Brasil

Controles Internos para Coordenador de Ofertas Públicas de Distribuição de Valores Mobiliários

Resumo	**Política e procedimentos aplicáveis ao processo de Controle Internos para Coodenadores de Ofertas Públicas de Distribuição de Valores Mobiliários conforme regulamentação vigente**
Área emissora/Área responsável pelas atualizações	**Risk and Permanent Controls (RPC)**
Aplicabilidade	**GMD/Securitização – Distribuição de Ofertas Públicas**
Data Emissão (E) **Data Publicação (P)**	**(E) 26/06/2023** **(P) 26/06/2023**
Referência Cruzada - Textos Locais	▪ **Código de Ética** ▪ **Código de Conduta Anticorrupção** ▪ **Política Regras de Negociação e Subscrição em Valores Mobiliários** ▪ **Política de Segurança se Sistemas de Informação** ▪ **Política de Privacidade** ▪ **Política de Gestão de Continuidade de Negócios**
Número total de páginas	**09 (nove)**
Abrangência	**Banco Crédit Agricole Brasil S/A (BCAB)**
Propósito	**Atender os requerimentos regulatórios da Comissão de Valores Mobiliários (CVM) expressos em sua Resolução nº 161 de 13/06/2022**
Aprovação	**26/06/2023**

Índice

IMPORTANTE: O TEXTO A SEGUIR DESCREVE PROCEDIMENTOS LOCAIS CONFORME CONFIGURAÇÃO DO CA BRASIL, PORTANTO ELE É COMPLEMENTAR ÀS NORMAS EMITIDAS PELO GRUPO CRÉDIT AGRICOLE. PARA MAIS DETALHES, CONSULTE O RPC.

I. INTRODUÇÃO

Esta Política visa adequar o Banco Crédit Agricole Brasil S.A. (BCAB) para atender os requerimentos estabelecidos no Capítulo IV, Artigo 11 II, da Resolução emitida pela Comissão de Valores Mobiliários (CVM) nº 161, de 13 de junho de 2022, que trata sobre as regras, procedimentos e descrição dos controles internos para coordenadores de ofertas públicas de distribuição de valores mobiliários.

O documento é aplicável a todos os colaboradores que atuam na coordenação de ofertas públicas, mais especificamente, os colaboradores da equipe de Securitização e os diretores responsáveis conforme definido pela citada Resolução.

II. DEFINIÇÕES

Para fins desta Política, são aplicáveis as seguintes definições:

- "B3": Brasil, Bolsa, Balcão – Bolsa de Valores.
- "BCAB": Banco Crédit Agricole Brasil S.A.
- "BCB": Banco Central do Brasil.
- "CA-CIB": Crédit Agricole Corporate and Investment Bank.
- "Colaborador": pessoa física que possui cargo, função, posição, ou relação empregatícia, comercial, profissional, contratual ou de confiança com o BCAB, assim como estagiários e *trainees*.
- "CVM": Comissão de Valores Mobiliários.
- "*Front Office*": áreas de linha de frente que possuem contato com clientes.
- "Grupo": Grupo Crédit Agricole.
- "Linhas de Negócios": áreas de negócios do Banco Crédit Agricole Brasil S/A.
- "Políticas Globais": as Políticas e Procedimentos globais do Grupo Crédit Agricole.
- "Políticas Internas": as Politicas e Procedimentos locais do BCAB.
- "Política": a presente Política Conheça seu Cliente.
- *"RM": Relationship Manager*.

III. PROCEDIMENTOS DE COORDENAÇÃO DE OFERTAS PÚBLICAS

De acordo com a legislação, o coordenador da oferta pública deve garantir, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentos 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.

Esta Política estabelece os mecanismos adequados para controle de informações relevantes e não públicas, existência de testes periódicos de segurança e um programa de treinamento aos colaboradores sobre privacidade de informação, visando garantir o sigilo das informações durante a coordenação de ofertas públicas que abrange os ritos de Registro Automático de Distribuição e Registro Ordinário de Distribuição determinados pela CVM.

Em caso de atuação como coordenador líder de 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 por meio de canal de comunicação especifíco para esse fim.

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

Por meio de mecanismos internos, o BCAB aplica diligências utilizando criterioso processo de verificação de todos os participantes a fim de mitigar eventuais riscos regulamentares e legais, e respeitar as condições estabelecidas nas normas da CVM.

Antes que o BCAB aceite participar de qualquer transação, são realizados comitês (*Business Pipeline Committees*) pelas áreas de *Front Office* e de Crédito, em diferentes instâncias, para avaliar se a oferta pública está de acordo com as principais políticas internas e analisar a

materialidade de eventuais riscos associados. Somente após esses comitês que a participação é confirmada. Os documentos e atas dos comitês são armazenados em rede corporativa que contém a segurança necessária.

IV. BARREIRAS DA INFORMAÇÃO

Visando prevenir o uso indevido de informações sensíveis, o BCAB adota Barreiras de Informação (*Chinese Wall*) para limitar o fluxo de informações sensíveis entre as diferentes Linhas de Negócios dentro do Banco. As Barreiras de Informação consistem em um conjunto de regras destinados a restringir o acesso a informações sensíveis e permitir que as áreas do Banco continuem suas atividades de pesquisa, vendas, negociação e consultoria com relação aos instrumentos financeiros de um emissor, enquanto outra área possui informações sensíveis sobre o assunto.

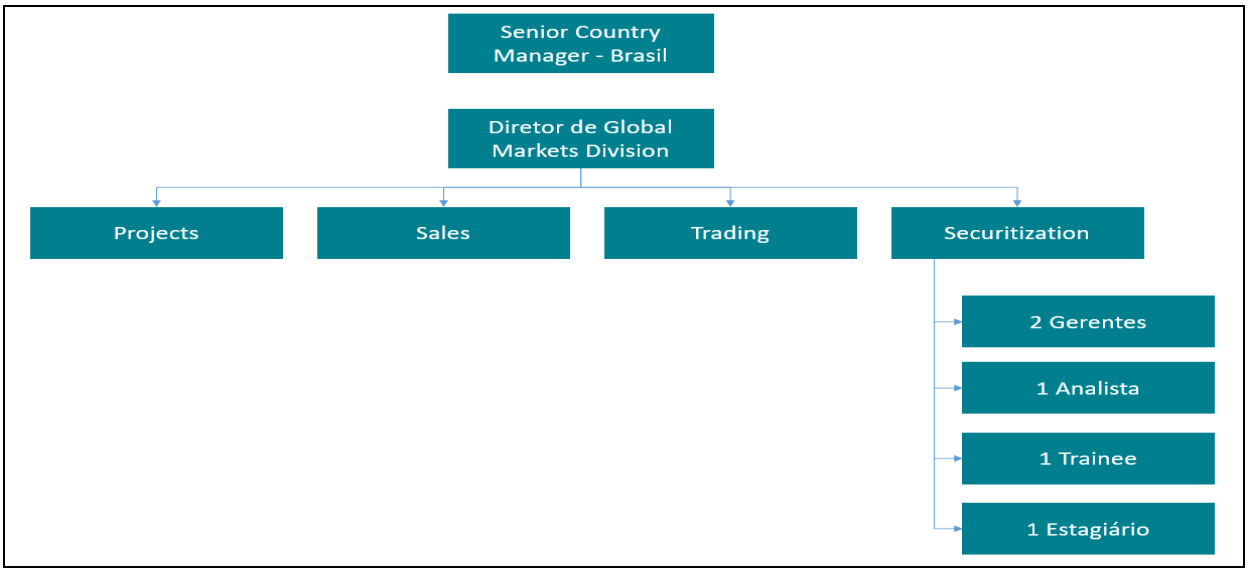
Todos os colaboradores assinam no ato da admissão e renovam anualmente, termo de compromisso em relação à confidencialidade das informações a que tiver acesso. O BCAB classifica os colaboradores de duas formas em relação às informações:

- Sensível 1 – acesso frequente à informação sensível: membros da Diretoria; colaboradores de Country Management, Global Investment Banking, Global Markets Division, Legal, Compliance e Financial Security; analistas de crédito, *relationship managers (RMs)* e colaboradores com funções similares de International Transaction Banking, Structured Finance, Financial Institutions, bem como qualquer outro colaborador que possa receber ou ter acesso à informação sensível;
- Sensível 2 – acesso ocasional à informação sensível: colaboradores da auditoria, procuradores e qualquer outro colaborador que possa receber ou ter acesso à informação sensível.

Outra forma de Barreira de Informação existente é a segregação física e lógica da área de Securitização que fica em sala com acesso restrito, feito por meio de crachá, cujos sistemas informatizados e rede coporativa são totalmente apartadas, com o objetivo de preservar a integridade e confidencialidade das informações.

V. ESTRUTURA ORGANIZACIONAL

A coordenação e execução do escopo de responsabilidades acerca das ofertas públicas de distribuição de valores mobiliários é organizada pela área de *Global Markets Division* - Securitzação, cuja estrutura atual é:



VI. CÓDIGO DE ÉTICA

O BCAB possui Código de Ética e Código de Conduta Anticorrupção que estabelecem as diretrizes de comportamento esperado de todos os colaboradores, sempre observando os mais altos padrões éticos e em linha com as políticas globais determinadas por nossa Matriz.

Todos os colaboradores tomam conhecimento dos Códigos no ato da admissão e renovam anualmente. Os documentos estão divulgados em nossa intranet e no *website* do BCAB disponível na rede mundial de computadores.

VII. CONFIDENCIALIDADE

Por meio de processos internos, há controles rigorosos a respeito da utilização de informações sensíveis recebidas, restringindo a divulgação interna para diretores, administradores, funcionários, representantes, conselho, ou outros agentes que precisem conhecê-las (*need to know*) para as finalidades da execução de suas funções e por motivos de conformidade jurídica ou de gestão de risco, sempre considerando que o BCAB instruiu todos os representantes sobre a natureza confidencial das informações.

Os documentos e informações referentes às ofertas são armazenados de acordo com os procedimentos descritos em políticas internas, com aplicação de testes periódicos de segurança/vulnerabilidade dos sistemas e infraestrutura de rede. 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.

Todo colaborador envolvido no processo é instruído a respeitar a confidencialidade profissional e seguir normas e diretrizes de controles internos para elaboração, manuseio, reprodução, divulgação, armazenamento, e descarte de informações e documentos referentes às ofertas, públicas, respeitando os níveis de proteção e de classificação da informação estabelecidos em políticas internas. Em caso de descumprimento das normas estabelecidas, os colaboradores estão sujeitos ao processo de Análise de Violações de Leis/Regulamentos/Políticas e podem ser submetidos a Comitê específico.

VIII. TESTES PERIÓDICOS

Conforme desritos em políticas internas, são realizados periodicamente, testes de segurança visando prevenir incidentes que possam causar interrupção nos negócios. Os principais testes são:

- Análise de Vulnerabilidade – visa identificar vulnerabilidades em sistemas, aplicações e infraestrtura de rede;
- Análise de Conformidade de Configurações – visa verificar se as configurações de acessos estão em conformidade e aderentes às políticas internas;
- *Penetration Testing (Pen Test)* – visa executar testes de intrusão com o objetivo de garantir a confiabilidade das ferramentas de segurança cibernética.

IX. TREINAMENTO E DESENVOLVIMENTO

O Grupo Crédit Agricole estabelece regras para a disseminação de cultura e conhecimento sobre temas de Compliance, Prevenção à Lavagem de Dinheiro, Fraudes e Segurança da Informação e Cibernética. Para isso, disponibiliza aos colaboradores, consultores e prestadores de serviços, treinamentos que visam a conscientização e o comprometimento de todos.

Com o intuito de assegurar o cumprimento dos requerimentos globais, o Grupo dispõe de ferramenta automatizada onde treinamentos e cursos são disponibilizados para aplicação periódica e obrigatória. O programa de treinamentos prevê 3 (três) campanhas anuais onde

diversos temas são aplicados aos usuários, de acordo com sua área de atuação, sendo os temas citados acima obrigatórios a todos, sem exceção.

Além disso, visando o cumprimento dos requerimentos locais exigidos pelos órgãos reguladores e/ou entidades representativas de classe, há a aplicação de treinamentos específicos, presenciais e remotos (*e-learnings*), para disseminação da legislação brasileira sobre os temas relevantes de prevenção, conformidade e confidencialidade.

O material utilizado, listas de presença e avaliações dos participantes quanto ao conteúdo ministrado nos treinamentos são arquivados pela área de Compliance.

É dever de todos participar, de forma satisfatória, dos treinamentos obrigatórios. Os casos de descumprimento são submetidos ao processo de Análise de Violações de Leis/Regulamentos/Políticas e, consequentemente, ao Comitê específico.

X. CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

O BCAB possui Política de Gestão de Continuidade de Negócios (BCP) que tem por objetivo garantir a continuidade dos processos de negócios quando os componentes que os suportam falharem em função de algum evento, ameaça ou desastre tecnológico, humano, natural e/ou físico.

Desta forma, 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. Além disso, garante a segurança dos colaboradores e dos visitantes facilitando e guiando 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, assegura a restauração das atividades, instalações e equipamentos na maior agilidade possível e garante a continuidade dos processos de negócios críticos.

X.1. Estratégias do BCP

As Estratégias de BCP são articuladas a partir de 5 (cinco) cenários de crise definidos pelo Grupo Crédit Agricole, que devem ser cobertos por todas as entidades do Grupo:

- Indisponibilidade do ambiente de trabalho: Este cenário baseia-se na indisponibilidade ou inacessibilidade, por qualquer motivo, do(s) ambiente(s) de trabalho proporcionado(s) pelo BCAB para que os colaboradores realizarem as suas atividades;
- Indisponibilidade dos usuários: Este cenário baseia-se na indisponibilidade dos colaboradores (incl. terceirizados) do BCAB, seja qual for o motivo (eventos possíveis de greve dos transportes públicos, pandemia, inundação etc.);
- Indisponibilidade física do Sistema de Informação/Datacenter: Este cenário baseia-se na indisponibilidade física, por qualquer motivo, do Datacenter ou da sala informática do BCAB (eventos possíveis de destruição física ou inacessibilidade de um datacenter ou de acesso à rede para o datacenter);
- Indisponibilidade lógica de Sistemas de Informação/Datacenter: Este cenário baseia-se na indisponibilidade lógica, por qualquer motivo, do centro de dados ou sala informática do BCAB ou de recursos utilizados em outras geografias do Grupo (eventos de ciberataque viral, intrusão, destruição acidental do armazenamento de dados, *bug* informático que afete as bases de dados);
- Perda Maciça das Estações de Trabalho: Este cenário baseia-se na indisponibilidade por qualquer motivo, de um grande número de estações de trabalho do BCAB (eventos de ciberataque viral, incêndio no local de trabalho).

X.2. Soluções do BCP

- Site de recuperação de desastre (DR Site – 'Disaster Recovery Site');
- Datacenter secundário;
- Solução de acesso remoto à rede CA-CIB usada pelo BCAB.

A descrição das soluções de BCP, bem como seu uso prático, é formalizada como parte do material de instruções de crise do BCAB e os testes com usuários. Todos são atualizados anualmente.

Os testes de BCP são realizados uma vez por abrangendo:

- Perda do Escritório Principal: Este exercício tem como objetivo simular a perda de instalações onde os colaboradores estão realizando suas atividades, com o uso do DR Site. O objetivo é validar o aspecto operacional do canteiro de recuperação com a participação de representantes das Linhas de Negócios e funções de apoio desenvolvendo atividades críticas;
- Perda do Datacenter: Este exercício tem como objetivo simular a indisponibilidade do Datacenter que hospeda a produção de TI (aplicativos e infraestrutura), com o uso do Datacenter Secundário. O objetivo é validar o aspecto operacional do plano de recuperação de TI (ativação e inicialização do ambiente de backup no prazo solicitado no BIA, 'switch' para o Datacenter Secundário).
- *Acesso remoto: Este exercício visa manter a conscientização da equipe sobre o uso de capacidades de acesso remoto (via laptops, tokens etc.), bem como confirmar o aspecto operacional da arquitetura técnica em termos de carga de conectividade.*

XI. 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 nº 161/2022 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:

- as conclusões dos exames efetuados;
- as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
- 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 BCAB e à CVM, por meio de sistema eletrônico disponível na página da CVM na rede mundial de computadores.

XII. GUARDA DE DOCUMENTAÇÕES

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

Segue abaixo a relação dos principais documentos arquivados:

- 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, e-mails de comunicação com as partes envolvidas na oferta pública, relatório de despesas, comprovante de recebimento de honorários, e outros documentos.

XIII. LEIS E REGULAMENTOS APLICÁVEIS

- Resolução CVM nº 161/2022 alterada pela Resolução CVM nº 173/2022
- Resolução CMN nº 4.968/2021