo da DG;

III. Os sistemas corporativos e o e-mail corporativo são gravados e ficam registrados nos servidores, disponíveis para eventuais inspeções do Diretor de Compliance e Risco; e

IV. O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da DG;

O recebimento de e-mails muitas vezes não depende do próprio colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da DG, bem como avisar prontamente o Diretor de Compliance e Risco.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

OBJETIVOS

As responsabilidades e obrigações dos Colaboradores perante este Manual incluem as diretrizes:

I. Não discutir questões confidenciais de trabalho, presencialmente ou por telefone, em ambientes públicos;

II. Garantir responsabilidade sobre informações e uso de ferramentas durante o desenvolvimento de suas atividades a fim de manterem seguras as informações, de forma que as ferramentas sejam utilizadas apenas para as atividades que envolvam diretamente a DG;

III. Não conectar à rede de computadores da Gestora nenhuma ferramenta própria;

IV. Utilizar as ferramentas disponibilizadas pela DG exclusivamente para as atividades às quais estiver devidamente autorizado;

V. Não utilizar a conta de correio eletrônico fornecida pela DG para envio de mensagens particulares, principalmente aquelas com conteúdo não relacionado aos assuntos de sua atividade profissional;

VI. Não utilizar os acessos disponibilizados à Internet para navegação em sites não relacionados à sua atividade na DG;

VII. Não executar tentativas de violação ou acessos (lógicos ou físicos) a instalações, sistemas, equipamentos (servidores, microcomputadores) informações e documentos;

VIII. Não fornecer ou emprestar a terceiros as senhas que lhe forem confiadas;

IX. Não instalar softwares e/ou sistemas nos equipamentos cedidos pela Gestora sem autorização;

X. Não manter informações confidenciais impressas à vista em estações de trabalho, salas de reunião ou qualquer outro ambiente do escritório ou fora dele, e armazenar as informações de maneira adequada e protegida;

XI. Não transportar ou retirar informações da DG, seja através de correio eletrônico, transferência eletrônica de dados, arquivos ou qualquer tipo de ferramenta capaz de transportar documentos eletrônicos, registros, dados e informações;

XII. Compreender ameaças externas que podem afetar a segurança das informações, como vírus de computador, interceptação de mensagens eletrônicas e telefônicas, sequestro de informações e ferramentas de ***phishing*** utilizadas para cometer fraudes, e notificar o encarregado pela manutenção dos sistemas de Tecnologia da Informação;

XIII. Não abrir ou executar arquivos eletrônicos de origem desconhecida; e

XIV. Cumprir as leis e normas que regulamentam a propriedade intelectual no que se refere às informações de propriedade ou controladas pela DG.