# POLÍTICA DE CONTROLES INTERNOS PARA COORDENADORES DE OFERTAS PÚBLICAS DE DISTRIBUIÇÃO DE VALORES MOBILIÁRIOS

## Fevereiro 2023

**Data de Aplicação:** 06 de fevereiro de 2023

# ÍNDICE

1. INTRODUÇÃO ..... 3
   1.1 Propósito ..... 3
   1.2 Escopo ..... 3
   1.3 Periodicidade de Revisão ..... 3
2. POLÍTICAS E PROCEDIMENTOS RELACIONADOS ..... 3
3. PRINCÍPIOS DA POLÍTICA ..... 4
   3.1 Processo de Coordenação Ofertas Públicas de Distribuição de Valores Mobiliários ..... 4
   3.2 Estrutura Organizacional ..... 8
   3.3 Código de Ética ..... 9
   3.4 Confidencialidade ..... 9
   3.5 Testes periódicos de segurança para os sistemas de informações ..... 10
   3.6 Programa de Treinamento e Desenvolvimento ..... 11
   3.7 Planos de contingência, continuidade de negócios e recuperação de desastres adotados ..... 12
   3.8 Relatório de efetividade das regras, políticas, procedimentos e controles internos ..... 14
   3.9 Guarda de documentações ..... 15
4. FUNÇÕES E RESPONSABILIDADES ..... 15

# 1. Introdução

## 1.1 Propósito

Este documento visa adequar o Scotiabank Brasil S.A Banco Múltiplo ("Banco"), que faz parte do Grupo Scotiabank Brasil ("Grupo SBB") em conjunto com a Scotiabank Brasil S.A CTVM ("Corretora") aos requerimentos definidos pela Resolução CVM nº 161 de 13 de julho de 2022, mais especificamente em seu capítulo IV (Artigo 11 II) que trata sobre as regras, procedimentos e descrição dos controles internos para Coordenadores de Ofertas públicas de distribuição de valores mobiliários.

## 1.2 Escopo

Esta políica é aplicável a todos os colaboradores que atuem nas funções de Coordenadores de Ofertas Públicas no Grupo Scotiabank Brasil, mais especificamente aos colaboradores da área Investiment Banking, M&A e diretores responsáveis pela Resolução CVM nº 161.

## 1.3 Periodicidade de Revisão

Este documento deverá ser revisado pelo menos a cada 2 (dois) anos, ou quando houver alterações no ambiente regulatório local que exija o cumprimento de requisitos específicos.

# 2. Políticas e Procedimentos Relacionados

Esta Política deve ser lida e aplicada em conjunto com os seguintes documentos:

- Código de Ética – Coodenador de Ofertas Públicas;
- Manual de Código de Conduta;
- Regras de Negociação e Subscrição em Valores Mobiliários ;
- Política de Segurança da Informação;
- Política de Treinamento e Desenvolvimento;
- Manual de Continuidade e Procedimentos & Contingência;
- Política de Privacidade.

# 3. Princípios da Política

## 3.1 Processo de Coordenação Ofertas Públicas de Distribuição de Valores Mobiliários

Conforme estabelecido pela CVM, o coordenador da oferta pública deve garantir, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, referentes aos diferentes ritos de registro de oferta pública, à própria atividade de intermediação de ofertas públicas de distribuição de valores mobiliários e aos padrões ético e profissional.

A política de controles internos para coordenadores de ofertas públicas prevê os mecanismos adequados para controle de informações relevantes e não públicas, existência de testes periódicos de segurança e um programa de treinamento aos funcionários sobre privacidade de informação, durante a coordenação de ofertas públicas, nos ritos de Registro Automático de Distribuição e Registro Ordinário de Distribuição previstos na norma da CVM.

Em caso de atuação como um dos coordenadores líderes das ofertas públicas de valores mobiliários distribuídas por meio do Balcão B3, o anúncio de encerramento das distribuições no dia de sua realização será encaminhado à B3 através de canal de comunicação definido pela própria B3.

O controle interno de documentos e informações confidenciais é realizado por um alto padrão de segurança digital, submetido a testes periódicos de risco e vulnerabilidade. As informações obtidas durante o processo de coordenação da oferta são armazenadas dentro do prazo mínimo de 5 (cinco) anos, ou por prazo superior em caso de determinação expressa da CVM.

- ***Equity Commitment Committee – ECC***

Através de uma política interna de diligência, o Banco segue criteriosos e robustos requisitos e arcabouços a fim de mitigar eventuais riscos regulamentares e legais, e a respeitar as condições estabelecidas nas normas da CVM. O Banco conta com a presença de um comitê interno ("*Equity Commitment Committee* – ECC"), responsável por avaliar se a oferta pública está de acordo com as principais políticas internas e analisar a materialidade de eventuais riscos associados à oferta.

Antes que o Banco aceite participar de qualquer transação, o ECC deve ser consultado para dar aprovação. O ECC pode também, dependendo da transação e do cronograma, exigir uma segunda reunião antes do lançamento de uma transação para revisão final da diligência, caso a diligência não tenha sido concluída no momento da primeira reunião.

O ECC tem o dever de analisar as transações submetidas para aprovação, incluindo a documentação relativa às informações financeiras do emissor, perfil comercial, concorrentes e do mercado para os títulos e, conforme apropriado, tomar medidas para mitigar os riscos de reputação e outros riscos associados a essas transações e/ou aos clientes envolvidos nelas.

Para seguir com os requisitos do ECC, os colaboradores do Banco envolvidos na execução da oferta pública precisam submeter ao comitê um memorando, com formato pré-estabelecido, contendo informações relacionadas à estrutura organizacional do emissor, à equipe administrativa, às informações financeiras, aos termos da transação proposta, ao relacionamento do Banco com o emissor/vendedor e outras informações relevantes. As informações utilizadas no desenvolvimento do memorando são retiradas dos documentos desenvolvidos no andamento da oferta pública, como também, diagnósticos internos, relatórios e pareceres enviados por auditores e representantes legais da Companhia.

O ECC é um fórum altamente confidencial e nenhum outro funcionário será convidado para o ECC. A equipe envolvida na oferta (e se for o caso, analista de *research*) será convidada apenas para apresentar sua transação específica. Após a conclusão do processo, sua participação será encerrada pelo presidente.

Os documentos apresentados ao comitê, assim como as atas de registro dos participantes das reuniões e o resultado das reuniões, são mantidos pelo secretário do ECC, que incluirá detalhes das transações propostas juntamente com os nomes dos membros do comitê de aprovação envolvidos para alcançar o quorum.

O ECC é composto pelos seguintes membros:

**Membros Votantes:**

Dos Estados Unidos (EUA)

*Head of U.S. Equity Capital Markets (Chair)*

*Head of U.S. Equity Syndicate (Alternate Chair)*

*Director of U.S. Equity Capital Markets*

*Pelo menos um dos três U.S. CIB Senior Managing Directors*[1]

*Head of U.S. Corporate & Investment Banking*

*Head of U.S. Equity Research*

*Head of U.S. & LatAm Equity Sales & Trading**

*Head of U.S. GBM**

*SCUSA CEO**

De fora dos Estados Unidos

*Head of Global Equity Capital Markets*

*Head of Equity Capital Markets Syndication*

*One of Global Co-Heads of CIB**

*ECM CIB Vice Chairman**

Representantes do Departamento Jurídico e de Compliance serão convidados para o ECC, sem direito a voto e com capacidade consultiva, para fornecer contribuições em relação a preocupações regulamentares ou legais específicas relacionadas a uma transação. Um secretário para o ECC também será nomeado e ele/ela também não terá direito a voto.

**Membros Não Votantes**

*U.S. Compliance**

*U.S. Legal Counsel**

*Committee Secretary*

1 *U.S. CIB Managing Directors* não poderão votar em transações que ocorram em seu setor

* A presença destas pessoas não é obrigatória, embora quaisquer preocupações observadas por qualquer parte devam ser compartilhadas com a Presidência de forma oportuna

A tabela abaixo estabelece os requisitos de quórum para aprovação das transações, dependendo do papel que a Banco assumirá no acordo:

| **Tipo de Transação** | **Requisito de Quórum** |
|---|---|
| Compromisso firme (*Bought Deal*) | 4 Votos (mínimo de 3 deve ser de membros dos EUA) |
| Melhores Esforços (*Active Bookrunner*) | 4 Votos (mínimo de 3 deve ser de membros dos EUA) |
| Melhores Esforços (*Passive Bookrunner and Co-Manager*) | 3 Votos (mínimo de 2 deve ser de membros dos EUA) |

- **Barreiras de Informação (*Chinese Wall*)**

Para se proteger contra o uso indevido de informações sensíveis, o Banco adota a Barreiras de Informação (*Chinese Wall*) para limitar o fluxo de informações sensíveis entre diferentes grupos de negócios dentro do Banco. As Barreiras de Informação consistem em um conjunto de políticas e procedimentos destinados a restringir o acesso a informações sensíveis e permitir que as unidades do Banco continuem suas atividades de pesquisa, vendas, negociação e consultoria com relação aos instrumentos financeiros de um emissor, enquanto outra unidade possui Informações Sensíveis sobre o assunto.

A partir de abril de 2021, o Banco implementou um bloqueio de comunicações eletrônicas que proibe e-mails diretos entre as áreas de *Banking* e *Research*. Quase todas as interações entre *bankers* e analistas de *research* requerem um contato via *Chaperone*. O *Chaperone* é uma função independente que monitora as comunicações para garantir a conformidade com os padrões de comunicação do Banco. Para interações telefônicas ou presenciais, é necessária a presença/inclusão de um membro do *Chaperone* na chamada.

Outra forma de Barreira de Informação existente é a segregação física da área de *Investment Banking*, através de uma sala com acesso restrito aos colaboradores da área com o objetivo de preservar a integridade e confidencialidade das informações dos projetos.

- ***Information Control List – ICL***

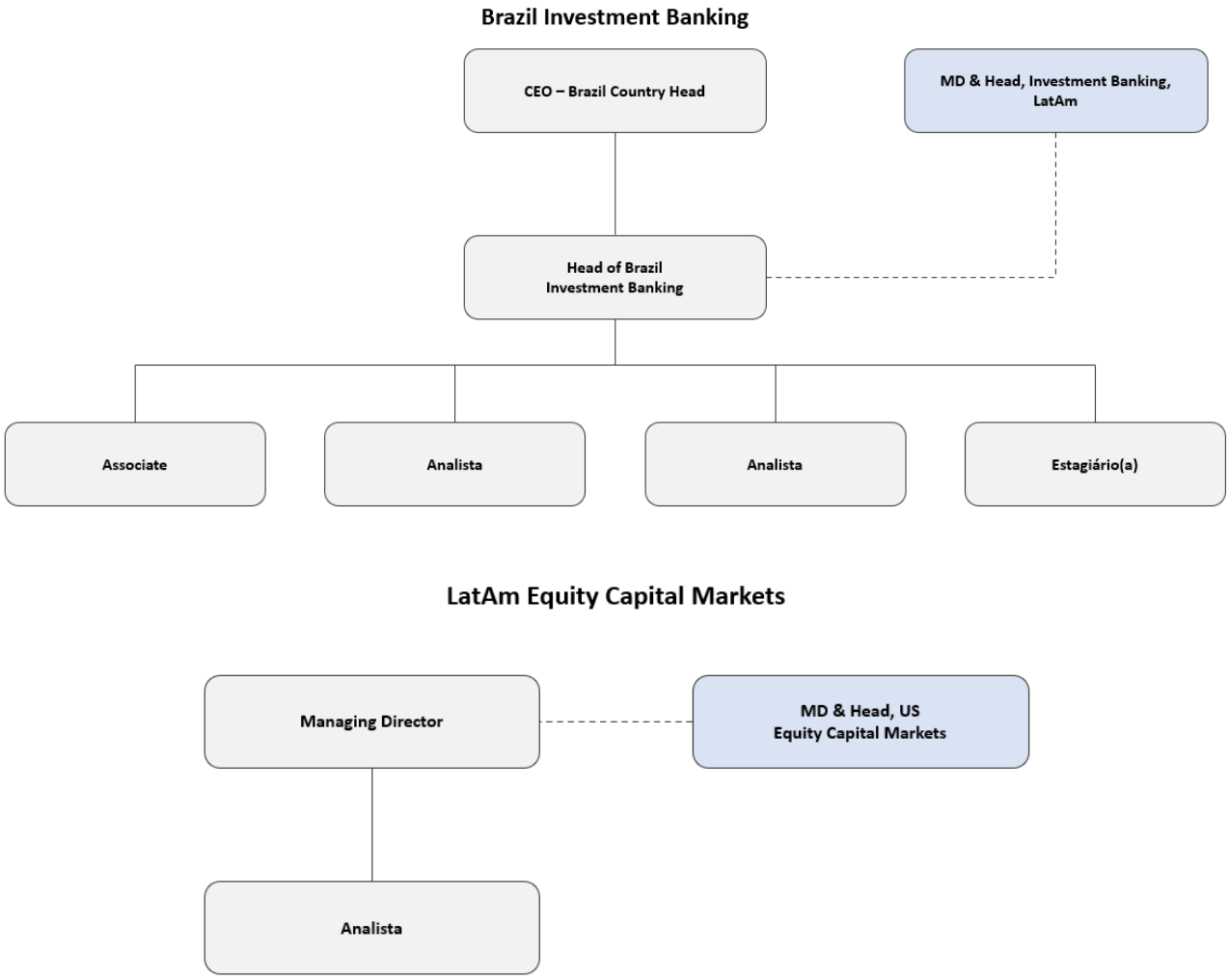
Para controle interno de acesso as informações confidenciais, a equipe alocada na execução da oferta pública é responsável por elaborar uma *Information Control List* (ICL), que é um documento interno projetado para auxiliar o Banco no controle dos colaboradores com acesso a informações sensíveis. Normalmente, a ICL conterá os nomes dos membros da equipe envolvida no projeto, funcionários que são trazidos acima da Barreira (*over the Barrier*), bem como detalhes de quaisquer comitês que revisaram a transação em potencial.

Embora a área de *Compliance* seja responsável por manter as listas de colaboradores com acesso a informações sensíveis, o Compliance pode buscar a assistência dos grupos de negócio do Banco para garantir a precisão dessas listas.

Todas as medidas razoáveis devem ser tomadas para assegurar que os indivíduos de uma ICL ou uma lista de informação privilegiada sejam informados dos deveres legais e regulamentares envolvidos (incluindo restrições às suas atividades pessoais e comerciais) e estejam cientes das penalidades aplicáveis ao *Insider Trading* (de outra forma referido como *Insider Dealing*) e da divulgação ilegal de informações sensíveis.

## 3.2 Estrutura Organizacional

A coordenação e execução do escopo de responsabilidades acerca das ofertas públicas de distribuição de valores mobiliários é organizada pelas áreas de *Investment Banking* Brasil e *LatAm Equity Capital Markets*. As respectivas estruturas organizacionais podem ser encontradas abaixo:




## 3.3 Código de Ética

O Código de Ética do Coodenador de Ofertas Públicas está alinhado com o *Scotiabank Code of Conduct* (o "Código de Conduta Global") da matriz do *The Bank of Nova Scotia* ("BNS"), da qual o Grupo SBB é subsidiário, e com o "Manual do Código de Conduta" do Grupo SBB.

Este documento foi divulgado a todos os colaboradores do Grupo SBB e está disponível também no site do Grupo SBB (https://www.br.scotiabank.com/Regulamentos_e_Politicas.html).

## 3.4 Confidencialidade

O Banco salvaguardará e controlará rigorosamente a divulgação das informações recebidas e restringirá a divulgação destas para o Banco e seus afiliados, diretores, administradores,

funcionários, representantes, conselho, ou outros agentes que precisem conhecê-las para as finalidades da execução do serviço e por motivos de conformidade jurídica ou de gestão de risco (considerando que o Banco informe esses representantes sobre a natureza confidencial das informações e que sejam instruídos pelo Banco para que tratem as informações provenientes de forma confidencial).

Os documentos e informações referentes às ofertas são armazenados com as devidas políticas de segurança de informação, com periódicos testes de segurança/vulnerabilidade dos sistemas e infraestruturas de redes, conforme esclarecido na seção 3.5 do documento. O acesso a qualquer documento referente a transação fica restrito às pessoas que tenham necessidade de conhecer essas informações e/ou com envolvimento na execução da oferta pública de ações.

Cada colaborador envolvido é instruído a respeitar a confidencialidade profissional e seguir as normas e diretrizes de controles internos do Banco para elaboração, manuseio, reprodução, divulgação, armazenamento, e descarte de informações e documentos referentes às ofertas, respeitando os níveis de proteção e de classificação da informação estabelecidos no regimento interno. Em caso de descumprimento das normas estabelecidas, o funcionário do Scotiabank estará sujeito a avaliação interna, encerramento de contrato, ou medidas judiciais subsequentes, conforme políticas internas, bem como legislação aplicável.

Ainda, conforme menciona anteriormente todos os colaboradores envolvidos na coordenação e execução de ofertas públicas são devidamente alocados no controle dos colaboradores ("*Information Control List* – ICL") com acesso a informações sensíveis, concordando previamente com o Código de Ética do Coodenador de Ofertas Públicas interno do Banco, e podendo responder a medidas internas em caso de descumprimento com o regimento interno do banco.

## 3.5 Testes periódicos de segurança para os sistemas de informações

Conforme descrito na Política de Segurança da Informação, os Testes de Segurança são conduzidos por Bank of Nova Scotia ("BNS"), de forma periódica a fim de minimizar incidentes que possam causar a interrupção nos negócios. Os respectivos relatórios, em sua maioria, podem ser acessados via rede e/ou enviados regularmente pelas áreas responsáveis. Os principais testes

são:

- **Análise de Vulnerabilidade (Vulnerability Assessment)**

Trata-se de um processo de identificar e definir vulnerabilidades nos sistemas, aplicações e infraestrutura de rede. BNS usa Tripwire IP360 para executar a rotina de análise.

Frequência: diária

Área Responsável: Information Security BNS – Compliance Vulnerability Reporting

- **Análise de Conformidade das Configurações (Configuration Compliance Assessments)**

Análise das Configurações, também conhecida como Compliance Scanning, refere-se aos testes para assegurar que as definições de configurações estão em conformidade e aderentes à política do Banco.

Frequência: semanal / mensal

Área Responsável: Information Security BNS – Compliance Vulnerability Reporting

- **Penetration Testing**

A equipe de CSRT, Cyber Security Red Team, é responsável por executar e coordenar os testes de intrusão globalmente, além de garantirem que os testes sejam executados em conformidade com os requisitos e regulamentações globais.

Frequência: anual / por solicitação.

Área Responsável: Cyber Security Red Team BNS – Enterprise Security Services

Mensalmente os relatórios de Vulnerabilidade e de Compliance são avaliados pela equipe de TI São Paulo a fim de garantir que o ambiente do Grupo Scotiabank Brasil esteja contemplado e, caso alguma ocorrência seja encontrada, a mesma será tratada. O Teste de Penetração (Pen Test) é avaliado anualmente, após realização do teste pela equipe de BNS. A formalização se dará através de email para o Head de TI informando o status das análises do mês corrente.

## 3.6 Programa de Treinamento e Desenvolvimento

O Grupo Scotiabank Brasil mantém constantes esforços para a disseminação de conhecimento

acerca dos seguintes temas: Compliance, Prevenção à Lavagem de Dinheiro e Fraudes. Para tanto, disponibiliza aos funcionários, consultores, estagiários e prestadores de serviços, se aplicável, de tempos em tempos, treinamentos e palestras que visam à conscientização e o comprometimento de todos.

Com o intuito de assegurar o cumprimento dos requerimentos de órgãos regulatórios (Banco Central do Brasil e CVM), assim como recomendações de entidades representativas de classe (ABBI, Febraban, Anbima, B3, CRC, OAB e etc.), os Gestores do Grupo Scotiabank Brasil devem comunicar à área de RH e Compliance, quando aplicável, sobre a necessidade de treinamentos e/ou palestras para a disseminação de conhecimentos exigidos por tais órgãos e/ou entidades representativas, assim como, enviar ao RH os devidos comprovantes exigidos pelos mesmos.
A área de RH e Compliance atuarão em conjunto com as áreas responsáveis para definir de que forma tais treinamentos e palestras serão ministrados.
O material de treinamento, a lista de presença, assim como a avaliação dos participantes quanto ao conteúdo ministrado nas palestras e treinamentos são arquivados pela área de Compliance.
É dever de todos os funcionários e demais colaboradores participar, de forma satisfatória, em treinamentos e palestras. O Grupo Scotiabank Brasil reserva-se no direito de aplicar sanções disciplinares, caso o funcionário e/ou colaborador não participe de quaisquer desses treinamentos e palestras. Conforme Política Disciplinar.

## 3.7 Planos de contingência, continuidade de negócios e recuperação de desastres adotados

O objetivo do Plano de Contingência é permitir a continuidade dos processos de negócios, do Grupo Scotiabank Brasil, quando os componentes que os suportam falharem em função de algum evento, ameaça ou desastre tecnológico, humano, natural e/ou físico. Desta forma, o Plano visa fornecer orientações e segurança razoável para que os sistemas que suportam os processos de negócios críticos sejam recuperados dentro do tempo aceitável de interrupção e o negócio tenha continuidade. Além disso: ele garante a segurança dos empregados e dos visitantes;

facilitando e guinando a tomada de decisão diante de uma situação de desastre; de forma a minimizar eventuais danos imediatos e perdas decorrentes de situações de emergência. Por fim, o Plano assegura a restauração das atividades, instalações e equipamentos na maior agilidade possível e garante a continuidade dos processos de negócios críticos.

- **Site de Contingência**

O Grupo Scotiabank Brasil possui um local externo denominado de "Site de Contingência", que armazena e compreende informações de sistemas, procedimentos de recuperação, bem como instalações, equipamentos e serviços. É destinado a suportar e dar continuidade aos processos de negócios críticos, definidos em conformidade com a análise de impacto dos negócios descritas nos Business Continuity Plan (BCP) específicos junto às áreas do Conglomerado.

Todos os dados do Grupo Scotiabank Brasil são replicados diariamente para o Site de Contingência.

- **Data Center (CPD)**

Grupo Scotiabank Brasil possui um Data Center em São Paulo (denominado de CPD – Central de Processamento de Dados), que é um ambiente projetado para abrigar servidores, computadores e sistemas responsáveis pelo processamento de dados da organização. Cujo objetivo principal é garantir a disponibilidade de equipamentos que rodam sistemas cruciais e disponibilizar os serviços de TI.

Como medida de segurança, além de todos os dados serem replicados para o Site de Contingência, são realizados, também, Backups diários e mensais das informações processadas no CPD (SP). Estas informações são salvas em fitas e arquivadas nas instalações de uma empresa especializada denominada Iron Mountain.

- **Plano de Continuidade de Negócios**

A Continuidade de Negócios é um processo abrangente que identifica ameaças potenciais inerentes aos negócios do banco e os possíveis impactos nas operações provenientes de tais ameaças. Para fornecer uma estrutura em que se desenvolva um nível de resiliência organizacional que seja capaz de responder efetivamente e proteger os interesses das partes envolvidas, reputação, marca da organização e suas atividades de valor agregado, o Grupo

Scotiabank Brasil optou pelo desenvolvimento dos Business Continuity Plans. Estes Planos de Continuidade de Negócios podem ser definidos como a divisão da organização em vários departamentos, onde cada processo possui um conjunto de atividades, que é realizado periodicamente, e que produz algo de valor para a organização.

Os BCP's estabelecem uma estrutura estratégica e operacional adequada para:

- Melhorar proativamente a resiliência da organização, mitigando os riscos de interrupções e diminuindo o tempo de resposta a possíveis incidentes;

- Recuperar a operacionalização por meio de um método sistemático para retorno em tempo aceitável dos serviços críticos após um incidente;

- Obter capacidade de gerenciar uma interrupção, no negócio, de forma a evitar impactos para o mercado, protegendo a reputação da organização.

O Manual de Continuidade e Procedimentos & Contingência com o detalhamento de todo o processo de contingência e continuidade de negócios foi divulgado a todos os colaboradores do Grupo SBB.

## 3.8 Relatório de efetividade das regras, políticas, procedimentos e controles internos

O Diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Resolução CVM 161 irá elaborar, 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 responsável a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

O relatório será encaminhado aos Diretores do Grupo SBB e à CVM, por meio de sistema eletrônico disponível na página da CVM na rede mundial de computadores.

### 3.9 Guarda de documentações

Os documentos e informações referentes às ofertas serão armazenados pelo prazo de 5 (cinco) anos, ou por prazo superior em caso de determinação expressa da CVM, com as devidas políticas, sendo esses documentos de natureza pública ou confidencial.

Segue abaixo a relação dos principais documentos arquivados segmentado por categoria de aplicação:

- Documentos da oferta solicitados pela CVM: Prospectos, documentos de diligência, formulário de referência, contratos de distribuição, termo de adesão com corretoras, termo de aceitação para investidores, avisos ao mercado, fatos relevantes, anúncio de início da oferta, anúncio de encerramento da oferta, e outros documentos;
- Apresentações e documentos de *marketing* direcionados aos potenciais investidores: Apresentações corporativas de *Roadshow*, apresentações setoriais complementares, relatórios de *feedback* de investidores, e outros documentos;
- Documentos de organização interna: Cronograma da oferta, documentos de diligência interna, ata/registros de comunicação com o ECC, *e-mails* de comunicação com as partes envolvidas na oferta pública, relatório de despesas, comprovante de recebimento de honorários, e outros documentos.

## 4. Funções e Responsabilidades

| **Função** | **Responsabilidade** |
|---|---|
| **Responsável pela Política:**<br>Head of Investment Banking | • Manter atualizada esta política;<br>• Garantir que os controles descritos nesta política sejam executados e formalizados. |

| | |
|---|---|
| **CRO** | • Elaborar o relatório de efetividade das regras, políticas, procedimentos e controles internos;<br>• Encaminhar o relatório de efetividade; para os Diretores Executivos SBB e CVM. |
| **Diretoria Executiva SBB** | • Aprovar a Política de Controles Internos para Coordenadores de Ofertas Públicas. |