Schroders

Política de Regras, Procedimentos e Controles Internos

Schroders Brasil

Junho 2023

Schroders

Sumário

1. Objetivo e Abrangência

1.1 Objetivo

A presente Política de Regras, Procedimentos e Controles Internos ("Política") foi elaborada pela Schroder Investment Management Brasil Ltda. ("Schroder Brasil"), com o objetivo de (i) dispor sobre os padrões técnicos, operacionais e éticos que regem o funcionamento e o desenvolvimento das atividades da Schroder Brasil; (ii) estabelecer regras, procedimentos e controles internos para atendimento às normas e regulamentações aplicáveis à Schroder Brasil; bem como (iii) dispor sobre demais princípios relativos às empresas controladoras, controladas e coligadas do grupo Schroders ("Grupo").

A presente Política abrange:

- Regras de compliance da Schroder Brasil;
- Regras de confidencialidade que regulam o sigilo e confidencialidade de informações;
- Política de Segurança da Informação;
- Regras de negociação pessoal, que regulam os termos e condições aplicáveis à negociação de títulos e valores mobiliários por parte dos Colaboradores (conforme abaixo definido);
- Normas específicas para tratamento de situações que possam configurar conflitos de interesses.

Esta Política observa os parâmetros legais estabelecidos para o exercício da atividade de gestão de recursos, notadamente as regras, procedimentos e controles internos dispostos na Resolução CVM nº 21, de 25 de fevereiro de 2021 ("Resolução. CVM nº 21") conforme alterada, bem como no Código de Administração de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA").

1.2 Abrangência

Esta Política é aplicável a todos os diretores, colaboradores, empregados, trainees, estagiários, fornecedores e terceiros contratados para a prestação de serviços nas dependências da Schroder Brasil ou que desenvolvam, direta ou indiretamente, atividades relacionadas àquelas conduzidas pela Schroder Brasil ("Colaboradores").

É de responsabilidade de todos os Colaboradores conhecer e cumprir todas as obrigações legais e regulatórias que são importantes para as suas atividades, bem como observar os mais altos padrões de conduta profissional ao conduzir seus negócios.

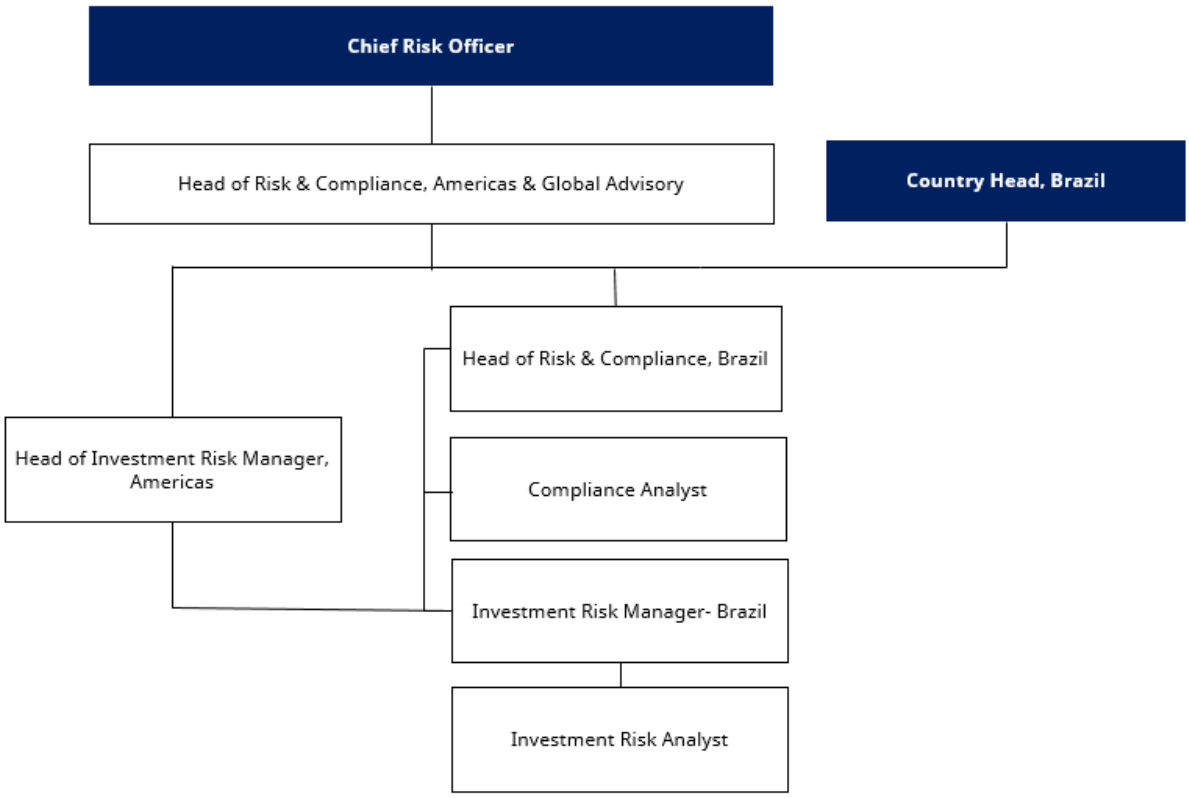
2. Área de Risco e Compliance

2.1 Área de Risco e Compliance da Schroder Brasil

A área de Risco e Compliance da Schroder Brasil ("Área de Risco e Compliance") atua com independência e autoridade e dispõe de profissionais experientes e capacitados para o desempenho de suas funçõesNa estrutura organizacional do Grupo, a área de Risco e Compliance se reporta ao chefe de Risco e Compliance das Américas e atua em conjunto com as áreas de Compliance da América Latina, dos Estados Unidos e do Reino Unido na elaboração, planejamento, execução e controles das políticas do Grupo e cumprimento das legislações aplicáveis.

A Schroder Brasil conta com 4 (quatro) profissionais dedicados às atividades de Risco e Compliance, todos

com qualificação técnica e experiencia condizentes com o exercício das respectivas funções na área de Risco e Compliance, conforme se verifica no organograma a seguir:



O Head of Risk & Compliance ("Diretor de Compliance") atua com autoridade e independência e é o responsável pela fiscalização e garantia de que serão tomadas todas as providências necessárias para ajustar continuamente a exposição aos riscos das carteiras de investimento sob gestão da Schroder Brasil, utilizando como base os limites previstos nos documentos dos fundos de investimento geridos pela Schroder Brasil. É vedado ao Head of Risk & Compliance atuar em funções relacionadas à administração de carteiras de valores mobiliários, à intermediação e à distribuição de cotas de fundos de investimentos, ou em qualquer atividade que limite a sua independência, na Schroder Brasil ou em instituição terceira.

Já os demais integrantes da Área de Risco e Compliance, ou seja, Compliance Analyst, Investment Risk Manager e Investment Risk Analyst, são os responsáveis por auxiliar o Diretor de Compliance no desempenho de suas funções, atuando de maneira independente, estando em contato constante com o *Business* e outras áreas da Schroder Brasil a fim de identificar, avaliar, monitorar, mitigar e relatar os potenciais e efetivos riscos regulatórios e de conduta que cerceiam a atividade da Schroder Brasil e seus Colaboradores. Importante esclarecer que os documentos e informações referentes ao compliance da Schroders Brasil são arquivados em pasta protegida, cujo acesso é permitido apenas ao Country Head e aos colaboradores da àrea de compliance.

São exemplos de condutas adotadas pela Área de Risco e Compliance:

- Promover altos padrões de conformidade e conduta ética.
- Assessorar o *business* e a alta administração sobre as leis, regras e padrões atuais e futuros, supervisionar as mudanças regulatórias e participar e relatar nas reuniões do Conselho, Comitê e outros grupos de trabalho.
- Treinar a equipe sobre as regras e requisitos regulatórios aplicáveis, estabelecendo políticas e procedimentos de conformidade importantes, prestando consultoria nas consultas de conformidade ad-hoc do dia a dia e auxiliando o *business* no desenvolvimento de sistemas e controles.
- Detectar e prevenir crimes financeiros (lavagem de dinheiro, suborno e corrupção, financiamento do terrorismo, evasão fiscal, violação de sanções económicas e abuso de mercado).
- Identificar, avaliar e prevenir e/ou mitigar riscos regulatórios e de conduta associados às atividades de negócios do Grupo (por exemplo, produtos, processos de negócios e operacionais, relações cliente/terceiros), incluindo a realização de avaliações de risco de conformidade.
- Fornecer supervisão independente das atividades de negócios em uma abordagem baseada em risco por meio de garantia de conformidade (vigilância, monitoramento e testes). Relatar todas as descobertas materiais à alta administração e aos Conselhos/Comitês da entidade legal, conforme apropriado.
- Relatar todas as descobertas materiais à alta administração e aos Comitês da entidade legal, conforme aplicável.
- Manter relacionamentos positivos com reguladores localmente e atuar como a primeira linha de contato com reguladores e, quando necessário, relatar e supervisionar a resolução de violações e outras questões regulatórias significativas.

2.2 Mecanismos de Compliance

O acompanhamento do cumprimento das regras de compliance é realizado de forma extensiva e contínua. A Schroder Brasil adota métodos preventivos de compliance, como a adesão de todos os Colaboradores da Schroder Brasil às suas políticas, regras, procedimentos e manuais aplicáveis e relacionados aos serviços prestados por cada Colaborador e conta com sistemas do Grupo para controle e monitoramento dessas políticas.

Todos os Colaboradores deverão ser regularmente avaliados e suas atividades devem ser monitoradas, a fim de identificar quaisquer situações atípicas ou suspeitas no desempenho de suas atividades profissionais, bem como qualquer descumprimento das políticas da Schroder Brasil e do Grupo.

Ademais, por meio do *Annual Attestation,* todos os Colaboradores devem confirmar anualmente que têm conhecimento das Políticas do Grupo Schroders e das Políticas locais.

Adicionalmente, a Schroders Brasil realiza anualmente, ou em tempo menor se necessário, atividades de monitoramento apropriadas para o *business* e avaliações de risco. O objetivo desta avaliação de risco é confirmar que os riscos de compliance foram identificados e avaliados adequadamente, para formar uma base sólida para determinar as prioridades de monitoramento de conformidade.

A avaliação de risco ajuda a área de Compliance a formar uma opinião sobre o risco apresentado pelos processos de negócios e a eficácia dos controles, além de identificar áreas de maior risco que devem ser avaliadas com mais atenção e frequência.

Todos os processos de monitoramento e avaliação de riscos serão documentados e compartilhados com a Diretoria da Schroder Brasil

2.3 Auditoria Interna

Além do monitoramento realizado pela Àrea de Risco e Compliance, o Grupo realiza procedimentos de auditoria interna. O relatório do resultado da auditoria interna é circulado e reportado para a administração do Grupo, dentre eles o Chief Executive Officer e o Chief Financial Officer globais do Grupo Schroders, e eventuais requerimentos da auditoria são registrados no sistema de risco operacional para acompanhamento e resolução. Este documento é de uso interno do Grupo Schroder.

2.4 Política de Treinamento dos Colaboradores

Todos os Colaboradores, incluindo aqueles recém-contratados, deverão participar de programas de treinamento, atualização e conscientização, os quais ocorrem anualmente, das regras e procedimentos de conduta adotados pela Schroder Brasil e pelo Grupo (“Programas de Treinamento”).

Os Programas de Treinamento deverão ter conteúdos programáticos específicos (incluindo carga horária e temas abordados) definidos pelo representante da área de Compliance da Schroder Brasil e do Grupo Schroder e poderão ser alterados/adaptados sempre que necessário.

Cada Programa de Treinamento deverá, necessariamente, abordar todos os dispositivos das respectivas políticas da Schroder Brasil e do Grupo abordadas em tal programa.

Os Programas de Treinamento deverão ser pautados pela clareza, acessibilidade e simplicidade na veiculação das informações.

Os Programas de Treinamento serão realizados online e será mantido registro eletrônico de controle de participação dos Colaboradores. Quando necessário, os Programas de Treinamento poderão ser realizados de maneira presencial, desde que seja mantido o registro de controle dos participantes (lista de presença), bem como seja registrado o contepudo ministrado no treinamento.

3. Política de Confidencialidade e Segurança da Informação

3.1 Regras gerais aplicáveis sobre Confidencialidade

A Schroder Brasil adota regras para assegurar o controle de Informações Confidenciais a que tenham acesso seus Colaboradores. Os Colaboradores da Schroder Brasil, no desempenho de suas funções, poderão vir a ter acesso a diversas informações classficiadas como confidenciais.

Para fins desta Política, “Informações Confidenciais” significa qualquer informação em qualquer forma ou meio, seja escrita, entregue eletronicamente, tangível ou intangível, cuja natureza confidencial a Schroder Brasil e o Grupo desejam manter, incluindo (sem limitação): i) todas informações comerciais, financeiras, comercialmente sensíveis, operacionais, regulatórias, tecnológicas, estratégicas ou outras informações, processos ou dados de qualquer tipo em (sem limitação); ii) software, códigos-fonte, fluxos de processo, metodologias de desenvolvimento, descrições de banco de dados, processos, propriedade intelectual e descrições de funcionalidade relacionadas à gestão de ativos e sistemas similares desenvolvidos por ou em

nome da Schroder Brasil ou do Grupo; iii) todo o know-how, documentação e outras informações relacionadas à gestão de ativos e sistemas similares desenvolvidos por ou em nome da Schroder Brasil ou do Grupo, e quaisquer trabalhos e assuntos relacionados ou similares; iv) relações ou correspondência com clientes, parceiros de negócios, reguladores ou outros membros da Schroder Brasil e do Grupo; e v) demais informações de propriedade da Schroder Brasil e do Grupo.

Os Colaboradores deverão observar a natureza confidencial dos assuntos relacionados a Schroder Brasil e seus clientes, obtidas no desenvolvimento de suas atividades. Informações Confidenciais devem ser transmitidas apenas dentro do Grupo e somente para aqueles que devem tomar conhecimento daquela informação (*need-to- know*) ou, senão, autorizadas pelo respectivo gerente, em conformidade com esta Política,devendo o Colaborador preservar sua confidencialidade, inclusive, após o rompimento de seu vínculo com a Schroder Brasil.

Os Colaboradores também deverão evitar fazer divulgação desnecessária de qualquer informação interna relacionada ao Grupo ou suas relações comerciais, devendo utilizar tais informações de forma prudente e adequada, sempre de acordo com os interesses do Grupo e de seus clientes.

Informações relativas às carteiras de todo e qualquer produto gerido pela Schroder Brasil são consideradas confidenciais e não devem ser reveladas a terceiros, salvo se aprovado expressamete pelo Diretor de Compliance, e na ocorrência de requerimento legal ou regulatório de autoridade competente.

A reprodução ou transferência, sob qualquer forma, de conteúdo sigiloso será considerada falta grave quando não se pautar nas estritas funções delegadas aos Colaboradores e caso ocorra em violação ao disposto na presente Política.

O acesso eletrônico à Informações Confidenciais e a informações internas é controlado a partir do usuário atribuído a cada Colaborador de acordo com suas atribuições profissionais.

Os sistemas e aplicativos de rede da Schroders são protegidos por senhas e permitem o controle dos acessos. A Schroders restringe e controla o acesso de pessoas às dependências da sua sede e aos documentos e informações de sua propriedade, armazenados física ou virtualmente, por meio de login e senhas de segurança apropriada individuais para cada Colaborador. O Colaborador deve manter em local seguro suas senhas e não divulgar a terceiros em nenhuma hipótese.

Com o objetivo de proteger as Informações Confidenciais e internas, os Colaboradores devem aderir às normas, diretrzes e políticas internas do Grupo Schroders que tratem sobre o tema.

A Área de Risco e Compliance irá apurar os casos de divulgação indevida de informação confidencial e o responsável por tal divulgação estará sujeito à penalidades descritas nesta Política, sem prejuízo de sanções na esfera cível e criminal.

3.2 Política de Segurança da Informação

A Política de Segurança da Informação tem por finalidade definir os requisitos, processos e controles no que tange à proteção dos dados da Schroder Brasil, de forma a garantir a confidencialidade e integridade de tais dados. A Schroder Brasil segue a Política do Grupo, a qual, entre outros, define detalhadamente todas as regras a serem seguidas pelas empresas do Grupo, medidas de prevenção e risco, mapeamento de vulnerabilidades, controle de acessos.

A estrutura de Segurança da Informação é projetada para estabelecer controles apropriados para identificar,

proteger, detectar, responder e se recuperar contra as ameaças que estão em constante evolução.

Os cinco objetivos a seguir fornecem a base da nossa estrutura de Segurança da Informação:

1. Governança: A Schroders e sua alta administração supervisionam e compreendem a importância do risco de segurança cibernética para as operações.
2. Identificação de Risco: Avaliar continuamente as principais ameaças cibernéticas que podem desafiar e impactar a Schroders
3. Proteção do sistema, ativos, dados e capacidades: Salvaguardas apropriadas são implementadas pela Schroders para garantir a prestação de serviços comerciais.
4. Detecção de eventos de segurança da informação: Atividades apropriadas são implementadas para identificar a ocorrência de eventos que afetam a Schroders.
5. Responder e recuperar um incidente de segurança da informação: As práticas são estabelecidas e implementadas para garantir que atividades apropriadas sejam realizadas quando um evento é detectado e está afetando a Schroders.

3.2.1. Principios e Responsabilidades

A segurança da informação está presente em toda a organização e é uma parte inerente da tecnologia e um componente chave de nossos processos operacionais.

A Política de Segurança da Informação identifica o risco ao:

- Garantir que a empresa entenda e avalie a ameaça de segurança cibernética às operações.

- Avaliar dados, pessoal, dispositivos, sistemas e instalações com sua importância relativa para os objetivos de negócios e a estratégia de risco da empresa por meio de:

  - Confidencialidade, alguém vendo ou acessando os dados que não deveria.
  - Integridade, alguém alterando os dados que não deveria ou alterando os dados incorretamente
  - Disponibilidade, o serviço não está disponível.

- Estabelecer processos operacionais para avaliar e gerenciar os riscos da cadeia de suprimentos em termos de segurança cibernética. Terceiros avaliados como críticos ou que hospedam informações altamente confidenciais estão sujeitos a revisões anuais de segurança da informação.

- Investigar regularmente a inteligência de ameaças, bem como contratar especialistas para testar nossas defesas e abordagem em relação à segurança cibernética.

A Segurança da Informação é protegida por processos operacionais para mitigar o risco de acesso não autorizado a ativos físicos e lógicos. Os funcionários devem ser autorizados antes de receberem privilégios de acesso, bem como são informados sobre a confidencialidade das informações com as quais lidam, a fim de protegê-las contra divulgação não autorizada, corrupção ou perda.

A Schroders fornece treinamento anual de conscientização sobre segurança cibernética com o intuito de garantir que os funcionários sejam adequadamente treinados para desempenhar suas funções e responsabilidades relacionadas à segurança da informação. Os tópicos abordados podem incluir: Phishing, Malware, Ransomware, Mídia Social, Navegação na Web, Viagens e Trabalho Remoto, Manuseio de Dados,

Comportamento de Senha e Autenticação Multifator.

Ademais, treinamento de segurança cibernéticaé fornecido para novos funcionários dentro de oito semanas de trabalho.

- Operar soluções técnicas e processuais de segurança para garantir a segurança e resiliência de sistemas e ativos:

  - Os logs de auditoria de acesso são revisados e atividades suspeitas são investigadas e relatadas.
  - A mídia removível está protegida.
  - O princípio da menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais.
  - O acesso às aplicações e sistemas avaliados como críticos são recertificados anualmente.
  - As redes de comunicação e controle são protegidas.
  - Os sistemas operam em estados funcionais predefinidos para obter disponibilidade (por exemplo, sob pressão, sob ataque, durante a recuperação, operações normais)

A Segurança da Informação detecta potenciais eventos adversos por meio da(o):

- Revisão de atividades anômalas em tempo hábil e avaliação do impacto potencial dos eventos.

- Monitoramento de sistemas e ativos de informação para identificar eventos de cibersegurança e verificar a eficácia das medidas de proteção.

- Manter e testar processos e procedimentos para garantir a conscientização oportuna e adequada de eventos anômalos.

3.2.2. Testes Periódicos de Segurança

A Schroder Brasil realiza análise e testes periódicos que objetivam a identificação de eventuais vulnerabilidades técnicas e processuais que porventura venham a apresentar risco às informações e seus sistemas críticos de negócios. Tais testes periódicos de segurança são confidenciais de forma a garantir a confiabilidade de seus resultados e a sua eficiência.

A estratégia de segurança de informação da Schroder Brasil envolve a constante modificação dos sistemas internos e externos adotados de forma a garantir a segurança de seus clientes, Colaboradores e acionistas de ataques externos. Para tanto, a Schroder Brasil conta com uma equipe de Segurança daInformação responsável por monitorar e mitigar eventuais riscos relacionados à segurança da informação.

Toda nova tecnologia ou novos processos, quando adotados, estão sujeitos à testes de implementação, bem como à testes periódicos de forma a verificar potenciais riscos e vulnerabilidades dos mesmos.

Além dos pontos descritos acima, a Schroder Brasil contrata pessoal terceirizado para testar a segurança de seus sistemas e demais tecnologias relacionadas à segurança da informação. Os sistemas informatizados que contem com acesso à internet, por exemplo, são testados anualmente de forma a verificar sua penetrabilidade.

Adicionalmente, o Diretor de Compliance da Schroders Brasil, em conjunto com a área de tecnologia, realizará verificações periódicas de segurança para os sistemas de informação, a fim de: (i) minimizar preventivamente eventuais riscos operacionais e de descumprimento do disposto no Código de Administração de Recursos de

Terceiros, na Resolução CVM n° 21/21 e nesta Política; e (ii) garantir que a estrutura tecnológica conte com proteção a tentativas de ataques cibernéticos.

3.3 Política de Privacidade e Proteção de Dados

Dados pessoais são informações referentes a um indivíduo, que permitem identificar especificamente tal indivíduo. Dados pessoais incluem, por exemplo, nomes, endereços, endereços de e-mail, entre outros dados cadastrais. A Schroder Brasil, no exercício de suas atividades, pode ter que coletar, armazenar, processar ou transferir determinados dados pessoais relativos aos indivíduos envolvidos nas operações que realiza.

A Schroder Brasil processa diferentes tipos de dados pessoais no desempenho de suas atividades. Os Colaboradores responsáveis por processar ou manipular dados pessoais deverão garantir que os seguintes requisitos sejam cumpridos:

- Os dados pessoais devem ser utilizados apenas para os fins que forem solicitados para o seu titular e conforme permitido por esta política de segurança da informação.
- Dados pessoais confidenciais não devem ser processados ou armazenados a menos que seja necessário (e desde que o titular dos dados forneça seu consentimento explícito).
- Os dados pessoais só devem ser armazenados durante o período necessário para cumprir o propósito do negócio e sua manutenção deve ser precisa e atualizada.
- Os dados pessoais devem ser armazenados e gerenciados de forma segura, em conformidade com a Política de Segurança da Informação, esta Política e demais normas similares do Grupo.
- O titular dos dados possui o direito de solicitar informações sobre quais dados pessoais estão sendo processados.
- Os Colaboradores deverão notificar os organismos reguladores de proteção de dados, conforme aplicável, sobre o tipo de atividades de processamento de dados realizadas, em conformidade com as leis aplicáveis para cada jurisdição.
- As áreas operacionais da Schroder Brasil deverão notificar o Representante de Proteção de Dados pertinente sobre mudanças no processamento de dados pessoais antes de realizarem qualquer alteração.
- Todos os sites do Grupo, aplicativos e sistemas de TI, incluindo sistemas terceirizados externos que coletam dados pessoais, devem respeitar as exigências da Política de Segurança da Informação e desta Política.
- Os Colaboradores devem estar cientes de que leis locais, regulamentações e diferenças culturais podem impor requisitos diferentes sobre dados pessoais daqueles previstos nesta Política. Leis e regulamentos locais, quando forem mais rigorosos, sempre deverão prevalecer e, na hipótese de dúvidas, o representante de proteção de dados local deverá ser contatado o quanto antes.
- A utilização ou acesso a dados pessoais sem autorização é considerado uma infração disciplinar grave, podendo constituir também uma ofensa criminal.
- Se, a despeito das medidas de segurança tomadas para proteger os dados pessoais adotadas, houver uma violação ou suspeita de quebra de segurança, as práticas definidas na Política de Eventos de

Riscos do Grupo deverão ser observadas de forma razoavelmente praticável.

- Quaisquer exceções a esta Política deverão ser relatadas e aprovadas através do processo de derrogação que, para fins de proteção de dados pessoas, deverá incluir uma consulta feita ao Responsável pela Proteção de Dados do Grupo ou, na impossibilidade deste, ao Coordenador de Proteção de Dados.

Para maiores informações sobre as regras relacionadas a proteção de dados, consulte nossa Política de Privacidade.

3.3.1. Papéis e Responsabilidades

Responsável pela Proteção de Dados do Grupo

O Responsável pela Proteção de Dados do Grupo tem como atribuição supervisionar a proteção de dados em todo o Grupo, incluindo as questões ou perguntas que não podem ser tratadas de maneira satisfatória pelos Representantes de Proteção de Dados.

Coordenador de Proteção de Dados do Grupo

O Coordenador de Proteção de Dados do Grupo é responsável por auxiliar o Responsável pela Proteção de Dados do Grupo.

Representante Local de Proteção de Dados

O Representante Local de Proteção de Dados é o contato dos Colaboradores que presta o esclarecimento de quaisquer dúvidas ou preocupações relacionadas a proteção de dados dos Colaboradores e, quando for necessário, direciona as questões ao Coordenador ou ao Responsável pela Proteção de Dados.

Representantes de Proteção de Dados do Grupo

Os Representantes de Proteção de Dados do Grupo são responsáveis por checar a conformidade com os requisitos de proteção de dados dentro da sua área de negócio ou jurisdição. O Representante de Proteção de Dados do Grupo deve estar localizado no país, e, idealmente, servir uma função de controle (Jurídico, Risco, Compliance).

Todos os funcionários da Schroder Brasil, em alguma medida, são responsáveis por processar dados pessoais no exercício de suas respectivas atividades, de forma que é essencial que todos estejam cientes de suas responsabilidades individuais relacionadas à proteção desses dados.

4. Regras de Negociação Pessoal

Tendo em vista que os negócios do Grupo envolvem pesquisa e investimento em nome de clientes, podem surgir situações, reais ou aparentes, que envolvem conflitos de interesse e exposição de informações confidenciais ou sensíveis ao preço. Tais situações podem representar riscos regulatórios e de reputação significantes tanto para os Colaboradores, como para o Grupo como um todo.

Os Colaboradores devem cumprir com as normas aplicáveis contidas na Política de Compra e Venda de Valores Mobiliários por Colaboradores no Brasil. Além disso, os Colaboradores não devem realizar transações pessoais que possam representar uso indevido de informação privilegiada e/ou manipulação de mercado, atividade criminal, conflito de interesse material que não seja mitigado ou que seja uma violação do dever

fiduciário.

Isso inclui transações (sem limitação):

- que sejam baseadas em informações privilegiadas;
- que envolvam o uso indevido ou a divulgação inadequada de informações confidenciais; ou
- que configurem conflito com, ou que estejam propensas a um conflito com, uma obrigação da Schroder Brasil com um cliente, incluindo o dever fundamental de agir de acordo com os melhores interesses dos clientes.

Para maiores informações sobre as regras e procedimentos relacionados a compra e venda de valores mobiliários por Colaboradores e outras pessoas relacionadas, vide a Política de Compra e Venda de Valores Mobiliários por Colaboradores no Brasil.

5. Política de Conflito de Interesse no Brasil

O Grupo possui uma Política de Conflitos de Interesses do Grupo Schroder com o objetivo de identificar, prevenir, registrar e gerenciar os conflitos efetivos e potenciais de interesses que surgem ou possam surgir no contexto da execução de suas atividades.

Nessa esteira, a Schroder Brasil tem como obrigação de identificar efetivos e potenciais conflitos de interesses na prestação de de seus serviços e no exercício de suas atividades que impliquem no risco de prejuízo material para um ou mais clientes.

5.1 Registro de Conflitos de Interesse

O Grupo mantém um registro dos conflitos de interesses (“Registros de Conflitos de Interesse”) que podem surgir e as respectivas políticas e processos de mitigação aplicáveis. Tal registro está disponível em ferramenta de gerenciamento de riscos do Grupo.

A Área de Risco e Compliance da Schroder Brasil e do Grupo, bem como a gerência sênior da área de negócios analisam, juntos, o registro de conflitos de interesses para verificar se ele continua apropriado em função da evolução dos negócios e das mudanças ao longo do desenvolvimento de atividades pela Schroder Brasil.

Quaisquer conflitos de interesses adicionais ou novos (e métodos para mitigar ou tratar tais conflitos) são avaliados de acordo com os procedimentos estabelecidos na Política de Conflitos de Interesses do Grupo. Para maiores informações sobre os princípios gerais observados e os procedimentos adotados em caso de efetivo ou potencial conflito de interesse que surgem ou possam surgir no âmbito da execução das atividades da Schroder Brasil, veja a Política de Conflitos de Interesse do Grupo.

5.2 Responsabilidade e Procedimentos

Todos os Colaboradores, incluindo aqueles recém-contratados, deverão participar de programas de treinamento, atualização e conscientização das regras e procedimentos de conduta adotados pela Schroder Brasil (“Programas de Treinamento”).

É responsabilidade da gerência sênior das áreas de negócios apresentar sistemas eficazes, controles e

procedimentos para prevenir e, onde não for possível, identificar e gerenciar conflitos de interesses que possam surgir.

Todos os Colaboradores têm a responsabilidade de identificar e reportar ao seus respectivos superiores quaisquer novos conflitos que surjam no decurso do seu trabalho na Schroder Brasil. Se um Colaborador tomar conhecimento de um potencial conflito de interesses, o mesmo deve ser verificado no registro de conflitos de interesse mantidos pela área de Compliance. Caso tal conflito não esteja listado em tal registro, os Colaboradores devem notificar o potencial conflito ao Compliance.

Além da identificação dos conflitos que possam surgir no decurso da prestação de produtos e serviços já existentes, é possível que surjam conflitos de interesses em novas linhas de negócios, novos produtos e outros processos de gestão. É importante identificar onde conflitos de interesses potenciais ou efetivos podem surgir e estabelecer métodos adequados de prevenir ou gerenciar esses conflitos.

Potenciais conflitos de interesses devem ser especialmente observados nos seguintes processos de negócios, sem prejuízo de outros cenários que também devem ser eventualmente analisados:

- A avaliação da aquisição de empresas, alienações, joint ventures, alianças, terceirização e acordos de subcontratação;
- A utilização de um novo ativo financeiro;
- A nomeação ou alteração de um gestor de fundos terceirizado para prestação dos serviços de gestão de investimento;
- A concepção e lançamento de um novo fundo como parte do processo de desenvolvimento de produto, sob a supervisão do Comitê de Desenvolvimento de Produto;
- A estruturação e desenvolvimento de uma nova proposta de investimento sob a supervisão do Comitê de Estratégia de Produtos;
- A captação de um novo cliente, de acordo com a Política de Captação de Clientes do Grupo; e
- Mudanças na estratégia de investimento e estrutura para a gestão do capital do Grupo sob a supervisão do Comitê de Capital.

Novos potenciais conflitos de interesses devem ser reportados e discutidos prontamente com a administração da Schroder Brasil e o Chefe Global de Compliance. Questões importantes devem ser reportadas pelos membros relevantes da gerência sênior ou do Compliance imediatamente ao Chefe Global de Compliance e do Conselho Geral do Grupo.

O Comitê de Gestão do Grupo e o conselho de cada entidade do Grupo devem rever formalmente os conflitos de interesses ocorridos e sua gestão em uma periodicidade anual. Essa revisão será reportada ao Chefe Global de Compliance e questões significativas serão relatadas ao Conselho de Auditoria e Risco do Grupo.

A Política de Conflito de Interesses do Grupo foi elaborada como um guia operacional interno para auxiliar na identificação de conflitos de interesses. Situações podem divergir uma das outras e fatos que podem gerar um conflito em uma situação, podem ocasionalmente não gerar conflito em outra situação diferente, desse modo as devidas ações de mitigação também podem diferir.

6. Política de PLD/FTP

No âmbito das atividades exercidas pela Schroder Brasil é necessário dispensar especial atenção às operações que possam constituir-se em sérios indícios de crimes de "lavagem" de dinheiro ou ocultação de bens, direitos e valores.

Nesse sentido, a Schroder Brasil elaborou Política de Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa ("PLD/FTP") com o intuito consolidar as regras sobre os procedimentos a serem adotados na prevenção e combate a possíveis operações que sejam facilitadoras para os crimes de lavagem de dinheiro, financiamento do terrorismo e outras atividades ilegais correlatas ("Lavagem de Dinheiro"), à luz das melhores práticas internacionais de governança corporativa, bem como da legislação e regulamento aplicáveis.

Os cadastros e registros, nos termos dos Capítulos II, V e VII da Resolução CVM nº 50, de 31 de agosto de 21, bem como a documentação que comprove a adoção dos procedimentos previstos nestes capítulos mencionados, serão conservados, à disposição da CVM, durante o período mínimo de 5 (cinco) anos, contados a partir do cadastro ou da última atualização cadastral, ou da detecção da situação atípica, podendo esse prazo ser sucessivamente estendido por determinação da CVM.

As contrapartes das operações realizadas pela Schroder Brasil, incluindo, por exemplo, as corretoras contratadas, são aprovadas por meio de procedimento de due diligence prévia (através de preenchimento de questionários e visitas in loco, dentre outros procedimentos), além de estarem sujeitas à aprovação do Comitê da área de risco de crédito do Grupo, que define limite para cada contraparte, no momento da contratação. Ainda, os volumes operados e corretagens são monitorados diariamente por sistema específico e as contrapartes são reavaliadas anualmente pela área de risco de crédito do Grupo.

Adicionalmente, os Colaboradores são orientados, tanto em treinamentos quanto por meio da Política de PLD/FTP, a reportar à àrea de Compliance quaisquer operações e eventos suspeitos, na forma da legislação e da regulamentação vigentes.

Para maiores informações sobre as regras e procedimentos adotados pela Schroder Brasil para prevenção e combate à lavagem de dinheiro. consulte a Política de PLD/FTP da Schroder Brasil.

7. Sanções

O não cumprimento das regras dispostas nas demais Políticas da Schroder Brasil e do Grupo levará à aplicação de sanções que podem variar conforme cada política, em uma escala que ecoluí de uma advertência até o desligamento do Colaborador e, quando cabível, o encaminhamento às autoridades governamentais e organizações de auto-regulamentação competentes.

8. Canal de Denúncias

O Canal de Denúncias é o meio pelo qual o Colaborador ou terceiro externo pode relatar preocupações ou suspeitas de irregularidades por um membro da equipe ou um terceiro externo (por exemplo, um cliente, custodiante, fornecedor, prestador de serviços, intermediário ou corretor).

Se o Colaborador ou terceiro externo suspeitar de delito, impropriedade, comportamento antiético ou suspeitas de irregularidade, poderá comunicá-las confidencialmente de uma das maneiras a seguir.

- Chefe direto, Diretoria ou Compliance
- Safecall
- Via web (www.safecall.co.uk)

Para maiores informações, consultar a Política de Denúncias do Grupo.

9. Manutenção de Informações e Registros

As informações e registros de que trata esta Política devem serão mantidos e conservados conforme regras de manutenção de informações e registros do Grupo ou conforme legislação aplicável, caso maior.

10. Relatório Anual

Nos termos da Res. CVM nº 21/21, o Diretor de Compliance e Gestão de Risco da Schroder Brasil deve encaminhar ao Comitê Executivo (o qual é composto pelos diretores da Schroder Brasil), até o último dia útil do mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo:

(i) as conclusões dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação do Diretor de Investimento ou, quando for o caso, do Diretor de Compliance e Gestão de Risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

O referido relatório ficará disponível para a Comissão de Valores Mobiliários (“CVM”) na sede da Schroder Brasil.

11. Vigência e Atualização

A presente Política deverá ser revista, no mínimo, a cada dois anos, levando-se em consideração, dentre outras questões, mudanças regulatórias ou eventuais deficiências encontradas.

Esta Política poderá ser também revista a qualquer momento, sempre que o Diretor de Compliance e Gestão de Riscos entender necessário.

Toda e qualquer alteração nesta Política deve ser previamente aprovada pela Diretoria e será disponibilizada para ciência dos Colaboradores através de mensagem eletrônica ou por escrito.

Documento: Política de regras, procedimentos e controles internos				
Edição	**Data da aprovação**	**Aprovado por:**	**Descrição de ações**	**Elaborado por:**
2ª Edição	Junho/2023	Danie Celano – Country Head Fábio Ferreira – Head of Compliance Fernando Cortez – Head of Intermediary and Discretionary Sales	Revisão Anual Alterações das informações sobre a área de compliance e informações referentes à política de confidencialidade e segurança da informação Inclusão de tópico de PLD/FTP, sançoes e Canal de Denúncias	Mariana Barbosa – Compliance Analyst
1ª Edição	Abril/2021	Fábio Ferreira – Diretor de Compliance e Risco	Versão Inicial	Assessoria Jurídica