Política de Confidencialidade

v.1.0.0 – abril/2021

Resumo

Estabelecer normas de utilização a serem adotadas por todos os funcionários, prestadores de serviços, colaboradores, fornecedores e/ou parceiros referente à Política de Confidencialidade, tendo como objetivo assegurar que a informação receba um nível adequado de proteção. Consideram-se as a proteções em seu nível físico, digital, ou através de implantação de restrições ou normas que impeçam o acesso às informações privilegiadas por pessoas não autorizadas.

invexa capital

Tabela de Versões:

Versão	Data	Descrição
1.0.0	Abril de 2011	Documento Original

Validade: Indeterminado, com prazo de atualização não superior a 24 meses desde a última versão.

Área Responsável: Compliance

Aplicação: Invexa Capital

Responsável:

Assinatura Recuperável

X

Maria Carolina Damm
Compliance
Assinado por: 3a34bb60-027d-401a-87c3-99c097b1379a

Revisão / Aprovação:

Assinatura Recuperável

X

Marcelo Weber
Diretor Adm. Riscos e Compliance
Assinado por: 3a34bb60-027d-401a-87c3-99c097b1379a

Conteúdo do Documento

Esse documento mostra os procedimentos a serem realizados para o controle das políticas corporativas da empresa, e é composto pelos seguintes aspectos:

Áreas de Aplicação

Todos os sócios-gerentes, funcionários, estagiários, prestadores de serviço, fornecedores e/ou parceiros devem observar e atender a todas as normas que regulamentam as atividades da Instituição, que devem ser compulsoriamente observadas.

Norma de Controle de Informações Privilegiadas

A Informação alcançada em função da atividade profissional desempenhada na empresa não pode ser transmitida de forma alguma a terceiros não funcionários ou a funcionários não autorizados. Neste item, incluem-se, 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 dos fundos geridos pelo grupo, transações efetuadas e que ainda não foram publicadas.

Também é considerada informação sigilosa aquela oriunda de estudo interno efetuado pela instituição, mesmo que os ativos correspondentes não componham nosso portfólio.

Quanto à confidencialidade e tratamento da informação, o colaborador deve cumprir o estabelecido nos itens sobre informação privilegiada e *insider trading* e "dicas", conforme a seguir:

Confidencialidade

A confidencialidade da informação é a garantia de que a esta é acessível somente a pessoas autorizadas a terem acesso, condição essencial para preservar as informações, reduzindo as ameaças de ações não-autorizadas ou atos mal intencionados de terceiros. Nesta política são destacadas as normas que abrangem o acesso de informações e confidencialidade através das restrições sobre o uso de informações privilegiadas, e os meios utilizados para esse impedimento, através de proteção física, proteção digital, normas administrativas, classificação de informações.

Os critérios usados para a preservação das informações são feitos em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização. Os seus respectivos controles de proteção levam em consideração as necessidades de compartilhamento ou restrição de informações e os respectivos impactos nos negócios, associados com tais necessidades.

Informação Privilegiada

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

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 caracterizável como confidencial de uma empresa com a Empresa ou com terceiros.

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

O colaborador que tiver acesso a uma informação privilegiada deverá comunicar seu acesso ao seu superior, não podendo comunicá-la a outros membros da instituição, profissionais de mercado, amigos e parentes, tampouco usá-la, seja em seu próprio benefício ou de terceiros. Ainda que não exista certeza quanto ao caráter privilegiado da informação, deve-se rapidamente relatar o ocorrido à Empresa. As empresas envolvidas serão incluídas na lista de empresas com restrições para negociação, a qual será mantida sigilosamente pelo *Compliance*.

Insider Trading e "Dicas"

1. *Insider Trading* baseia-se na compra e venda de títulos ou valores mobiliários com o uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo a própria instituição e colaboradores).
2. "Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.
3. É proibida a prática dos casos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da empresa ou de terceiros.
4. O disposto nos itens de "Informação Privilegiada" e neste "*Insider Trading* e Dicas" deve ser analisado não só durante a vigência de seu relacionamento profissional com a Empresa, mas mesmo após o seu término.
5. Para impedir conflitos de interesse e impossibilitar condutas antiéticas de *insider* trading e front running, o diretor responsável pela atividade de administração de carteiras não assumirá outras funções ou atividades na Invexa Capital, nem em outras instituições.
6. A instituição está ciente da prática de *insider trading* e não praticará condições artificiais de demanda, oferta ou preço de valores mobiliários, manipulação de preços, operações fraudulentas ou práticas não equitativas, nem buscará artificialmente modificar preços de ativos, à alta ou à baixa, como forma de manipulação do mercado(*spoofing*).
7. Além de observar as vedações à negociação, as pessoas impedidas deverão manter sigilo sobre informações relativas às operações realizadas pela empresa para suas carteiras. Subordinados e terceiros participantes do processo de gestão também deverão guardar sigilo absoluto sobre informações do Processo de Seleção e Alocação de Valores Mobiliários;

Normas de Controles Administrativos

Os controles administrativos são importantes para a confidencialidade das informações, sendo executados através da interação entre pessoas com diferentes responsabilidades para que esses procedimentos possam ser executados de forma segura e controlada. Abaixo cita-se as principais formas de controle administrativo adotadas na empresa.

1. **Políticas** – O principal controle administrativo relacionado à confidencialidade é a **Política de Segurança da Informação e Cibernética** da organização. Entretanto, a criação de políticas adicionais pode ser utilizada para garantir a confidencialidade de informações, caso necessário.
2. **Revisão e Aprovação** – Qualquer ação individual que tenha uma maior relevância do ponto de vista de segurança e confidencialidade dever ser feita em mais de um passo, com responsabilidade de execução e revisão distintas, incluído autorização para concretização. Dessa forma, criamos mecanismos naturais de proteção e obrigamos as pessoas a se monitorarem, criando assim uma cadeia de proteção administrativa.
3. **Separação de tarefas** – Alguns procedimentos podem possuir problemas de confidencialidade se uma divisão não for feita entre seus passos, incluído a divisão de certas responsabilidades. Esse princípio recebe o nome de separação de tarefas. Assim a fragmentação e o acesso de parte das informações e processos facilita a confidencialidade desta.

Normas de Classificação das Informações

As classificações de informações procuram destacar os documentos de conteúdo confidencial, visando dar maior proteção e menor acessibilidade ao mesmo. Deve-se procurar a separação entre tipos de acordo com os benefícios obtidos por esta norma. Esquemas excessivamente complexos podem tornar o uso incômodo e ser inviáveis

economicamente ou impraticáveis. De forma geral, podem ser descritos alguns aspectos gerais da classificação de informação.

1. Os procedimentos para rotulação da informação precisam abranger tanto os ativos de informação no formato físico quanto no eletrônico. Itens que devem ser considerados incluem relatórios impressos, telas, mídias magnéticas (fitas, discos, CD), mensagens eletrônicas e transferências de arquivos.
2. A rotulação e o tratamento seguro da classificação da informação é um requisito-chave para os procedimentos de compartilhamento da informação. Os rótulos físicos são uma forma usual de rotulação. Entretanto, alguns ativos de informação, como documentos em forma eletrônica, não podem ser fisicamente rotulados, sendo necessário usar um rótulo eletrônico.
3. Devem-se incluir convenções para classificação inicial e reclassificação ao longo do tempo, de acordo com algumas políticas de controle de acesso predeterminadas. Isto também deve incluir os procedimentos para a cadeia de custódia e registros de qualquer evento de segurança relevante.
4. Caso venha-se a ter acordo com outras organizações, que incluam o compartilhamento de informações deve-se considerar procedimentos para identificar a classificação daquela informação e para interpretar os rótulos de classificação de outras organizações.

Classificação

Os arquivos, textos, planilhas, mídias, correspondências eletrônicas, relatórios e demais documentos da empresa serão classificados em dois níveis de segurança: confidenciais e de livre acesso.

1. **Documentos Confidenciais** – incluem-se nos documentos confidenciais quaisquer itens que apresentem saldo, movimentação financeira, histórico de transações, quotas, etc. que explicitem direta ou indiretamente os clientes da empresa. Incluem-se nesta categoria todos os documentos que contenham informações sobre a empresa, tais como fluxo de caixa, pagamentos, contratos jurídicos e demais itens que sejam de interesse estratégico da empresa.
2. **Documentos de Livre Acesso** – são todos os documentos que não fazem parte da denominação anterior, que tenham alguma relação com a atividade da empresa.

Processo

1. **Reclassificação -** cada novo documento criado deverá ter uma classificação inicial, com revisão ao longo do tempo. Para documentos confidenciais o prazo máximo de 5 (cinco) anos, e para documentos não confidenciais têm o prazo máximo estabelecido em 1 (um) ano.
2. **Armazenagem -** Os arquivos deverão ser armazenados no servidor, sendo que os arquivos confidenciais devem possuir acesso restrito. Os acessos aos arquivos livres dependerão da atividade e função exercida por cada colaborador na empresa.
3. **Transmissão** - Os arquivos deverão ser transmitidos de forma a evitar as possibilidades de fraudes e ações de pessoas mal intencionadas.
4. **Custódia** - Cada arquivo ou documento terá um responsável pela sua custódia, sendo este preferencialmente o proprietário da informação, que é a pessoa responsável pela área na qual a informação é utilizada. Quaisquer violações de confidencialidade serão atribuídas a essa pessoa, cabendo as providências estabelecidas, de acordo com a severidade da violação

Tipo de Documentos

Abaixo listamos as principais medidas a serem tomadas em relação aos tipos de documentos:

1. **Arquivos eletrônicos** – podem ter a classificação sendo mostrada dentro de seu conteúdo. Caso não seja possível, recomenda-se o armazenamento das informações nas propriedades dos arquivos que são extensíveis permitindo que a organização as personalize de acordo com sua necessidade. Deverão ser evitadas adicionais aos nomes dos arquivos o seu nível de segurança para potencializar as ações mal intencionadas.

2. **Correspondência Eletrônica** - E-mails que contenham informações dos negócios da instituição, classificados em nível de segurança confidencial, devem ser enviados apenas aos proprietários dos negócios, ou a destinatários autorizados a receberem estas informações. Os proprietários da informação deverão sempre ser copiados em e-mails de natureza confidencial, independentemente de estarem relacionados ao assunto em questão. Além disso, esses e-mails devem seguir todas as determinações dos controles internos e da legislação vigentes referentes ao sigilo de informações.
3. **Sistema e aplicativos** - Devem ser do tipo metadados para que os níveis de classificação possam ser armazenados junto com as informações. Todos os sistemas terceirizados passarão por avaliação que determinará a sua aderência às políticas de confidencialidade e segurança, de acordo com os controles por classificação.
4. **Documentos Físicos e Mídia** - Dever ser rotuladas visualmente com etiquetas como os documentos impressos, de acordo com os parâmetros supracitados, que incluem: (níveis de classificação, controles por classificação, duração, reclassificação, papéis e mudanças, referência aos procedimentos e instruções)

Responsabilidades

A **Política de Confidencialidade** só é efetiva se for claramente comunicada às pessoas de uma organização, e uma das principais formas de implantar e materializar as regras de confidencialidade é através de treinamento aos colaboradores. Neste caso, serão designados programas, levando em conta que diferentes pessoas que desempenham papéis diferentes e possuem responsabilidades distintas no processo organizacional. O principal objetivo é fazer separação clara entre proprietários e usuários das informações.

1. **Proprietários da Informação** - Entende-se como proprietário da informação a pessoa responsável pela informação em vigor, que, a priori, são os responsáveis pela área na qual a informação é utilizada. Deve-se incluir a conscientização sobre a responsabilidade no manejo das informações, inclusive monitorando e acompanhando o uso das informações pelos demais colaboradores. Será de responsabilidade do proprietário da informação definir a classificação de um ativo, analisando-o criticamente a intervalos regulares, e assegurar que ele está atualizado e no nível apropriado.
2. **Usuários da Informação** - Os demais colaboradores ou usuários da informação são responsáveis pelo zelo e bom uso das informações, devendo participar e seguir as regras descritas nesta política.

Por fim, os recursos e informações disponibilizados aos sócios-gerentes, funcionários, estagiários, fornecedores, demais colaboradores ou parceiros devem ser utilizados somente para os propósitos e finalidades aprovados pela instituição, de acordo com sua área de atuação.

Violação e Adesão

A violação ou não aderência aos procedimentos e normas constantes nesta **Política de Confidencialidade** pelos colaboradores podem ocasionar ações disciplinares e, em alguns casos, até a demissão de um funcionário ou o cancelamento de um contrato de serviço. No caso de tratamento aos colaboradores, primeiramente será dada uma notificação verbal. Em caso de reincidência na infração, será dada uma notificação por escrito. Por fim, em caso de nova reincidência, o colaborador será desligado da empresa.

A adesão à **Política de Confidencialidade** deve ser assinada em um **Termo de Adesão**, no qual o colaborador declara estar ciente das normas constantes na mesma. Esse termo detalhará todas as outras políticas da instituição, devendo ser assinado por todos os colaboradores da empresa. No caso de implementação ou modificação de qualquer política, bem como a instituição de novas políticas, novo termo deverá ser assinado pelos colaboradores da empresa, independente da prévia assinatura.

O responsável pela empresa em relação ao cumprimento da **Política de Confidencialidade** e também em relação aos órgãos regulares, clientes e demais agentes externos será um sócio-gerente previamente designado. Esse

responderá por todos os questionamentos, adequações, auditorias, monitoramento e bom uso e cumprimento desta política pela empresa.

Os cumprimentos desses quesitos e as sanções cabíveis à empresa estão discriminados no **Manual de Controles Internos**. Esse dispõe sobre os mecanismos de cumprimento, monitoramento da conformidade das normas e demais políticas da empresa além da adoção de medidas apropriadas em caso de infrações cometidas. Nessa política também constam os termos de adesão que devem ser assinados por sócios-gerentes e demais colaboradores da organização.