**Regras, procedimentos e descrição dos controles internos**
**Elaborados para o cumprimento da Resolução CVM Nº 21/2021 (antiga ICVM 558/2015)**

## Introdução

A abrdn Brasil Investimentos Ltda ("abrdn Brasil") descreve neste documento, em linhas gerais, quais são suas regras e procedimentos de controles internos, adotados para fins do cumprimento das exigências impostas pela Resolução CVM Nº 21/2021, bem como qual e como é a atuação da área de Risco e Compliance. Adicionalmente, este documento também contém algumas políticas que são mencionadas na Resolução CVM Nº21/2021.

## A abrdn Brasil

A abrdn Brasil está autorizada pela CVM, conforme Ato Declaratório nº 11.766 a atuar como administradora de carteira de valores mobiliários. Deste modo, na qualidade de gestora de recursos de terceiros a abrdn Brasil tem o dever de agir com boa fé, transparência, diligência e nos melhores interesses dos clientes, desempenhando suas atividades de modo a evitar práticas que possam ferir a relação fiduciária mantida com seus clientes.

## Departamento de Risco e Compliance

O departamento de Risco e Compliance tem como objetivo principal garantir que as atividades da abrdn Brasil estejam em conformidade com as exigências regulatórias e os mandatos de seus clientes. Para atingir este objetivo a área de Risco e Compliance atua: disseminando a cultura e controles internos com o intuito de mitigar conflitos de interesse; verifica a aderência dos funcionários, temporários (estagiários) e diretores e da empresa às políticas e regulamentações internas e dos órgãos reguladores; e realiza monitoramentos a fim de detectar e prevenir a ocorrência de violações. Além disso, a área de Risco e Compliance tem como prática acompanhar a edição e avaliar o impacto de novas regulamentações, assim como das mudanças em regras já existentes, além de orientar e educar a todos, por meio de comunicados e treinamentos.

O departamento de Risco e Compliance nas Américasconta com 1 profissional no Brasil e aproximadamente 15 profissionais baseados nos escritórios de Boston, Filadélfia, Nova York e Toronto (primordialmente, a maioria dos membros do time está no escritório da Filadélfia).

Nesta estrutura o departamento de Risco e *Compliance* no Brasil possui reporte ao ao *Chief Risk Officer – Americas.* O modelo atual fornece a estrutura necessária para as interações contínuas e o suporte mútuo entre o departamento de Risco e *Compliance* no Brasil e o restante do departamento em outras regiões das Américas.

É importante ressaltar que todo o departamento de Risco e *Compliance*-Américas possui independência da área de Gestão de Fundos de Investimentos.

**Procedimentos de Compliance**

- **Treinamento de Compliance**

Anualmente, a área de Compliance conduz treinamento presencial com todos os funcionários, temporários (estagiários) e diretores, a fim de relembrá-los e orientá-los quanto às políticas e procedimentos da Empresa. Neste treinamento é enfatizado que a prática da cultura de *Compliance*, para que a empresa se mantenha em cumprimento com as exigências regulatórias, é de responsabilidade de todos no exercício de suas atividades.

Quando do início de novos funcionários, temporários (estagiários) e diretores, a área de *Compliance* também realiza treinamento presencial, apresentando uma visão geral sobre a empresa e as políticas e procedimentos aos quais estarão sujeitos.

Além dos treinamentos presenciais, realizados ao longo do ano, também é solicitado aos funcionários, temporários (estagiários) e diretores que realizem treinamentos *online*. Assim que algum treinamento é designado, uma notificação por email é enviada aos funcionários, temporários (estagiários) e diretores informando o tema central e a data limite para a conclusão do treinamento. Tais treinamentos são complementares e abordam diversos temas relacionados não só às práticas e políticas da abrdn, como também, aos valores e a cultura da Empresa. Dentre os temas abordados destacamos: Conflitos de interesse, Risco operacional, Como tratar os clientes de maneira justa, Segurança cibernética, Proteção de dados, , Fraude, Anticorrupção entre outros.

- **Reportes**

Novos funcionários, temporários (estagiários) e diretores devem:

- Declarar seus investimentos pessoais bem como os investimentos das pessoas relacionadas[1];
- Responder o questionário de conflitos de interesse; e

Trimestralmente, todos os funcionários, temporários (estagiários), diretores e pessoas relacionadas[1], devem reportar todas as transações realizadas, envolvendo investimentos sujeitos ao Código de Ética, bem como anexar os extratos que comprovem tais transações e as posições mantidas no final de cada trimestre.

As informações acima são reportadas em um sistema específico de *Compliance*.

[1] *Qualquer membro da família imediata que compartilha a mesma casa ou qualquer indivíduo sobre cujas operações o funcionário tem influência ou controle.

**Manual de Compliance**

A abrdn Brasil mantém um Manual de Compliance, que contém políticas, diretrizes e procedimentos praticados pela abrdn Brasil. O Manual trata de vários assuntos dentre os quais incluem, mas não se limitam aos seguintes:.

- Código de ética e Conduta contendo a Política de Investimentos Pessoais aplicável a todos os funcionários, temporários (estagiários) e diretores;
- Política de Rateio e Divisão de Ordens;
- Práticas de Negociação (*Best Execution*);
- Politicas que endereçam situações de Conflitos de Interesses tais como: Presentes e Entretenimento, Atividades Comerciais Externas, Contribuições Políticas, Doações de Caridade;
- Gerenciamento de riscos;
- Contingência, Continuidade de Negócios e Recuperação de Desastres;
- Confidencialidade, Privacidade e Segurança da Informação;
- Exercício do direito de voto em assembleias gerais;
- Materiais de Marketing;
- Informações Privilegiadas;
- Prevenção à Lavagem de Dinheiro.

Estes assuntos constituem a base de um Programa de Compliance de um gestor de recursos, conforme os dispositivos da Resolução CVM Nº21/2021 bem como as exigências de outras regras da CVM também aplicáveis aos gestores de recursos.

**Testes de Compliance**

Abaixo segue breve descrição sobre o escopo de atuação de cada time responsável por desempenhar testes de conformidade.

Responsável pelo desenvolvimento e execução do programa de testes da região das Américas desenvolvidos para assegurar a aderência às regulamentações e políticas locais, bem como as políticas do Grupo. A equipe também é responsável pela supervisão periódica em relação a assegurar a aderência que está sendo realizada por outras equipes (ou seja, o time de *Investment Control*; *Distribution Compliance*) para a região.

**Retenção de Registros**

A abrdn Brasil manterá as informações e os documentos necessários ao exercício de sua atividade, conforme regulamentação aplicável, pelo prazo mínimo de 5 anos.

## PREVENÇÃO AO USO DE INFORMAÇÕES PRIVILEGIADAS

No curso de suas atividades de gestora de recursos de terceiros, a abrdn, seus funcionários, temporários (Ex: estagiários) e diretores ("Pessoas Cobertas") terão posse de informações confidenciais relacionadas a clientes e suas operações com valores mobiliários, bem como poderão ter, periodicamente, posse de informações "relevantes" e "não públicas a respeito de uma determinada empresa ou do mercado de negociação de seus valores mobiliários. Sendo assim, dependendo das circunstâncias, a abrdn e qualquer Pessoa Coberta envolvida poderão estar expostas a possível responsabilidade por uso de informações privilegiadas caso a abrdn ou qualquer Pessoa Coberta oriente clientes ou realize operações com valores mobiliários os quais a Empresa possui informações relevantes e não públicas.

Portanto, as Pessoas Cobertas da abrdn têm a responsabilidade ética e legal de manter a confidencialidade dos clientes da Empresa e proteger as informações confidenciais e exclusivas desenvolvidas ou confiadas à Empresa como ativos valiosos. Além disso, as violações das leis contra uso de informações privilegiadas por Pessoas Cobertas da abrdm podem expor a abrdn e qualquer Pessoa Coberta envolvida a responsabilidade criminal e civil grave.

É importante mencionar que embora a abrdn respeite o direito de suas Pessoas Cobertas se envolverem em atividades de investimento, é importante que essas práticas evitem qualquer aparência de impropriedade, bem como permaneçam em plena conformidade com a lei e os mais altos padrões éticos. Assim, as Pessoas Cobertas devem exercer bom senso ao se envolverem em operações com valores mobiliários, respeitando sempre o Código de Ética e a Política de Investimentos Pessoais da abrdn.

## PROTEÇÃO DE OUTRAS INFORMAÇÕES CONFIDENCIAIS

Informações relacionadas à atividades passadas, presentes ou futuras da Empresa ou de seus clientes, que não tenham sido divulgadas publicamente, não deverão ser divulgadas ou compartilhadas com pessoa fora da Empresa ou internamente, exceto no caso de uma finalidade específica e/ou necessidade das áreas envolvidas da abrdn. Espera-se que Pessoas Cobertas usem seu próprio bom senso e julgamento em relação a informações de outras pessoas.

Além disso, informações relacionadas a assuntos médicos, financeiros, de trabalho, legais ou pessoais de outras Pessoas Cobertas, também são confidenciais e não podem ser divulgadas a qualquer pessoa, dentro ou fora da abrdn, sem o consentimento da Pessoa Coberta ou no caso de uma finalidade específica, sem a autorização do departamento de *Compliance.*

## PRIVACIDADE

A abrdn têm como objetivo proteger a privacidade de seus clientes atuais, ex-clientes e clientes potenciais na medida do possível. Deste modo, a abrdn mantém política de privacidade descrevendo o tipo de informações pessoais coletadas, a finalidade para a qual as informações são utilizadas, as circunstâncias nas quais as informações podem ser compartilhadas, e as medidas que são adotadas para proteger as informações e, consequentemente, a privacidade de clientes atuais, potenciais e ex- clientes.

### Para quem as informações pessoais são divulgadas

A abrdn não divulga informações pessoais para terceiros, exceto conforme descrito na Política de Privacidade, disponível no endereço eletrônico www.abrdn.com.br .

A divulgação de informações para terceiros poderá incluir o compartilhamento desses dados com terceiros, para fins do cumprimento de suas atividades, que prestem serviços à abrdn Estas empresas são obrigadas a garantir o uso de medidas de segurança adequadas e manter a confidencialidade das informações recebidas, bem como usar as informações pessoais apenas em relação ao fornecimento de seus serviços e somente para as finalidades determinadas pela abrdn.

Além disso, informações pessoais podem ser divulgadas para atender instruções ou de acordo com o consentimento expresso. Em circunstâncias específicas, informações pessoais poderão ser divulgadas para terceiros conforme permitido, ou de acordo com a regulamentação e as leis aplicáveis como por exemplo, em razão de processos judiciais ou semelhantes, para proteção contra fraudes, e para cooperar com a aplicação da lei ou autoridades regulatórias. Por fim, vale destacar que a abrdn não vende informações pessoais.

### Privacidade e a Internet

A abrdn tem o compromisso de garantir a segurança de suas informações pessoais. Para evitar o acesso e a divulgação não autorizados, proteger e garantir as informações pessoais, são aplicados procedimentos físicos, eletrônicos e administrativos adequados.

## SEGURANÇA DA INFORMAÇÃO

### Objetivos da Política

É parte da política da abrdn:

- Proteger as informações contra acesso não autorizado.
- Garantir a confidencialidade das informações.
- Disponibilizar as informações na medida em que seu conhecimento seja necessário.
- Manter a integridade das informações.
- Manter e testar os planos de Continuidade de Negócios apropriados.
- Garantir a existência de controles adequados de retenção e destruição de dados.
- Respeitar as exigências regulatórias e legais.

- Assegurar que quaisquer violações de segurança da informação, reais ou presumidas, sejam investigadas por pessoas qualificadas e comunicadas à alta diretoria.

Responsabilidade

Todos os funcionários da abrdn, independentemente do tipo do contrato de trabalho, são responsáveis por assegurar a conformidade com a Segurança da Informação e a Proteção de Dados.

Proteção de Dados Sigilosos

A abrdn assegura a Proteção de Dados Sigilosos e Sistemas de Computador por meio de diretrizes sobre:

1. Necessidade de Ter Conhecimento

A divulgação não autorizada de informações sigilosas representa uma séria ameaça para o Grupo. Segundo o conceito da Necessidade de Ter Conhecimento (*Need-to-Know*), as informações sigilosas devem ser fornecidas apenas para as pessoas que dependem delas para desempenhar suas funções.

2. Mesa Limpa e Tela Limpa

É essencial proteger as informações sigilosas contra divulgações inadequadas ou roubo. O ambiente do escritório é frequentado por fornecedores, equipes de limpeza e manutenção etc. Portanto, com o objetivo de proteger as informações sigilosas permanentemente, todos devem certificar -se de alguns cuidados, que incluem, mas não se limitam a :

- Manter os documentos sigilosos trancados em gavetas ou arquivos quando eles não estiverem sendo usados;
- Proteger o seu PC/laptop etc. antes de se afastar, usando o comando CTRL+ALT+DEL para bloquear a tela;
- Descartar materiais sigilosos no recipiente de Resíduo Confidencial/triturador;
- Retirar imediatamente as impressões ou cópias contendo informações sigilosas de impressoras/faxes/fotocopiadoras.
- Não deixar papéis nas salas de reuniões.

3. Uso de Equipamentos de fax

4. Uso de Telefones

5. Proteção de Documentos e Arquivos de Dados Sigilosos

   Documentos e arquivos de dados devem ser salvos em um local apropriado de uma unidade de disco da rede. Os arquivos salvos nesses locais serão copiados automaticamente (*backup*), com regularidade.

6. Uso de SMS/Mensagens de Texto
   SMSs/mensagens de texto **não** devem ser usadas para realizar transações/negociações comerciais.

7. Descarte de Dados/Papéis

8. Proteção de Sistemas de Computador

- Senhas
  As pessoas autorizadas a acessar os sistemas de computador da abrdn recebem um nome de usuário e uma senha específicos. O nome de usuário e a senha são confidenciais, não devendo ser divulgados ou anotados, exceto se esses registros puderem ser armazenados de forma segura. Cada funcionário é responsável pelas atividades realizadas com o seu nome de usuário e senha.

O compartilhamento de senhas é proibido, podendo resultar em ações disciplinares.

- Uso do E-mail
- Uso da Internet
- Uso de Sistemas
- Conexão de Dispositivos Externos ao Computador, Laptop ou iPad
  A abrdn tem como política bloquear as portas USB, sendo este um procedimento padrão para todos os PCs (computadores) e laptops. Apenas as chaves USB ou discos rígidos emitidos e autorizados por TI poderão ser usados na Rede da abrdn. Dispositivos não autorizados serão bloqueados automaticamente.
  Os dados copiados de/para portas USB de PCs/laptops serão registrados e monitorados.

9. Trabalho fora do escritório:

- Acesso remoto
- BYOD – *Bring Your Own Device* ("traga seu próprio dispositivo")
  A abrdn permite o uso de dispositivos próprios dos funcionários desde que sejam respeitadas algumas regras internas como por exemplo: em caso de perda ou roubo do dispositivo, a área de TI deverá ser informada imediatamente, para que o dispositivo possa ser varrido remotamente, e os dados da abrdn possam ser protegidos.

10. Segurança Física
    Trata do acesso de visitantes e funcionários às dependências da Empresa, cartões de identificação e retirada de propriedade da Empresa..

11. Gestão e Retenção de Registros

A abrdn possui responsabilidade legal e regulatória de manter os registros durante um período mínimo de tempo.
Os registros deverão refletir corretamente o que foi comunicado ou decidido, ou as ações tomadas. Os registros também deverão apoiar as necessidades do negócio, ou serem úteis para a área à qual eles se referem.

12. Incidentes de Segurança

- Comunicação de Incidentes
  Os casos de suspeita de violação real ou potencial da segurança da informação, ou preocupações sobre qualquer aspecto relativo à segurança de dados, devem ser reportados ao departamento de Compliance local ou ao departamento de Segurança da Informação. Tais casos também podem ser comunicados via canal confidencial que está disponível para os funcionários.

13. Monitoramento e Privacidade

Embora seja desejável permitir um nível razoável de privacidade aos usuários, eles deverão estar cientes que os dados criados nos sistemas da abrdn são de propriedade da Empresa. E por esta razão a abrdn reserva-se o direito de monitorar e registrar qualquer uso dos sistemas de informação da Empresa.

**Atualizado em: Agosto de 2022**