PROCEDIMENTO DE COORDENAÇÃO E DISTRIBUIÇÃO DE OFERTAS PÚBLICAS DE AÇÕES RES. CVM 161/22

Este documento visa detalhar os procedimentos adotados pelo Banco Santander Brasil S.A. e a Santander Corretora Câmbio e Valores Mobiliários, para cumprimento das exigências previstas na Resolução CVM 161/22, como responsáveis pela coordenação e distribuição de valores mobiliários.

0 ÍNDICE DE CONTEÚDO

1 INTRODUÇÃO

1.1 Definição e escopo

Este procedimento tem por objetivo, estabelecer as diretrizes e controles adotados pelo Banco Santander Brasil S.A. e pela Santander Corretora de Câmbio e Valores Mobiliários S.A. (“Santander”) para atender aos requisitos previstos na Resolução CVM 161/22, na atividade de coordenação e distribuição de ofertas públicas de valores mobiliários.

1.2 Regras, procedimentos e controles internos

O Santander possui um conjunto de regras, políticas e procedimentos internos que visam atender as boas práticas no que se refere a gestão de informações sensíveis e não públicas, segregação de atividades, conflitos de interesse e gestão de acessos.

As regras e procedimentos descritas no presente documento, são complementares às diretrizes previstas nas políticas internas relacionadas a seguir e que tem por objetivo assegurar o controle de informações relevantes e não públicas, bem como a conduta de seus colaboradores no exercício de suas atividades, visando um comportamento ético:

- Código de Ética e Conduta;
- Política de Conflito de Interesses;
- Política de Informação Sensível;
- Política de Acesso Físico às Áreas Separadas;
- Política Cyber Security - Requerimentos de Segurança Cibernética;
- Política de Investimentos Pessoais;
- Código de Conduta nos Mercados de Valores (CCMV).

2 PROCEDIMENTOS

2.1 Segregação física de atividades

As regras e procedimentos referentes a segregação física de atividades do Banco Santander e da Santander CCMV são aplicáveis a todos os colaboradores elegíveis ao Código de Conduta nos Mercados de Valores Mobiliários (CCMV).

As áreas separadas, são áreas que desempenham funções que tratam de informações sensíveis, confidenciais, privilegiadas e relevantes e necessitam estar segregadas das demais áreas do banco e da corretora.

Atualmente as áreas separadas que possuem controle de acesso físico são:

- Banking;
- Assessoria de Investimentos;
- Private Banking;
- Comercializadora de Energia;
- Compliance;
- Corretora;
- Desenvolvimento Corporativo;
- Gestão financeira/ALM;
- Global Debt Financing (GDF);
- Global Trade Services (GTS);
- Investment Banking (IB);
- Macroeconomic Research;
- Relações com Investidores;
- Research;
- Tesouraria;

Das áreas acima citadas, as seguintes áreas atuam respectivamente, na distribuição e coordenação de ofertas públicas do Banco Santander e da Santander Corretora:

- Global Debt Financing (GDF)
- Equity Capital Markets (divisão de Investment Banking),
- Corretora;

- Assessoria de Investimentos.

As solicitações de acesso às áreas separadas, para funcionários do Banco Santander e da Santander Corretora devem ser solicitadas para a área de Compliance Assessorias que após análise enviará a autorização ou a recusa, comunicando a área de Controle de Acessos, que por sua vez comunicará ao solicitante.

O mesmo procedimento deve ser utilizado na solicitação de acesso para prestadores externos, tais como auditorias, prestadores ou visitas de colaboradores do Grupo Santander.

As solicitações de acesso para funcionários que atuam na manutenção das áreas são liberadas somente pela equipe de Controle de Acesso e semestralmente devem ser revisadas.

2.1.1 Controle de informações relevantes e não públicas

O Santander possui um conjunto de diretrizes e procedimentos pré-definidos para controle de informações sensíveis. Esses controles também chamados de Chinese Wall, são compostos pelas barreiras físicas e controle de acessos descritos no item 2.1, e pelos procedimentos de barreiras eletrônicas que asseguram que as informações concebidas em uma área de negócio permaneçam dentro de tal área e só sejam compartilhadas com outras áreas se houver uma necessidade legítima. Além disso, permitem ao Banco realizar atividades de banco de investimento em mercados primários ao passo que as equipes de Research atuam em mercados secundários, com base em informações públicas.

Áreas Privadas e Áreas Públicas são termos utilizados para descrever os 2 lados das Barreiras de Informações, sendo:

Áreas Privadas: áreas que possuem Informações Privilegiadas que podem influenciar, direta ou indiretamente o mercado de valores, ou seja, refere-se às áreas de negócio relacionadas ao Santander Corporate & Investment Banking (SCIB) e a Corretora Santander.

Área Pública: atividades relacionadas aos mercados secundários como a área de Research. Observe que essa área produz relatórios de análise baseados exclusivamente em informações públicas. No entanto, os relatórios de pesquisa

(anteriores à publicação) são considerados Informações Confidenciais e, nesses casos, Research adota medidas cautelares semelhantes aos das Áreas Privadas.

O princípio "*Need to Know*" é o princípio de conceder o conhecimento de uma Informação Sensível a outro colaborador exclusivamente para exercer suas atividades dentro do Santander e deve ser seguido por todos os funcionários.

As Informações Sensíveis só podem ser compartilhadas seguindo estritamente a este princípio, inclusive quando não há Barreiras de Informações oficialmente estabelecidas. As implicações do princípio "Need to Know" são amplas, por exemplo, um funcionário não pode compartilhar Informações Sensíveis com outro membro de seu departamento se não for estritamente necessário para o desenvolvimento da atividade.

Quando há a necessidade, de conceder a informação sensível de uma área privada para um colaborador de área pública, a área de Compliance Control Room avalia a solicitação e entra com procedimentos de barreiras eletrônicas para que o funcionário da área pública possa ter acesso a informação da área privada, esse procedimento é denominado “transposição de barreira”. O analista de Research que estiver transposto não poderá emitir opiniões e relatórios sobre a companhia a qual teve acesso a informação sensível e não pública até o final do projeto, quando a informação se tornará pública e a barreira poderá ser retirada.

Compliance mantém a lista de valores mobiliários monitorados (Restricted List), lista confidencial de transações nas quais o Santander está mandatado ou mantém Informações Privilegiadas (geralmente transações que envolvem empresas com valores mobiliários negociados na bolsa, que, se conhecidas pelo mercado, teriam um efeito significativo nos preços de valores mobiliários ou de instrumentos financeiros derivativos relacionados).

A lista de valores mobiliários monitorados permite ao Compliance controlar a integridade das Barreiras de Informações, administrar Conflitos de Interesse, supervisionar operações de investimentos pessoais de funcionários e dar continuidade aos processos de Transposição de Barreiras.

Por meio desses procedimentos a área de Compliance realiza o monitoramento de informações sensíveis diariamente, além disso, todos aqueles que tem acesso a informações sensíveis são classificados como iniciados e devem seguir diretrizes internas que visam a utilização dessas informações exclusivamente para o desempenho de suas atividades.

Além da condição de Área Privada e Área Pública, certos indivíduos têm o status de Iniciado Permanente, ou seja, são aquelas pessoas que se considera como tendo ou com possibilidade de chegar a ter conhecimento, em geral, de todas as operações, projetos, oportunidades e pipelines de Áreas Separadas.

Serão considerados Iniciados Permanentes, pessoas que têm conhecimento de todas as operações ou projetos de sua área de negócios, embora não sejam membros da equipe designada para cuidar do dia a dia de cada operação ou projeto, e/ou aqueles que possam ter um conhecimento mais amplo dos pipelines das Áreas Separadas.

Implicações/precauções por ser considerado Iniciado Permanente:

- Deve conhecer as obrigações compreendidas no Código de Conduta nos Mercados de Valores (CCMV) relacionadas com Informações Sensíveis e Barreiras de Informações;
- Adotar o princípio "Need to Know" em todas as suas comunicações;
- Aplicar as medidas de segurança físicas e eletrônicas com relação às informações sensíveis;
- Desenvolver um papel-chave na gestão de conflitos de interesses surgidos no negócio;
- Cumprir com as obrigações compreendidas no CCMV com relação à operação pessoal com Valores Mobiliários negociados em Bolsa de Valores, sendo consciente de que devido à natureza de sua posição pode estar sujeito às restrições para operar.

2.1.2 Controle de Acessos

Na Política de Segurança Cibernética do Santander são definidos os procedimentos de gestão de acessos de usuários para ferramentas que contenham informações corporativas. O principal objetivo no controle de acessos é de identificar, autenticar, autorizar e definir a responsabilidade do acesso ao usuário, seguindo as categorias de controles de confidencialidade, integridade e disponibilidade.

- Os controles de acesso de confidencialidade garantem que apenas os sujeitos autorizados possam acessar os objetos. Quando sujeitos não autorizados são capazes de acessar sistemas ou dados, isso resulta em perda de confidencialidade.

- Os controles de acesso de integridade garantem que os dados ou as configurações do sistema sejam modificados somente quando autorizados ou se ocorrerem alterações não autorizadas, os controles de segurança detectam as alterações. Se ocorrerem alterações não autorizadas ou indesejadas em objetos, isso resultará em perda de integridade.
- Os controles de acesso de disponibilidade devem conceder acesso a sistemas e dados a sujeitos autorizados, dentro de um período razoável. Se os sistemas não estiverem operacionais ou os dados não estiverem acessíveis, isso resultará em perda de disponibilidade.

As informações sensíveis e não relevantes relacionadas a oferta pública de ações e outros projetos do Santander, são mantidos em diretórios segregados, sendo o acesso permitido somente mediante autorização prévia do gestor responsável, por meio de chamado aberto no sistema interno de requisições.

Cada área possui diretório de rede segregado e o acesso solicitado a pastas e sistemas corporativos, deve estar relacionado as atividades que o colaborador irá exercer, caso não esteja, a requisição será negada e o acesso não será concedido.

Adicionalmente são realizados monitoramentos periódicos de envio e recebimento de e-mails externos, para mitigar riscos de incidentes cibernéticos.

2.2 Gestão de conflitos de interesse

São consideradas Conflitos de Interesse as situações nas quais um funcionário, o Grupo ou uma parte do Grupo têm um interesse comercial ou pessoal que possivelmente concorra com o interesse de um ou mais clientes ou de uma parte do Grupo envolvendo dinheiro, status, conhecimento ou reputação; e tais interesses podem tornar difíceis para os funcionários e/ou para o Grupo cumprir com suas funções de maneira imparcial e podem ser prejudiciais para os interesses de um cliente se não são adequadamente administrados.

Um Conflito de Interesse sem evidência de ações incorretas, pode criar uma aparência de inadequação que poderia reduzir a confiança na capacidade do Grupo ou de seus funcionários para atuar adequadamente.

Os conflitos de interesse podem surgir entre as diversas partes, incluindo:

- O Grupo e um ou mais de seus clientes;
- Um funcionário e um ou mais dos clientes;
- Duas entidades do Grupo Santander;
- Um funcionário e uma entidade do Grupo Santander;
- Dois ou mais clientes;
- Um prestador de serviços e uma entidade do Grupo Santander;
- Um prestador de serviços e clientes;
- Dois ou mais funcionários.

O Santander atua de forma ativa e diligente para administrar seus conflitos de interesse de forma apropriada, para mitigar o risco de ações legais, perdas de receita, crítica e censura por parte de órgãos reguladores, prejuízo à reputação e outras razões éticas associadas.

Sempre que uma nova operação/projeto das áreas de negócios é iniciada esta deve ser comunicada para a área de Compliance que irá adotar as medidas de gestão de informações sensíveis, tais como lista de iniciados, transposição de barreiras (se houver), ativos restritos, nesse momento também são avaliados se existem possíveis conflitos com outros projetos já abertos, em caso positivo, os responsáveis por cada projeto são contatados e são levantados mais detalhes sobre as operações.

Compliance irá avaliar e emitir opinião e entrará com os responsáveis das áreas de negócios para tomada de decisão quanto as medidas que devem ser adotadas. Não havendo conflito a operação segue seu fluxo normal seguindo as medidas de gestão de informações sensíveis.

O fato de Compliance realizar a avaliação de conflitos no recebimento da abertura dos projetos, não isenta os responsáveis das áreas de negócios de informar no momento do envio das informações do projeto, caso tenham conhecimento sobre qualquer possibilidade de conflitos com outras operações.

2.3 Vulnerabilidades e testes periódicos

O Santander e suas subsidiárias contam com uma estrutura consistente de Tecnologia, Segurança das Informações e testes periódicos para identificação de vulnerabilidades sistêmicas.

Os testes têm como objetivo a identificação, gestão e remediação de vulnerabilidades para prevenir e mitigar o risco de ataques cibernéticos e outros incidentes de segurança.

As vulnerabilidades podem ser identificadas por meio de testes regulares ou por correções, bugs e atualizações sistêmicas e são classificadas em emergencial, críticas, alta, média e baixas.

Os testes regulares são consistem em revisar regularmente os riscos relevantes e o nível de proteção para descobrir e corrigir proativamente os pontos fracos dos principais sistemas e informações.

A Verificação de Vulnerabilidade é uma técnica utilizada para testar sistemas quanto à ocorrência de vulnerabilidades publicadas em repositórios públicos e a execução de testes pré-gravados como injeção de sequências SQL, testes de overflow, manipulação de cookies e outras técnicas automatizadas.

Os testes de penetração são avaliações especializadas em sistemas de informação ou componentes individuais do sistema que tenta duplicar as ações de adversários na realização de ataques cibernéticos hostis. Este teste fornece uma análise mais aprofundada de várias fraquezas/deficiências relacionadas à segurança que podem ser exploradas para comprometer a rede e obter acesso a sistemas de informação e dados.

O Red Team é um exercício direcionado para emular os recursos de ataque ou exploração de um adversário em potencial contra uma rede de entidade e um perímetro de defesas de segurança, normalmente com duração mais longa do que os testes de penetração. O objetivo do Red Team é obter acesso aos sistemas da entidade e informações relevantes, de forma a evitar ser detectado, e demonstrar os impactos de ataques bem-sucedidos, avaliando as capacidades de detecção e resposta da organização.

2.4 Programa de treinamentos

O processo de onboarding de novos funcionários do Santander compreende a disponibilização de diversos treinamentos mandatórios por meio da ferramenta interna “Academia Santander”.

Com relação aos treinamentos disponibilizados na Academia que tratam de informações relevantes, não públicas e conflitos de interesse e são destinados ao público elegível ao CCMV, podemos destacar os seguintes:

- Conflitos de interesse;
- Código de Conduta nos Mercados de Valores;
- Código de Ética e Conduta;
- Prevenção ao Abuso de Mercado – Market Abuse;
- Segurança da Informação.

Os treinamentos são disponibilizados em até 1 (um) dia útil da data de início do colaborador e é determinado um prazo de 90 (noventa) dias para sua conclusão.

Além dos temas relacionados acima, outros treinamentos considerados mandatórios com base nas políticas internas do Santander e na função que o colaborador irá exercer, também são disponibilizados na Academia.

3 GOVERNANÇA DA POLÍTICA

3.1 Titularidade do procedimento

A elaboração deste procedimento é de responsabilidade da área de Compliance Regulatório e Reputacional e sua aprovação realiza-se conforme o modelo normativo de riscos.

3.2 Interpretação

Corresponde à área de Compliance Regulatório a interpretação deste procedimento.

4 CONTROLE DE VERSÕES

Versão (mês/ano)	Titular	Revisor	Validação corporativa	Aprovação	
				Alçada	Data
07/2023	Aline Lima	Mayra Melo	n/a		14/08/2023
Versão (mês/ano)	**Descrição da alteração**				
07/2023	Elaboração do documento				