ESCOLA DE GUERRA NAVAL

CMG (IM) SANDRO BARRETO VILLELA

GESTÃO DE RISCOS:
Comparação entre os Programas de Integridade da Caixa Econômica Federal, Banco de Desenvolvimento, Banco Central do Brasil e Marinha do Brasil com foco na gestão de riscos à integridade.

Rio de Janeiro
2024

CMG (IM) SANDRO BARRETO VILLELA

GESTÃO DE RISCOS:
Comparação entre os Programas de Integridade da Caixa Econômica Federal, Banco de Desenvolvimento, Banco Central do Brasil e Marinha do Brasil com foco na gestão de riscos à integridade.

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) **FONTOURA**

Rio de Janeiro

Escola de Guerra Naval

2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria. Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Sandro Barreto Villela

Documento assinado digitalmente
gov.br
SANDRO BARRETO VILLELA
Data: 19/11/2024 15:38:47-0300
Verifique em https://validar.iti.gov.br

RESUMO

O objetivo da pesquisa é verificar se os gerenciamentos de riscos à integridade estão sendo conduzidos dentro dos Programas de Integridade da Caixa Econômica Federal, do Banco de Desenvolvimento, do Banco Central do Brasil e da Marinha do Brasil, identificando de modo comparativo as similaridades e as singularidades. Usando a pesquisa investigativa com produção de conhecimento para comprovar a execução e o monitoramento da parte teórica registrada nos planos e políticas que abordam o tema, quanto ao comprometimento e apoio da alta administração, a existência de unidades responsáveis pela implementação dos programas no órgão ou na entidade, com foco na gestão dos riscos associados ao tema da integridade e por fim como está sendo realizado o monitoramento contínuo dos atributos do programa de integridade, descrevendo as características dos itens que compõe os programas de integridade nos bancos e na Marinha do Brasil e como eles estão sendo executados, considerando a Instrução normativa conjunta do MP/CGU n.º 01, de 10 de maio de 2016 da CGU. Concluiu-se que, apesar de todo arcabouço teórico escrito pelos bancos e pela Marinha do Brasil, não há um gerenciamento de riscos adequado com todas as suas etapas bem definidas e estruturadas (Identificação, Análise, Avaliação, Monitoramento e Controle) tanto nos bancos supracitados como também na Marinha do Brasil. Apoiado nas conclusões obtidas, busca-se sustentar uma proposta de gerenciamento de riscos para a Marinha do Brasil que seja efetivamente colocada em prática.

Palavras-Chave: Programa de Integridade; Gerenciamento de Riscos; Gestão de Riscos.

ABSTRACT

The objective of the research is to verify whether integrity risk management is being conducted within the Integrity Programs of Caixa Econômica Federal, the Development Bank, the Central Bank of Brazil and the Brazilian Navy, identifying in a comparative way the similarities and singularities. Using investigative research with knowledge production to prove the execution and monitoring of all the theoretical part recorded in the plans and policies that address the topic, regarding the commitment and support of senior management, the existence of units responsible for implementing the programs in the body or in the entity, focusing on the analysis, evaluation and management of risks associated with the topic of integrity and finally how continuous monitoring of the attributes of the integrity program is being carried out. Initially, describe the characteristics of the items that make up the integrity programs in banks and the Brazilian Navy and how they are being executed, considering the CGU normative Instruction. It concluded that despite all the theoretical framework written by the banks and the Brazilian Navy, there is no adequate risk management with all its stages well defined and structured (Identification, Analysis, Evaluation, Monitoring and control) both in the aforementioned banks and also in the Brazilian Navy. Brazil. Based on the conclusions obtained, the aim is to support a risk management proposal for the Brazilian Navy that is effectively put into practice.

Keywords: Integrity Program; Risk management; Risk management

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AIC	-	Unidade de Integridade e Compliance
BCB	-	Banco Central do Brasil
CCIMAR	-	Centro de Controle Interno da Marinha
CCBCB	-	Código de Conduta dos Servidores do BCB
CCSM	-	Centro de Comunicação Social da Marinha
CEBCB	-	Comissão de Ética do Banco Central do Brasil
CEF	-	Caixa Econômica Federal
CET	-	Comissão de Ética do Sistema BNDES
CG	-	Conselho de Gestão
CISET	-	Secretaria de Controle Interno
CMN	-	Conselho Monetário Nacional
COAUD	-	Comitê de Auditoria
COFAMAR	-	Conselho Financeiro e Administrativo da Marinha
COGER	-	Corregedoria-Geral do Banco Central do Brasil
COPLAN	-	Conselho do Plano Diretor
COSO ERM	-	Comitê das Organizações Patrocinadoras/ Gestão de Riscos Empresarial
DEPES	-	Departamento de Gestão de Pessoas, Educação, Saúde e Organização
DERIS	-	Departamento de Riscos Corporativos e Referências Operacionais
DGMM	-	Diretoria Geral do Material da Marinha
DGPM	-	Diretoria Geral de pessoal da Marinha
GR	-	Gestão de Riscos
INC	-	Instrução Normativa Conjunta
MPOG	-	Ministério do Planejamento, Desenvolvimento e Gestão
ODS	-	Órgão de Direção Setorial
OE	-	Objetivo Estratégico
OGSA	-	Ordenança Geral para o Serviço da Armada
PAR	-	Programa de Aplicação de Recursos

LISTA DE ABREVIATURAS E SIGLAS (continuação)

PAR	-	Processos Administrativos de Responsabilização de Entes Privados
PGBCB	-	Procuradoria-Geral do Banco Central
PGR-BCB	-	Política de Gestão Integrada de Riscos do BCB
PMR	-	Plano de Mitigação de Riscos
RDM	-	Regulamento Disciplinar da Marinha
SAC	-	Serviço de Atendimento ao Cliente
SCIMB	-	Sistema de Controle Interno
SECET	-	Secretaria da Comissão de Ética
SEGOV	-	Secretaria de Governança, Articulação e Monitoramento Estratégico
SGM	-	Secretaria Geral da Marinha
SWOT	-	Forças (Strengths), Fraquezas (Weaknesses), Oportunidades (Opportunities) e Ameaças (Threats)
UAP	-	Unidades de Atendimento ao Público
UMG	-	Unidade de Monitoramento e Gestão

SUMÁRIO

1 INTRODUÇÃO

De acordo com o artigo 1º da Instrução Normativa Conjunta (INC) nº 1, de 16 de maio de 2016, do Ministério da Transparência e Controladoria-Geral da União (CGU) e Ministério do Planejamento, Desenvolvimento e Gestão (MPOG), “os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança. ” (CGU/MPOG, 2016, p.1)

Especificamente quanto à integridade, as entidades também ficam obrigadas a instituírem Programas de Integridade conforme artigo 19º do Decreto 9.203/2017, reforça que “com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção”, que comprometam o alcance dos objetivos estratégicos (OE) (PR, 2017, p.6).

Nesse contexto, será analisado, de modo comparativo, os Programas de Integridade na Caixa Econômica Federal (CEF), no Banco de Desenvolvimento (BNDES), no Banco Central do Brasil (BCB) e na Marinha do Brasil (MB) evidenciando as singularidades e similaridades na estrutura de governança, com foco na GR e também como se realiza a execução e o monitoramento desses programas.

A pesquisa é justificável pelo fato de que qualquer evento de risco à integridade, afetará a imagem da MB. Apenas um acompanhamento e o monitoramento dos riscos à integridade fornecerá uma segurança quanto à realização dos OE da MB.

Em consonância ao disposto na INC e no Decreto supracitados, a MB possui uma Política de Riscos e também um Plano de Integridade elaborados pelo Estado Maior da Armada (EMA) com o objetivo de fortalecer as instâncias de integridade, capacitando a gestão na identificação das incertezas e na resposta a eventos que representem riscos à integridade e questões que envolvam violações éticas.

Primeiramente e na fase investigativa, contextualizar o leitor com a Gestão de Riscos e o Programa de Integridade; apresentar um referencial teórico com os principais conceitos; posteriormente descrever os principais aspectos dos Programas de Integridade, da CEF, do BNDES, do BCB e da MB; analisar a GR à integridade estruturada (identificação, análise, tratamento, monitoramento e controle) dentro dos Programas; e verificar como a MB trata a Gestão de Risco em suas normas de Integridade, prescrevendo uma sistemática que poderia ser implementada na MB.

2 REFERENCIAL TEÓRICO

Neste capítulo será apresentado os principais conceitos utilizados neste trabalho, utilizando como referência as publicações relacionadas abaixo.

2.1 COSO ERM (COMITÊ DAS ORGANIZAÇÕES PATROCINADORAS/ GESTÃO DE RISCOS EMPRESARIAL)

Criada em 1985, por iniciativa do setor privado, independente, sem fins lucrativos, para estudar as causas da ocorrência de fraudes em relatórios financeiros.

De acordo com o COSO ERM (2004) com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização com a estrutura de gerenciamento de riscos:

> É um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos (COSO ERM, 2004).

O COSO ERM (2004) definiu oito componentes em sua estrutura (Figura nº 1), quais sejam: ambiente de controle, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta a risco, atividades de controle, informações e comunicações e monitoramento.

Figura 1- Cubo do Coso

Fonte: COSO ERM, 2004

2.1.1 Ambiente de Controle

Na estrutura organizacional interna, as atitudes e as ações dos Conselhos e da Administração são evidenciadas pelo fortalecimento dos controles internos. Está intrinsicamente ligado aos controles relacionados com os valores das pessoas e requer técnicas que confirmem o comprometimento de todos e em todos os níveis da organização (COSO ERM, 2004).

2.1.2 Fixação de Objetivos

A alta administração define os OE que devem estar alinhados à missão, compatíveis com o apetite aos riscos e divulgados a todos os membros da organização (COSO ERM, 2004).

2.1.3 Identificação de Eventos

Os eventos são situações que ocorrem e podem causar algum impacto no atingimento dos OE, eventos negativos chamados de riscos e os positivos como possíveis oportunidades.

Após a identificação dos eventos, separa-se as oportunidades dos riscos por meio da avaliação de riscos e identifica-se a forma de tratamento para cada risco, e qual o tipo de resposta a ser dada a esse risco (COSO ERM, 2004).

2.1.4 Avaliação de Risco

Requer uma abordagem sistemática para avaliar a natureza dos riscos, probabilidade de ocorrência e possíveis consequências, determinando o significado dos riscos e priorizando de acordo com a probabilidade e impacto, usando uma matriz de risco.

Implementar uma avaliação de risco eficaz ajuda a garantir que as organizações possam antecipar e responder proativamente às incertezas, minimizando impactos negativos e maximizando oportunidades (COSO ERM, 2004).

2.1.5 Resposta a Riscos

A resposta é individualizada para cada risco identificado, podendo ser: evitar, aceitar, compartilhar ou reduzir. De acordo com o COSO, “Evitar” caso nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. “Reduzir” ou “Compartilhar” reduzem o risco a um nível compatível com as tolerâncias desejadas ao risco, enquanto “Aceitar” indica que o risco esteja dentro das tolerâncias ao risco da organização (COSO ERM, 2004).

2.1.6 Atividades de Controle

São ações realizadas para tratar os riscos ao cumprimento dos OE. Alguns exemplos são: normas internas, controles físicos, segregação de funções, capacitação e treinamento, indicadores de desempenho etc. (COSO ERM, 2004).

2.1.7 Informação e Comunicação

Possibilita que todas as pessoas que fazem parte da organização possam colaborar com a coleta e a troca de informações para conduzir, gerenciar e controlar suas operações, utilizada como um canal de informações em todas as direções, do ambiente externo para o interno e vice-versa (COSO ERM, 2004).

2.1.8 Monitoramento

É o acompanhamento dos controles internos, que asseguram a adequação aos OE, ao ambiente, aos recursos e aos riscos. Deve ser monitorado e modificado continuamente por meio de medições contínuas e avaliações independentes (auditorias internas e externas) (COSO ERM, 2004).

O monitoramento ocorre nas atividades da administração. As medições e avaliações irão medir o gerenciamento dos riscos e a eficácia dos controles internos.

Podem ser realizadas por métodos como: observações, questionamentos, revisões e outros, o importante é a verificação se os controles estão implementados por toda a organização e suas subordinadas (COSO ERM, 2004).

2.2 INTEGRIDADE

A Controladoria Geral da União (CGU), uma das principais autoridades no Brasil, esclarece que a Integridade é um princípio essencial para a boa governança. Esse conceito se fundamenta na honestidade e na imparcialidade, buscando elevar os padrões de decência e correção na administração dos recursos públicos e nas atividades da instituição, refletindo tanto nos processos de decisão quanto na qualidade dos relatórios de desempenho e até nos financeiros (MP/CGU, 2016).

2.2.1 Integridade Pública

Refere-se à honestidade, ética, transparência e responsabilidade no cumprimento das tarefas, nas decisões e no comportamento dos servidores públicos. É uma qualidade essencial para garantir a confiança e o respeito da população em relação ao governo e suas instituições.

A integridade pública revela a atuação dos servidores públicos com os mais altos padrões éticos, colocando o interesse público acima de interesses pessoais ou partidários. Isso inclui a prestação de contas, a transparência nas ações e decisões, a honestidade no uso dos recursos públicos e a adesão estrita às leis e regulamentos.

A integridade é fundamental para a construção de relacionamentos saudáveis, seja em nível pessoal ou profissional. Ela contribui para a confiança mútua entre as pessoas e é uma base sólida para uma sociedade bem estruturada. Quando alguém é conhecido por sua integridade, geralmente é admirado e respeitado pelos outros (MP/CGU, 2016).

2.2.2 Programa de Integridade

É o conjunto estruturado de medidas institucionais voltadas para a prevenção, detecção, punição e remediação de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta (CGU, 2019).

2.2.3 Plano de Integridade

É um documento, validado pela alta administração, contendo todas as ações de integridade a serem cumpridas em um período de tempo determinado, normalmente ao ano, com a finalidade de prevenir, detectar e remediar os fatos de quebra de integridade, sendo revisado periodicamente (CGU, 2019).

2.2.4 Medidas de Integridade

São medidas relacionadas à ética e a integridade que se destinam à prevenção, detecção e correção dos fatos que violam a integridade. São exemplos de medidas de integridade: treinamentos, canal de denúncias, campanhas, normas internas (conflito de interesses, nepotismo, corrupção etc.).

2.2.5 Conflito de Interesse

Quando o servidor público, ao exercer funções públicas tome decisões que priorizem interesses particulares e que prejudiquem as decisões administrativas, ou que suscitem dúvidas sobre a imparcialidade que lhe é devida.

De acordo com a Recomendação do Conselho de Prevenção da Corrupção (CPC) de 8 de janeiro de 2020, a questão de conflitos de interesses no setor público tem assumido um lugar de destaque na Comunidade Internacional, a par da problemática da corrupção. Um conflito de interesses prejudica um agente público de desempenhar suas obrigações e responsabilidades.

2.2.6 Nepotismo

Vínculo de parentesco nas relações trabalhistas. O nepotismo exclui a avaliação de mérito no exercício da função pública pela influência de laços afetivos. Configura nepotismo nomear parentes para cargos em comissão, ainda que sem vínculo efetivo com a administração pública nem as funções apresentem similaridade ou impliquem subordinação hierárquica entre eles (CGU, 2018).

2.2.7 Risco para a Integridade

Ocorrência de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta, podendo comprometer os OE da organização (CGU, 2018).

2.3 GESTÃO DE RISCOS (GR)

Conforme artigo 2º da Portaria nº 915 de 12 de abril de 2017, “são os princípios, os objetivos, a estrutura, as competências e os processos formalizados para se gerenciar os riscos eficazmente (CGU, 2017).

2.3.1 Gerenciamento de Riscos

É o processo realizado para identificação, avaliação, monitoramento e controle de possíveis eventos, com o objetivo de minimizar os efeitos negativos que impeçam o alcance dos OE (CGU, 2017).

2.3.2 Controle Interno da Gestão

São todos os procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, destinados a enfrentar os riscos e proteger o alcance dos OE (CGU, 2017).

2.3.3 Medidas de Controle

São medidas para tratar os riscos, aumentando a probabilidade para o alcance dos OE e metas organizacionais (CGU, 2017).

2.3.4 Apetite a Risco

Conforme artigo 2º da Portaria nº 915 de 12 de abril de 2017, o apetite ao risco “É o nível de risco que uma organização está disposta a aceitar” (CGU, 2017).

3 ANÁLISE DOS PROGRAMAS DE INTEGRIDADE

Nesse capítulo será apresentado o atual andamento dos Programas de Integridade da CEF, do BNDES, do BCB e da MB de acordo com o Decreto Nº 9.203 de 22 de dezembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Diz o Decreto:

> Art. 19. Os órgãos e as entidades da administração direta, autárquica e fundacional instituirão programa de integridade, com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção, estruturado nos seguintes eixos:
> I - comprometimento e apoio da alta administração;
> II - existência de unidade responsável pela implementação no órgão ou na entidade;
> III - análise, avaliação e gestão dos riscos associados ao tema da integridade; e
> IV - monitoramento contínuo dos atributos do programa de integridade.
> (BCB, 2022)

Inicialmente vamos analisar a estrutura de governança pública existente nas organizações, o Decreto supracitado traz a integridade como princípio da Governança Pública (art. 3º, inciso II) e reforça a necessidade de um comitê interno de governança para auxiliar a alta administração no desenvolvimento e acompanhamento de ações que visem a melhorar o desempenho organizacional.

De acordo com o estatuto da CEF, a estrutura de governança inclui uma Diretoria Executiva que é responsável por conduzir a gestão de integridade, promover a cultura de integridade e assegurar que o monitoramento seja eficaz para mitigar riscos como conflitos de interesse, práticas de suborno, abuso de poder e tráfico de influência, visando evitar fraudes e práticas de corrupção.

No BNDES, a conduta ética dos empregados e estagiários são definidas pelo Código de ética do Sistema BNDES publicado pela alta administração. Além disso, são promovidas ações de comunicação e capacitação para fortalecer a cultura de integridade e reforçar as condutas e procedimentos esperados internamente.

A estrutura de governança do BCB está delineada na Portaria nº 104.238, de 9 de agosto de 2019 (BCB, 2019), que estabelece o Comitê de Integridade, e na Política de Conformidade (*Compliance*), definida na Resolução BCB nº 236, de 27 de julho de 2022 (BCB, 2022).

Criado para gerir a integridade no Banco Central do Brasil (BCB), o Comitê de Integridade é responsável pela coordenação do Programa, estruturação, execução e monitoramento do Plano de Integridade, identificação de vulnerabilidades e promoção de ações corretivas. Com o Decreto nº 11.529, de 16 de maio de 2023, o Comitê de Integridade passou a atuar como Unidade Setorial, colaborando com outros órgãos do Poder Executivo Federal sob a coordenação da CGU para aprimorar práticas de integridade pública (BCB, 2023).

O Comitê de Integridade é composto pelo Secretário-Executivo, que atua como coordenador, pelos chefes das unidades responsáveis pelo planejamento e implementação de assuntos relacionados à integridade, e pelo Secretário da Comissão de Ética do BCB (BCB, 2023).

A MB tem uma estrutura de governança complexa, que inclui diversos órgãos e hierarquias, sendo o EMA, o órgão responsável por assistir o Comandante da Marinha nas atribuições relacionadas ao planejamento, à coordenação e ao controle das atividades navais, procurando absorver e aprimorar as boas práticas de governança como conformidade, *accountability*, transparência, controle interno e correição.

Todas as organizações possuem uma estrutura adequada de governança pública para o cumprimento do decreto supracitado e para o bom andamento dos Programas de Integridade.

Nesse capítulo será analisado o comprometimento da alta administração com o Programa de Integridade a partir da análise de informações, como Regimentos internos e organogramas, para confirmar a existência de uma estrutura interna de governança, comprovar a existência de segregação de funções na tomada de decisão em processos críticos, comprovar a instituição de mecanismos para seleção, formação e avaliação de líderes, normativos internos que determinem a criação do Programa de Integridade contendo o Plano de Integridade, o gerenciamento de riscos, comunicados ao público interno e externo, treinamentos de integridade (verificação da participação da alta administração) e relatórios de monitoramento e avaliação do Programa de Integridade.

3.1 COMPROMETIMENTO E APOIO DA ALTA ADMINISTRAÇÃO

A introdução da GR e a contínua eficácia requer forte comprometimento por parte da alta administração, à qual convém: a) aprovar uma política de GR; b) assegurar o alinhamento da cultura da organização; e c) atribuir responsabilidades nos níveis apropriados.

Conforme o artigo 4º do Decreto nº 9.203/2017, é uma diretriz da governança pública “fazer incorporar padrões elevados de conduta pela alta administração para orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades”. (PR, 2017)

Todas as medidas de integridade implementadas pela estrutura de governança e alta administração irão demonstrar um forte comprometimento com a melhoria contínua do Programa de Integridade.

Segundo o Programa de Integridade da CEF (2021), a liderança ética adota medidas para prevenir, identificar e corrigir violações à integridade, influenciando tanto o comportamento dos subordinados quanto o ambiente organizacional. O sucesso de um Programa de Integridade depende necessariamente do comprometimento da Alta Administração, bem como da implementação e aperfeiçoamento contínuo de ações de prevenção e combate à corrupção.

A CEF inclui dentre seus objetivos empresariais "Fortalecer a governança e a eficiência operacional" e "Humanizar as relações de trabalho na CAIXA". Esses objetivos visam fortalecer o conglomerado CEF por meio da aplicação das melhores práticas de governança e integridade, confirmando que a existência de um Programa de Integridade é essencial para alcançar esses objetivos.

A Alta Administração do BNDES é composta pelo presidente, diretores e membros dos demais órgãos colegiados estatutários das empresas do Sistema BNDES e o comprometimento é percebido pelo apoio visível e inequívoco ao Programa de Integridade.

No BNDES, são realizados procedimentos de verificação de antecedentes de integridade para membros estatutários e assessores externos, com o objetivo de subsidiar a contratação e a eleição ou nomeação de membros dos colegiados do Sistema BNDES (Diretoria Executiva, Conselhos de Administração, Conselhos Fiscais, Comitê de Auditoria, Comitê de Riscos e Comitê de Pessoas, Elegibilidade, Sucessão e Remuneração) (BNDES, 2020).

O BNDES busca um ambiente ético, responsável e de conduta íntegra entre as pessoas envolvidas no processo. Além disso, estabelece diretrizes e atribuições para fortalecer a integridade no Sistema BNDES, com o objetivo de prevenir, detectar e remediar ocorrências de corrupção, desvios, fraudes, irregularidades e outros atos ilícitos, tanto no país quanto no exterior, em conformidade com as leis brasileiras e estrangeiras aplicáveis. O compromisso do Sistema BNDES é reforçado pela cooperação proativa com iniciativas nacionais e internacionais de integridade, em todas as suas formas (BNDES, 2020).

Para o BNDES, integridade significa atuar com base em valores, princípios éticos e na prevenção de práticas ilegais, abrangendo duas principais dimensões: o combate a fraudes, focado em prevenir, detectar e remediar desvios, irregularidades e atos ilícitos praticados contra a instituição ou terceiros, incluindo corrupção, apropriação indébita de ativos e demonstrações fraudulentas; e a prevenção à lavagem de dinheiro e o combate ao financiamento do terrorismo. As diversas medidas adotadas para manter um ambiente íntegro compõem o Programa de Integridade do BNDES (BNDES, 2020).

Desde o início do primeiro Programa de Integridade em outubro de 2018, o BCB vem incorporando as melhores práticas de integridade, congregando esforços das diversas áreas envolvidas no tema, com amplo respaldo e irrestrito comprometimento da alta administração da Autarquia, aprovou o Programa de Integridade e o Comitê de Integridade se reporta diretamente ao Comitê de Governança, Riscos e Controles (GRC), composto pelos membros da Alta Administração do BCB (BCB, 2017a/2017b).

Na MB o Programa de Integridade conta com o comprometimento da Alta Administração Naval, com a implementação e a continuidade de ações de prevenção e combate à corrupção e o fomento ao ambiente de integridade, cabendo a todas as Organizações Militares (OM) da MB conhecer e implementar as práticas do “Integridade Naval”, visando coibir fraudes, corrupção, irregularidades e desvios de conduta.

Não há dúvida sobre o comprometimento e apoio da alta administração para o bom estabelecimento de um Programa de Integridade, todas as organizações comprovaram haver documentos e estrutura interna de governança, compostos por conselhos ou comitês, auditoria interna, corregedoria interna, ouvidoria interna e comissão de ética, segregação de funções para a tomada de decisão em processos

críticos, normativos internos que determinaram a criação do Programa de Integridade, contendo o Plano de Integridade.

Esse apoio foi comprovado, é visível e inequívoco ao Programa de Integridade, praticar a liderança de modo a influenciar o comportamento do pessoal envolvido, disseminar a cultura de integridade por meio da divulgação do Programa tanto para o público interno como também para o público externo, manter o acompanhamento do Plano de Integridade, possuir conduta ética exemplar, evidenciada por meio de suas ações e decisões e em treinamentos, conferências, workshops, palestras (como palestrantes ou ouvintes) de forma a ajudar a organização a reforçar os seus valores.

3.2 EXISTÊNCIA DE UNIDADE RESPONSÁVEL E INSTÂNCIAS DE INTEGRIDADE

Este item relaciona as unidades responsáveis e as instâncias de integridade e as ações sob sua responsabilidade, com o objetivo de identificar oportunidades de aprimoramento no desempenho das atividades das instâncias do Programa de Integridade.

No Programa de Integridade da CEF (2021), é definido que as unidades responsáveis pelos mecanismos e procedimentos que constituem o programa são denominadas protocolos de integridade. Estas unidades estabelecem diretrizes normativas, mantêm atualizadas, assegura o seu cumprimento, implementando ações necessárias para seu aprimoramento e monitoramento, define claramente as responsabilidades e fornece informações para a gestão do Programa. Também é parte do Programa de Integridade garantir que as instâncias atuem de forma conjunta e coordenada, visando minimizar os potenciais riscos de integridade.

No BNDES, a instância que é responsável pela aplicação do Programa de Integridade possui independência, é bem estruturada e tem autoridade para contribuir com a gestão da ética no Sistema BNDES.

O Comitê de Governança, Riscos e Controles (GRC) do BCB é a instância decisória do Plano de Integridade, devido à sua competência para definir diretrizes e estratégias, bem como adotar medidas para a sistematização de práticas relacionadas à gestão de riscos e aos controles internos. A composição do GRC coincide com a da Diretoria Colegiada, composta pelo Presidente e Diretores, conforme estipulado na Portaria nº 93.608 do BCB (BCB, 2017b).

Criado como instância específica para a gestão da integridade no BCB, o Comitê de Integridade tem como atribuição, a coordenação do Programa, a estruturação, execução e monitoramento do Plano de Integridade. Isso inclui a identificação de vulnerabilidades à integridade nos trabalhos desenvolvidos pelo Banco, propondo, em conjunto com outras unidades, medidas para a promoção de ações relacionadas à gestão da integridade (BCB, 2017b).

O Comitê de Integridade atua como Unidade Setorial de Integridade Pública, compondo, em conjunto com os demais órgãos do Poder Executivo Federal, e sob a coordenação da Controladoria Geral da União (CGU), um sistema de informações e de aprimoramento das práticas de integridade pública.

Na MB, o EMA foi instituído como a Unidade Gestora de Integridade (UGI), em cumprimento ao Decreto nº 9.203/2017 e a Portaria nº 57/2019, da CGU ficando responsável por coordenar a estruturação, a execução e o monitoramento do Programa de Integridade, cabendo a todas as OM implementarem as ações contidas neste Plano, visando o combate a fraudes, atos de corrupção, irregularidades e desvios de conduta.

As instâncias de Integridade avaliam se a estrutura organizacional está adequada ao tamanho, complexidade, ao perfil de risco, observando as melhores práticas de governança, se atende às normas internas e externas, se as condições são favoráveis ao alcance dos resultados. Para cumprir essa responsabilidade, as UGI, os Comitês Internos de Governança contam com o apoio da Comissão de Ética, da Ouvidoria Interna, da Corregedoria Interna, da Auditoria Interna e do próprio Controle Interno que deve acompanhar e monitorar todo o processo.

3.2.1 Comissão de Ética

A Comissão de Ética é uma entidade deliberativa cuja principal função é promover os princípios da conduta ética entre os servidores. Compete a esta comissão orientar, supervisionar e atuar como instância consultiva para a alta administração, além de acolher e analisar denúncias feitas pelos servidores.

No contexto do Programa de Integridade da CEF (2021), a Comissão de Ética é um órgão autônomo de caráter deliberativo, encarregado de orientar, aconselhar e gerir a ética profissional dos dirigentes, bem como assegurar o tratamento ético no

relacionamento com as pessoas e na administração do patrimônio público. Além disso, esta comissão tem a responsabilidade de deliberar sobre comportamentos antiéticos e violações das normas da CEF que sejam reportadas.

A gestão da ética no Sistema BNDES é conduzida pela Comissão de Ética do Sistema BNDES (CET/BNDES) e pela Secretaria da Comissão de Ética (SECET/BNDES), de acordo com a legislação pertinente, em especial o Decreto nº 6.029, de 1º de fevereiro de 2007, e a Resolução nº 10, de 29 de setembro de 2008, da Comissão de Ética Pública (CEP), vinculada à Presidência da República.

O BNDES possui padrões de conduta e um código de ética aplicáveis a todos os participantes do Sistema BNDES, independentemente do cargo ou função exercidos. Esses padrões e o código são incluídos nos editais de licitação e nos contratos administrativos, de modo que os representantes legais e os profissionais das empresas prestadoras de serviços assumam a obrigação de respeitar essas disposições (BNDES, 2020).

Segundo o Plano de Integridade do Banco Central do Brasil, a promoção da ética e das regras de conduta é responsabilidade da Comissão de Ética do Banco Central do Brasil (CEBCB). Esta comissão, cujo Regimento Interno foi instituído pela Resolução BCB nº 165, de 23 de novembro de 2021, possui várias funções, incluindo a orientação dos servidores e colaboradores sobre ética no trato com pessoas e com o patrimônio público, a promoção da disseminação de valores, princípios e normas relacionados à conduta ética, e a divulgação do Código de Conduta dos Servidores do BCB (CCBCB). Este código, aprovado pela Diretoria, detalha as condutas esperadas dos servidores da autarquia, oferece diretrizes sobre ética profissional e dissemina conceitos sobre ética pública. Constitui um dos principais instrumentos de promoção da ética no BCB, e por isso, esforços de publicação e comunicação estão previstos no atual ciclo do Plano de Integridade (BCB, 2021a; 2021b).

Para complementar, a autarquia disponibiliza uma lista de perguntas frequentes para mitigar possíveis dúvidas dos servidores sobre como proceder em situações específicas, que abordam temas como o exercício de atividades paralelas, o recebimento de brindes e presentes, e a participação em eventos externos. No atual plano de integridade, está prevista uma ação para revisar a seção de perguntas e respostas da página da CCBCB na intranet, com base no novo Código de Conduta.

A autarquia também atua na prevenção de conflitos de interesse, contendo em seu Código de Conduta, os conceitos de conflito de interesses potencial e aparente.

Nesse contexto, a Corregedoria-Geral do Banco Central do Brasil (COGER) é responsável pelo cumprimento da Lei de Conflito de Interesses (Lei nº 12.813, de 16 de maio de 2013) no âmbito da instituição. A COGER realiza a análise preliminar de consultas de servidores sobre a existência de conflitos em situações concretas e individualizadas e de pedidos de autorização para o exercício de atividades de interesse particular (BCB, 2021b).

Visando promover e reforçar relacionamentos de trabalho positivos, atuar na prevenção e intervenção em prol da saúde mental dos servidores, consta do Plano de Integridade ações relativas ao Programa Cultura de Paz, desenvolvidas pelo Departamento de Gestão de Pessoas, Educação, Saúde e Organização (DEPES). Por fim, consta do atual plano uma ação sob responsabilidade da Secretaria de Governança, Articulação e Monitoramento Estratégico (SEGOV) voltada para a promoção de medidas de integridade para processos com maior risco para integridade no BCB.

Na MB os militares estão submetidos aos princípios éticos e às normas de conduta previstas, na Lei n° 6.880/1980 – que dispõe sobre o Estatuto dos Militares (EM), o Decreto nº 88.545/83 – Regulamento Disciplinar da Marinha (RDM) e Decreto nº 95.480/87 – Ordenança Geral para o Serviço da Armada (OGSA), sendo as infrações apuradas no âmbito das Organizações Militares.

Além disso, é observado o contido na DGPM-315 e, no que couber, as Regras de Conduta e Convivência entre militares da Marinha (Marinha, 2011).

O artigo 28º, do EM prevê que o sentimento do dever, o pundonor militar e o decoro da classe impõem, a cada um dos integrantes das Forças Armadas, conduta moral e profissional irrepreensíveis, com a observância de preceitos de ética militar.

A Comissão de Ética no âmbito da MB se aplica aos servidores civis e também observa o contido no Decreto nº 6.029/2007 – que instituiu o Sistema de Gestão da Ética do Poder Executivo Federal e a Resolução nº 10/2008, da Comissão de Ética Pública.

No tocante aos princípios éticos a serem seguidos pelos servidores civis deverá ser observado o Decreto n° 1.171/1994 – que estabeleceu o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

Em razão disso, compete à Comissão de Ética dos Servidores Civis da MB, instituída pela Portaria nº 59/DGPM/2021, o exame e julgamento de prática de ato, por servidores civis da MB, em respeito ao preceituado no Código de Ética Profissional

do Servidor Público Civil do Poder Executivo Federal, observando-se, para tanto, os procedimentos descritos na referida publicação.

Corroborando com o comprometimento da alta administração, houve a instituição das Comissões de Ética nas entidades, dotadas de condições de funcionamento, estrutura, corpo funcional e prerrogativas apropriadas às suas respectivas funções com recursos necessários ao cumprimento de suas obrigações (humanos, materiais e financeiros) e com os Códigos de Conduta formalizados.

3.2.2 Ouvidoria Interna

As atividades de ouvidoria, contribuem para o pleno exercício da consciência crítica, cabendo-lhe receber, tratar e responder as manifestações dos militares/servidores.

O “e-Ouv/Simplifique!” é o sistema informatizado que permite a qualquer cidadão reclamar, sugerir, denunciar, elogiar, solicitar providências e propor simplificação de serviços às ouvidorias.

Segundo o Programa de Integridade da CEF (2021), as denúncias podem envolver uma variedade de questões, como assédio, abuso de poder, discriminação, retaliação, conduta sexual inadequada, comunicação verbal ou escrita imprópria, corrupção, lavagem de dinheiro e financiamento ao terrorismo, conflito de interesses, nepotismo, desvio de recursos, uso indevido de informações (fraude interna) ou qualquer indício de irregularidade, seja por ação ou omissão.

A CEF disponibiliza um Canal de Denúncias que é externo e independente, destinado a receber informações sobre práticas irregulares ou atos ilícitos relacionados à conduta de seus empregados, independentemente do cargo ou função. A solução dessas denúncias depende das unidades apuratórias internas da CEF (CAIXA, 2021).

A Ouvidoria do BNDES, criada em 2003, tem desempenhado um papel importante no fortalecimento do diálogo entre a sociedade e as áreas internas do banco. A ouvidoria presta os esclarecimentos necessários aos cidadãos (tanto internos quanto externos) e sugere à alta administração melhorias nas normas e procedimentos a partir da análise das manifestações recebidas. Operando de forma autônoma, imparcial e sigilosa, a ouvidoria acolhe e responde demandas, além de

induzir reflexões e melhorias na instituição. Por meio do debate dos anseios dos cidadãos com as demais áreas do banco, a ouvidoria contribui para a construção de um ambiente que valoriza o diálogo, o aprimoramento do processo democrático e a inclusão social.

No Plano de Integridade do BCB (2021a) consta que são disponibilizados canais para recepção de denúncias sobre irregularidades cometidas por seus servidores e colaboradores, acessíveis tanto ao público interno quanto ao externo. As denúncias podem ser registradas através de diversos canais de atendimento da Ouvidoria, como a página do Banco Central na internet, a intranet do BCB, formulários em papel, correspondências, telefone da Central de Atendimento ao Público, ou ainda presencialmente. Após o recebimento das denúncias, a Ouvidoria, preservando o sigilo necessário, encaminha as informações para tratamento pelas unidades competentes: a Corregedoria-Geral do Banco Central do Brasil (COGER), se o denunciado for integrante da carreira de especialista (cargo de Analista ou Técnico), ou a Procuradoria-Geral do Banco Central (PGBCB), se o denunciado for integrante da carreira de procurador. Se a denúncia estiver relacionada a transgressões de natureza ética, a COGER ou a PGBCB, conforme o caso, poderão encaminhá-la à Comissão de Ética do Banco Central do Brasil (CEBCB).

Além da Ouvidoria, as denúncias podem ser encaminhadas diretamente à Corregedoria, à PGBCB ou à CEBCB, conforme o caso, mediante entrada por meio de protocolo nos setores de atendimento ao público, na sede e nas representações regionais da autarquia, ou por meio de mensagens enviadas aos canais próprios da COGER (coger@bcb.gov.br) ou da CEBCB (etica@bcb.gov.br).

É importante ressaltar que, embora a legislação exija que as denúncias contenham a identificação e o endereço do denunciante, são aceitas denúncias anônimas. Essas denúncias anônimas só levarão à instauração de procedimentos se houverem elementos mínimos que indiquem a veracidade dos fatos.

Para integrantes da MB, para os servidores civis e prestadores de serviços, orienta-se procurar o seu superior hierárquico ou utilizar a Plataforma Integrada de Ouvidoria e Acesso à Informação – “Fala.BR”, o que lhe for mais conveniente.

Cabe salientar, que em atendimento ao Decreto nº 9.492/2018, que instituiu o Sistema de Ouvidoria do Poder Executivo Federal (e-Ouv), o CCSM é o responsável pelas respostas às manifestações da ouvidoria da MB (sugestões, denúncias, reclamações, solicitações de providências, elogios e propostas de simplificação de

serviços públicos), que deverão ser registradas na Plataforma Integrada de Ouvidoria e Acesso à Informação – Fala.BR.

Adicionalmente, como previsto no Decreto nº 10.153 (2019), as informações dos denunciantes de ilícitos e de irregularidades estão plenamente salvaguardadas, de modo a preservar o sigilo daquele que denuncia.

Todas as entidades possuem um canal de ouvidoria para atendimento das inquietudes dos clientes.

3.2.3 Corregedoria Interna

O principal objetivo é zelar pela integridade, pela transparência e pelo bom funcionamento da instituição, além de promover a responsabilização dos indivíduos que violarem as normas internas ou cometerem condutas impróprias.

As atribuições específicas de uma corregedoria podem variar dependendo da instituição e do contexto em que está inserida, mas geralmente incluem a investigação de denúncias de irregularidades, a aplicação de medidas disciplinares, o acompanhamento de processos administrativos e a proposição de políticas e procedimentos para prevenir futuras infrações. Desempenha um papel fundamental na garantia da legalidade, da transparência e da ética no funcionamento de uma instituição, fortalecendo a confiança pública e as instituições democráticas.

Instituída em 2015, a Corregedoria da CAIXA tem como atribuição supervisionar a correção das atividades tributárias e da conduta dos empregados e membros da instituição. Este trabalho é realizado tanto de maneira preventiva quanto pedagógica, incluindo a proposta de melhorias nas atividades e processos de trabalho. Além disso, a Corregedoria é encarregada da execução dos Processos Administrativos de Responsabilidade de Entes Privados (PAR), conforme a Lei nº 12.846 (CN, 2013a), conhecida como Lei Anticorrupção. Esta unidade responde diretamente ao Conselho de Administração da empresa.

A Corregedoria do BNDES, subordinada ao Presidente da instituição e liderada pelo Diretor de *Compliance*, atualmente está administrativamente integrada na estrutura da Área de Integridade e *Compliance*. A unidade é composta pelo Corregedor, que chefia a Corregedoria, e por sua equipe permanente.

Para a execução de investigações e processos de apuração, são formadas comissões com empregados do BNDES, que podem ser integrantes da equipe permanente da corregedoria ou selecionados de uma lista formalizada por ato do Presidente do BNDES. Os empregados indicados para essa lista devem atender aos mesmos critérios exigidos para os membros da Equipe Permanente da Corregedoria.

Na perspectiva da transparência, consta do atual ciclo um conjunto de ações sob responsabilidade de implementação da Corregedoria-Geral do BCB, voltadas para a reformulação das informações da Corregedoria disponíveis na intranet e internet, a criação de conteúdo relativo a conflito de interesses e divulgação na página do BCB na internet, bem como a elaboração e publicação, na intranet, de ementário de decisões sobre conflito de interesses.

A Corregedoria-Geral do BCB é responsável por prevenir e investigar irregularidades atribuídas aos servidores da carreira de Especialista da instituição. Integrando o Sistema de Correição do Poder Executivo Federal, a unidade pode instaurar sindicâncias disciplinares acusatórias, que podem resultar na aplicação de advertências. Além disso, também são instaurados Processos Administrativos Disciplinares (PAD) que podem culminar na aplicação de penalidades aos servidores envolvidos.

Na MB, a Secretaria de Controle Interno (CISET) do Ministério da Defesa é responsável por conduzir inspeções administrativas e realizar correições tanto programadas quanto extraordinárias. Sua função é verificar o cumprimento, por parte dos gestores, do ordenamento jurídico nacional e das normas internas, além de fornecer orientação e consultoria quando necessário. A CISET também promove a apuração formal de possíveis irregularidades e transgressões, aplicando as penalidades cabíveis.

Todas as organizações estão alinhadas com o Guia de Integridade Pública da CGU, que institui uma Unidade de Correição dedicada a realizar essa tarefa. Na Marinha, por exemplo, cada OM é uma Unidade de Correição e é responsável pelos procedimentos de responsabilização, com exceção do Processo Administrativo de Responsabilização (PAR) – pessoa jurídica, que é de competência do Comandante da MB. A apuração de fatos (acontecimentos) e atos (documentos) é realizada por meio de sindicâncias, processos administrativos disciplinares e inquéritos policiais militares.

3.2.4 Auditoria Interna

Conforme a Instrução Normativa da CGU nº 03, de 9 de junho de 2017, e Instrução Normativa da CGU nº 08, de 6 de dezembro de 2017, a auditoria interna verifica o funcionamento dos controles internos e o cumprimento das recomendações de auditoria realizada por órgãos externos. (CGU, 2017a; CGU, 2017b)

A Auditoria Interna da CEF, em conformidade com a Lei nº 13.303/2016 (Lei das Estatais) e o Decreto nº 8.945/2016, oferece análises, recomendações e informações que auxiliam na administração do desempenho de suas funções e responsabilidades. Realiza avaliações periódicas sobre a eficácia dos sistemas de controles internos e dos principais riscos associados às suas atividades. A função de *Compliance* na CEF é independente das atividades de negócios e da unidade de auditoria interna para evitar potenciais conflitos de interesse através da segregação de funções.

Os riscos de *compliance* são identificados, monitorados e avaliados periodicamente pelas auditorias interna e externa, sendo acompanhados de maneira sistemática e oportuna à Alta Administração da CEF, conforme necessário.

A Auditoria Interna também apoia os trabalhos de auditoria e fiscalização realizados por órgãos de controle, fiscalização, agente supervisor e auditoria independente (CAIXA, 2023).

Pela Política Corporativa de Gestão de Continuidade de Negócios do Sistema BNDES é utilizado o conceito de camadas ou linhas de defesa para a gestão de risco operacional e controle interno, sendo a terceira linha de defesa representada pela Auditoria Interna. Esta tem a função de avaliar de forma objetiva a integridade e adequação do sistema de controle interno, da gestão de riscos e da governança corporativa do Sistema BNDES, além de realizar a interlocução com os órgãos externos de controle e fiscalização. Faz parte do Sistema de Controle Interno do Poder Executivo Federal e atua como órgão técnico de assessoramento e consultoria para os membros dos Conselhos de Administração e Fiscal do Sistema BNDES (BNDES, 2023).

Além disso, compete ao Comitê de Auditoria (COAUD) do Sistema BNDES: a) elaborar, conforme seu Regimento Interno, relatórios sobre as atividades, resultados, conclusões e recomendações do Comitê, incluindo uma avaliação da efetividade do sistema de controle interno, destacando as deficiências identificadas conforme a

legislação vigente; b) supervisionar as atividades desenvolvidas nas unidades de controle interno do Sistema BNDES; e c) avaliar e monitorar as exposições a riscos operacionais, bem como a qualidade e integridade dos mecanismos de controle interno (BNDES, 2023).

A Auditoria Interna do Banco Central do Brasil (BCB) avalia o processo de gerenciamento de riscos por meio de procedimentos de auditoria e auditorias nos departamentos. Dessa forma, contribui para o fortalecimento da gestão de riscos do BCB e da melhoria de todo o processo.

Na MB, o Sistema de Controle Interno (SCIMB), assim como o BNDES, alinha-se ao modelo de “Três Linhas de Defesa”, o qual deve comunicar as responsabilidades de todos os envolvidos, provendo uma atuação coordenada e eficiente, sem sobreposições ou lacunas, como disposto na Instrução Normativa nº 3/2017, da CGU (CGU, 2017a).

A “Terceira Linha de Defesa” é representada pelo Centro de Controle Interno da Marinha (CCIMAR), prestando serviços de auditoria e consultoria independente, autonomia técnica e objetividade, visando manter e melhorar os processos de governança, gerenciamento de riscos e controles internos das OM.

A auditoria interna é primordial, além de subsidiar a administração das organizações, também colabora e interage com os órgãos de controle, de fiscalização e de supervisão.

3.2.5 Controle Interno

Segundo a Instrução Normativa nº 3/2017, da CGU diz que a estrutura de controle interno deve contemplar as três linhas de defesa de gestão a seguir, especificando todas as responsabilidades dos setores envolvidos.

A primeira linha de defesa envolve os controles primários, que devem ser estabelecidos e mantidos pelos gestores responsáveis. Esta linha deve identificar, avaliar, controlar e mitigar os riscos, orientando o desenvolvimento e a implementação de procedimentos internos para garantir que as atividades sejam realizadas conforme as metas e objetivos estabelecidos (CGU, 2017a).

A segunda linha de defesa tem como objetivo assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de maneira

apropriada. Esta instância apoia o desenvolvimento dos controles internos da gestão e realiza atividades de supervisão e monitoramento das atividades da primeira linha de defesa, incluindo gerenciamento de riscos, conformidade, verificação de qualidade, orientação e treinamento (CGU, 2017a).

A terceira linha de defesa é representada pela atividade de auditoria interna governamental, que oferece serviços de avaliação e consultoria com base nos princípios de autonomia técnica e objetividade (CGU, 2017a).

O Programa de Integridade da CEF (2021) implementa e mantém continuamente sistemas de controles internos adequados. Além disso, promove ações internas para disseminar a importância desses sistemas e o engajamento de cada funcionário nos processos relacionados.

A eficácia do Sistema de Controles Internos da CEF é avaliada e monitorada periodicamente por meio da definição de responsabilidades com base no modelo das três linhas de defesa. O gerenciamento de riscos é estruturado com papéis e responsabilidades específicos, cobrindo o gerenciamento de riscos e o ambiente de controle, com atividades de controle definidas para todos os níveis de negócios, processos e riscos identificados (CAIXA, 2023).

A gestão de risco operacional e controle interno do Sistema BNDES é orientada pelas Resoluções CMN nº 4.557, de 23/02/2017, e nº 4.968, de 25/11/2021. O Sistema BNDES adota o conceito de camadas ou linhas de defesa para a gestão de risco operacional e controle interno:

a) A primeira linha de defesa é formada pelos gestores dos processos das diversas unidades do Banco, que são responsáveis por gerir os riscos operacionais dos processos em que atuam e por definir e manter controles adequados;

b) A segunda linha de defesa é composta pela Área de Integridade e Compliance, que apoia os gestores na identificação e avaliação dos riscos operacionais e dos controles correspondentes, dissemina a cultura desses temas e se reporta à estrutura de governança. Outras unidades que realizam atividades semelhantes dentro de suas atribuições também fazem parte desta linha; e

c) A terceira linha de defesa é representada pela Auditoria Interna, que tem a função de avaliar de forma objetiva a integridade e adequação do sistema de controle interno, da gestão de riscos e da governança corporativa do Sistema BNDES. Além disso, realiza a interlocução com os órgãos externos de controle e fiscalização, integrando o Sistema de Controle Interno do Poder Executivo Federal e atuando como

órgão técnico de assessoramento e consultoria para os membros dos Conselhos de Administração e Fiscal do Sistema BNDES (BNDES, 2023).

O BCB instituiu por meio da Resolução BCB nº 333, de 10 de agosto de 2023, que divulga a Política de Controle Internos com o objetivo de estabelecer princípios, diretrizes e responsabilidades para a sistematização dos controles internos e para a integração das informações, fortalecer a governança e estimular a cultura de controle interno na instituição (BCB, 2023a).

O SCIMB alinha-se ao modelo de “Três Linhas de Defesa”, o qual deve comunicar, de maneira clara, as responsabilidades de todos os envolvidos, provendo uma atuação coordenada e eficiente, sem sobreposições ou lacunas, como disposto na Instrução Normativa nº 3/2017, da CGU (CGU, 2017a).

A “Primeira Linha de Defesa”, composta por cada OM da MB, de acordo com a Instrução Normativa nº 3/2017, da CGU é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos destinados a garantir que as atividades sejam realizadas de acordo com as metas e objetivos da OM. Contempla os controles internos, que devem ser instituídos e mantidos pelos Agentes Responsáveis (Ordenador de Despesa, Agente Fiscal e Gestores) e o Conselho de Gestão, durante a execução de atividades e tarefas (CGU, 2017a).

A “Segunda Linha de Defesa” é composta pelo EMA, ODS, representados pelas suas Assessorias de Controle Interno, e suas respectivas Diretorias Especializadas. Tem por objetivo apoiar o desenvolvimento dos controles internos da gestão e realizar as atividades de supervisão e de monitoração das ações desenvolvidas no âmbito da “Primeira Linha de Defesa”, que incluem o gerenciamento de riscos, integridade, conformidade, controle orçamentário-financeiro, operacional, orientação e treinamento. O COFAMAR e o COPLAN também integram a “Segunda Linha de Defesa” (CGU, 2017a).

A “Terceira Linha de Defesa” é representada pelo CCIMAR, como já descrito anteriormente.

As estruturas de controle interno das organizações contemplam as três linhas de defesa de gestão e especificam todas as responsabilidades dos setores envolvidos.

3.3 GERENCIAMENTO DOS RISCOS ASSOCIADOS AO TEMA DA INTEGRIDADE

Cabe ao gerenciamento de risco à Integridade identificar riscos relacionados a corrupção, fraudes, irregularidades, desvios éticos e de conduta que impactem a organização, comprometendo assim os valores e padrões e seus OE.

Os eventos de risco que não afetam os OE, sejam eles conhecidos ou desconhecidos, não são preocupantes para quem realiza o gerenciamento de riscos.

O gerenciamento de riscos age de forma proativa, face aos eventos de risco inerentes a qualquer atividade que tenham pessoas, aumentando a probabilidade e o impacto da ocorrência de riscos.

Os eventos de risco à integridade não podem ser completamente eliminados, portanto é crucial gerenciá-los de maneira eficaz. Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT-2018) e vários autores, um evento de risco possui duas componentes principais: a probabilidade de ocorrência e o impacto indesejável. Para administrar esses eventos, é essencial conhecer, tratar e monitorar.

Autores concordam que o gerenciamento de risco segue um processo sequencial e cíclico, começando com a identificação dos riscos, seguida pela avaliação e, por fim, pela definição de estratégias para tratá-los. De acordo com Baker, Ponniah e Smith (1999), o processo de gerenciamento de riscos comumente envolve três etapas: análise, avaliação e controle, que são iterativas e contribuem para um ambiente de risco controlado. Clark, Pledger e Needler (1990) também dividem o processo em três estágios: identificação, análise e gestão da resposta.

Segundo o *Project Management Institute* (2004), o gerenciamento de risco começa com uma fase de preparação, na qual são definidas a abordagem e a execução das atividades de gerenciamento de risco, adaptadas à importância para a organização. Durante o planejamento, são estabelecidas abordagens, considerações específicas da empresa, equipe e metodologia, e são clarificadas as fontes de dados essenciais para o processo decisório.

Embora abordado de maneiras diferentes, a maioria dos autores concorda que o gerenciamento de riscos envolve as fases de planejamento, identificação de eventos de risco, avaliação com base na probabilidade e impacto, um plano de resposta e monitoramento contínuo das ações do plano de resposta, atentando-se para novos eventos de risco que possam surgir.

Gerenciar os riscos à integridade prevê proatividade e uma sistemática para identificar, avaliar, e mitigar possíveis ameaças à integridade. No gerenciamento de riscos é necessário seguir um processo estruturado para que os aspectos relacionados à integridade sejam adequadamente considerados e abordados. Abaixo estão os passos-chave para um eficaz gerenciamento de riscos à integridade:

Identificação de Riscos: Envolve a identificação de todas as possíveis ameaças à integridade da organização. Isso pode incluir fraudes, corrupção, conflitos de interesse, má conduta, entre outros.

Avaliação de Riscos: Depois da identificação, os riscos à integridade serão avaliados quanto à probabilidade de ocorrência e impacto que podem ter sobre a organização. Isso ajuda a priorizar os riscos e focar os esforços de mitigação nos mais críticos.

Mitigação de Riscos: Com base na avaliação, estratégias de mitigação devem ser desenvolvidas e implementadas visando a redução da probabilidade de ocorrência e do impacto. É fundamental a existência de controles internos, políticas e procedimentos claros, capacitação e uma forte cultura organizacional sobre o tema integridade.

Monitoramento e Controle: O gerenciamento de riscos à integridade é um processo contínuo que requer monitoramento constante para garantir que as estratégias de mitigação estejam funcionando conforme o esperado e para identificar novos riscos que possam surgir. É importante também realizar revisões periódicas para garantir sua eficácia e fazer ajustes conforme necessário.

Comunicação e Transparência: Uma comunicação clara e transparente sobre os riscos à integridade e as medidas de mitigação adotadas é crucial para o atingimento da credibilidade com os *stakeholders* e promover a cultura de integridade dentro da organização. Isso inclui relatórios regulares sobre o estado dos riscos à integridade e ações tomadas para enfrentá-los.

Seguindo este processo, as organizações podem fortalecer sua capacidade de proteger sua reputação, evitar danos financeiros e legais, e manter a confiança de seus *stakeholders*.

3.3.1 Gerenciamento de Riscos no Programa de Integridade da Caixa Econômica Federal

O Estatuto Social da CEF traz, em seu Artigo 38, as competências do Conselho de Administração:

> "determinar a implantação e supervisionar os sistemas de GR e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a CEF, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude", além de "aprovar o sistema de gerenciamento de riscos e de controles internos e suas revisões periódicas" e, por fim, "aprovar os níveis de apetite por riscos da instituição na Declaração de Apetite por Riscos e revisá-los, com o auxílio do Comitê Independente de Riscos, do Conselho Diretor e do Vice-Presidente designado para a função de gerenciamento de riscos" (CAIXA, 2017).

A CEF adota procedimentos para avaliação e gerenciamento dos riscos. Isso inclui a identificação, classificação, avaliação, monitoramento, mitigação e controle desses riscos nos projetos contratados.

De acordo com a Resolução CMN nº 4.943/2021, a CEF prevê o monitoramento das exposições a setores e regiões geográficas. Para isso, desenvolveu metodologias que permitem quantificar os riscos e o grau de vulnerabilidade. Os processos de monitoramento incluem:

Fornecedores: são as ações para cumprir a legislação, com foco na mitigação dos riscos, principalmente os de reputação relacionados às contratações de fornecedores.

Declaração de Apetite por Riscos: apresenta a relação entre o apetite por riscos do Banco e sua estratégia, impondo limites e a tolerância por meio dos indicadores. Contém procedimentos a serem seguidos quando houver violação dos limites, especificando os papéis e as responsabilidades dos gestores.

No âmbito do Sistema de Controle Interno da CEF, são estabelecidos procedimentos específicos e utilizadas ferramentas que oferecem suporte para a mitigação dos riscos atribuídos às unidades, incluindo a formulação de planos de ação. Além disso, o sistema prevê que as unidades de Segunda Linha de Defesa atuem contribuindo para o fortalecimento do ambiente de gestão de riscos.

A CEF possui uma Política de Controle Interno, *Compliance* e Integridade (CAIXA, 2023) que estabelece:

Diretrizes para prevenção, detecção, correção e mitigação de riscos relacionados ao *Compliance* e Integridade, contendo medidas para lidar com os

conflitos de interesses, para auxiliar líderes, conselheiros e funcionários da CAIXA em suas decisões e atuações.

Garantia de gerenciamento eficaz do risco de c*ompliance* e integridade com outros tipos de risco.

Promoção da efetividade e fortalecimento do Sistema de Controles Internos (SCI) e do Ecossistema de Integridade da CEF.

Ainda segundo a política supracitada há o estabelecimento de diretrizes e responsabilidades para reforçar o compromisso da CEF com práticas de prevenção, detecção e correção relacionadas à corrupção, que devem ser seguidas por administradores, dirigentes, conselheiros, funcionários e terceiros. Isso inclui a segregação de funções, mitigação de conflitos de interesses, cultura de *compliance*, mitigação de riscos por meio de controles internos eficazes e a promoção de conduta ética.

A CEF possui um Programa de Integridade da CEF (2021) estruturado em cinco pilares distribuídos em três eixos principais: Prevenção, Detecção e Correição, sendo dois desses pilares diretamente associados ao gerenciamento de riscos:

Segundo Pilar – Gestão Adequada de Riscos: engloba o mapeamento, identificação, avaliação e mitigação periódica dos riscos à integridade.

Terceiro Pilar – Protocolos de Integridade: com base na identificação e análise de riscos, a CEF desenvolve e implementa protocolos de integridade para prevenir, detectar e remediar potenciais ilícitos que possam comprometer seus objetivos, incluindo fraudes e corrupção (CAIXA, 2021).

A CEF dispõe de diversos protocolos de integridade destinados a minimizar os atos ilícitos em suas operações, tais como: Código de Ética e Comissão de Ética, Código de Conduta, Termos de Ciência relacionados ao Programa de Integridade, Registros e Controles Contábeis, Auditoria Interna, Processos de Contratação, Patrocínios e Doações, Pesquisas sobre Integridade, Canais de Denúncia e Proteção ao Denunciante (CAIXA, 2021).

Os protocolos de integridade são normas, políticas ou ferramentas projetadas para estabelecer diretrizes de conduta ética e controles internos, com o objetivo de prevenir, detectar e remediar eventos que possam comprometer a integridade, conforme estipulado pela Lei Anticorrupção nº 12.846 (CN, 2013a).

A CEF adota como premissa na sua gestão as melhores práticas de governança e transparência, controles internos e Gerenciamento de Riscos (GR) que

possam garantir a proteção e valorização do Banco. Este alinhamento visa também integrar a gestão com os compromissos assumidos com clientes, sociedade e órgãos externos de fiscalização e controle.

O modelo de GR da CEF inclui medidas que assegurem o alcance dos OE, oferecendo subsídios à tomada de decisões, facilitando os processos e mitigando potenciais desvios. Em situações de exposição a riscos que possam afetar o Banco, as medidas são acionadas para combater possíveis ilícitos, em consonância com nossa postura ética, íntegra e sustentável.

O GR desempenha um papel fundamental na sustentabilidade do Programa de Integridade, atuando nos eixos de prevenção, detecção e remediação de eventos que possam comprometer a conduta ética da organização.

Os riscos à integridade da CEF podem variar de acordo com diversos fatores, incluindo a complexidade das operações, o ambiente regulatório, a exposição a fraudes e corrupção, entre outros. Alguns dos principais riscos à integridade que a CEF pode enfrentar incluem:

Fraudes Financeiras: Como uma instituição financeira, a CEF está exposta a riscos relacionados à fraude financeira, como falsificação de documentos, roubo de identidade, lavagem de dinheiro e manipulação de dados contábeis.

Corrupção e Conflitos de Interesse: A natureza das operações da CEF, que envolve o fornecimento de serviços financeiros e programas sociais, pode criar oportunidades para corrupção e conflitos de interesse, tanto internamente quanto em parcerias externas.

Gestão de Riscos e Conformidade: A má GR e a falta de conformidade com regulamentos podem expor a CEF a multas, sanções e danos à reputação. Isso inclui questões relacionadas à conformidade com normas anti-lavagem de dinheiro, regulamentações bancárias, entre outros.

Cibersegurança e Proteção de Dados: A crescente ameaça de ciber-ataques representa um risco significativo à integridade da CEF, incluindo roubo de dados pessoais e financeiros dos clientes, interrupção de serviços e comprometimento da segurança das transações.

Gestão de Terceiros e Fornecedores: A terceirização de serviços e a dependência de fornecedores podem introduzir riscos à integridade, especialmente se os parceiros não aderirem aos mesmos padrões éticos e de conformidade que a CEF.

Gestão de Recursos Humanos: Questões como má conduta de funcionários, violações de políticas internas, assédio no local de trabalho e práticas inadequadas de contratação e promoção podem afetar a integridade da instituição.

Para mitigar esses riscos, a CEF deve implementar medidas robustas de GR, conformidade e segurança, incluindo controles internos eficazes, treinamento contínuo de funcionários, monitoramento proativo de atividades suspeitas, auditorias e colaboração com órgãos reguladores e autoridades de aplicação da lei. Além disso, promover uma cultura organizacional que valorize a transparência, a ética e a integridade é fundamental para proteger a reputação e a sustentabilidade da CEF.

A abordagem teórica do GR na CEF enfatiza a importância de identificar, avaliar e mitigar ameaças que possam impactar a estabilidade financeira e operacional da instituição, incluindo a integridade. Esta perspectiva sublinha a necessidade de frameworks robustos, normas e procedimentos que permitem uma compreensão abrangente dos riscos, incluindo os de crédito, mercado, operacional, *compliance* e de integridade. No entanto, sem a aplicação prática dessas diretrizes, a eficácia do GR permanece limitada, uma vez que a teoria, por si só, não testa a resiliência dos processos frente a situações reais. A implementação prática é crucial para validar e ajustar os modelos teóricos, assegurando que eles não apenas atendam às exigências regulatórias, mas também protejam a organização contra crises financeiras e operacionais reais.

3.3.2 Gerenciamento de Riscos no Programa de Integridade do Banco Nacional do Desenvolvimento (BNDES)

Conforme a Política Corporativa de Integridade do Sistema BNDES (BNDES, 2020), a manutenção adequada do Programa de Integridade segue os seguintes parâmetros para implementação e contínuo aprimoramento:

- Realização de análise periódica de riscos para ajustes necessários no Programa de Integridade;
- Implementação de regras, procedimentos e controles internos proporcionais aos riscos enfrentados pelo Sistema BNDES, com base em uma abordagem baseada em risco;

- Estabelecimento de padrões de conduta e código de ética aplicáveis a todos os participantes do Sistema BNDES, independentemente do cargo ou função exercidos.

No BNDES, fraude é definida como um ato intencional, consumado ou não, que envolve omitir, subtrair e/ou manipular transações, operações, sistemas, documentos, registros, relatórios, declarações, informações e demonstrações financeiras, entre outros elementos, físicos, virtuais ou monetários. Esse ato tem como objetivo enganar ou prejudicar outra parte, obtendo vantagem sobre ela ou não, conforme estipulado pela Política Corporativa de Gestão de Risco e Controle Interno. Os tipos de eventos de fraude estão detalhados na grade de eventos de risco operacional, desenvolvida e mantida pela Área de Integridade e *Compliance* (BNDES, 2020).

A Resolução CA BNDES nº12 (BNDES, 2023) relata que o processo de gerenciamento de risco e controle interno envolve as seguintes etapas: identificação, análise, avaliação, tratamento e monitoramento dos riscos.

Existem diversas modalidades para o tratamento de um risco:

a) Aceitação: decisão consciente de assumir um risco, seja pela baixa probabilidade de ocorrência e baixo impacto, seja porque a implementação de controles adicionais implicaria em custos superiores às eventuais perdas estimadas;

b) Transferência: distribuição acordada do risco com outras partes, total ou parcialmente;

c) Mitigação: adoção de medidas para reduzir a probabilidade e/ou impacto esperados de um evento de risco;

d) Eliminação: adoção de medidas que excluem determinado risco, podendo envolver mudanças, suspensões ou términos de atividades (BNDES, 2023).

Ainda pela Resolução CA BNDES nº12 (BNDES, 2023) o Sistema BNDES também adota o conceito de linhas de defesa para o gerenciamento de risco e controle interno. Na segunda linha de defesa, a Área de Integridade e *Compliance* apoia os gestores na identificação e avaliação dos riscos, implementação de controles, disseminação da cultura de integridade e *compliance*, além de reportar-se à estrutura de governança. Outras unidades desempenham tarefas semelhantes dentro de suas atribuições.

A terceira linha de defesa compreende a Auditoria Interna, responsável por avaliar objetivamente a integridade e adequação do sistema de controle interno, gerenciamento de riscos e governança. A Auditoria Interna também mantém

comunicação com órgãos externos de controle e fiscalização, integrando o Sistema de Controle Interno do Poder Executivo Federal e atuando como órgão técnico de assessoramento e consultoria para os membros dos Conselhos de Administração e Fiscal do BNDES (BNDES, 2020).

Cabe à Unidade de Integridade e *Compliance* (UIC):

a) elaborar e revisar anualmente a Política, submetendo ao Comitê de Riscos e de Gerenciamento de Riscos, garantindo a comunicação para todo o Sistema BNDES;

b) produzir relatórios de suas atividades e apresentá-los à Diretoria Executiva, Comitê de Riscos, Conselhos de Administração e Fiscal, bem como ao Comitê de Auditoria;

c) desenvolver e gerir metodologias de gestão de risco e controle interno; e

d) calcular o capital regulatório e econômico relacionado ao risco e administrar seu consumo (BNDES, 2020).

Cabe ao Comitê de Auditoria (COAUD):

a) elaborar, conforme o Regimento Interno do Comitê de Auditoria, relatórios sobre suas atividades, resultados, conclusões e recomendações, incluindo a avaliação da eficácia do sistema de controle interno, conforme a legislação aplicável, destacando as deficiências;

b) supervisionar as atividades realizadas nas unidades de controle interno do Sistema BNDES; e

c) avaliar e monitorar as exposições aos riscos do Sistema BNDES, bem como a qualidade e integridade dos mecanismos de controle interno (BNDES, 2020).

No BNDES, o programa de integridade é essencial que visa garantir a transparência, a ética e a conformidade nas operações do banco. No entanto, o gerenciamento de riscos dentro da organização tem um foco mais acentuado na qualidade da integridade dos mecanismos de controle interno. Essa abordagem enfatiza a importância de fortalecer as estruturas de controle interno para detectar e prevenir irregularidades, fraudes e erros, assegurando que os processos e operações estejam alinhados com os princípios de governança corporativa. Ao priorizar a integridade dos controles internos, o BNDES busca não apenas cumprir as exigências regulatórias, mas também fortalecer a confiança dos *stakeholders* na sua capacidade de gerir recursos públicos de forma eficaz e responsável.

3.3.3 Gerenciamento de Riscos no Programa de Integridade do Banco Central do Brasil (BCB)

Pelo artigo 6º da Resolução do BACEN nº 5.076 de 18 de maio de 2023 e pela Gestão Integrada de Riscos no Banco Central do Brasil, a estrutura de GR deve identificar, mensurar, avaliar, monitorar, reportar, controlar e mitigar o risco de crédito, o risco de mercado, o risco de variação das taxas de juros, o risco operacional, o risco de liquidez, o risco social, o risco ambiental, o risco climático e os demais riscos relevantes, segundo critérios definidos pela instituição (BCB, 2023b; BCB, 2017a).

A Política de Gestão de Riscos do BCB estabelece princípios, processo, estrutura e as responsabilidades na GR e a Política de Gestão Integrada de Riscos (PGR-BCB) define os aspectos de governança e as diretrizes da gestão dos riscos. A GR inclui, além da política, a metodologia, os sistemas e os processos de trabalho. Essa abordagem reflete o comprometimento da organização com o fortalecimento da governança para manter alinhado o processo de decisão ao seu apetite por riscos. O Departamento de Riscos Corporativos e Referências Operacionais (DERIS) é responsável por definir modelos e metodologias de risco e avaliação de resultados, com base em critérios estabelecidos pela Diretoria Colegiada, no âmbito do Comitê de Governança, Riscos e Controles (GRC)

Pela Gestão Integrada de Riscos, o BCB adota um sistema de GR que engloba a identificação das diversas fontes de risco enfrentadas pelo Banco, a interação entre essas fontes, a proposição de medidas para gerenciar esses riscos, a utilização das informações de eventos de riscos na gestão dos recursos, a promoção de uma cultura de risco e o aumento da transparência no processo decisório através do uso dessas informações. (BCB, 2017a)

Esse gerenciamento é sistêmico e estruturado, considerando as particularidades do Banco. É fundamentado nas evidências que permitem a avaliação e o tratamento dos eventos de risco, utilizando modelos e técnicas atualizados que refletem as melhores práticas disponíveis. Esse processo permite identificar ações para reduzir, evitar, transferir ou aceitar os riscos, enquanto a alta administração verifica a eficácia da estrutura de controles internos do BCB.

O processo de GR envolve etapas como identificação, mensuração, gerenciamento, controle e monitoramento dos riscos. Guias de melhores práticas para GR geralmente descrevem essas atividades, sendo responsabilidade de cada

organização desenvolver as técnicas necessárias adequadas ao seu contexto específico.

A mensuração dos riscos envolve probabilidade de ocorrência e impactos esperados desses eventos e a fase de avaliação, onde os riscos são elencados e priorizados em uma matriz que leva em conta os controles existentes. Eles são então categorizados em diferentes níveis de criticidade para priorização, utilizando critérios específicos de avaliação. Essa priorização guia a decisão sobre o tratamento adequado dos riscos (mitigação, aceitação, transferência ou evitação).

Durante a identificação e avaliação dos riscos, os departamentos sugerem ao Banco quais riscos devem ser aceitos, evitados, mitigados ou transferidos.

As ações decorrentes para mitigar, evitar ou transferir os riscos são formalizadas em Planos de Mitigação de Riscos (PMRs). Esses planos são validados pela alta administração. A responsabilidade pela elaboração dos PMRs cabe ao departamento responsável pelo processo.

A metodologia para identificar e avaliar os riscos permite uma priorização. Caso haja necessidade de um PMR, a não abertura do plano deve ser justificada e registrada.

A Diretoria Colegiada do BCB recebe informações dos departamentos sobre os riscos identificados e a forma de tratá-los. Em última instância, a Diretoria valida as sugestões de resposta ao risco ou recomenda as devidas alterações.

Em 2011, foi estabelecida a primeira Política de Gestão de Riscos (PGRs) em toda a organização, abrangendo tanto os riscos financeiros quanto os riscos organizacionais. A PGRs, atualizada em 2021, é fundamentada por diretrizes e recomendações provenientes dos principais documentos de referência em GR nas organizações, posicionando o BCB como referência no tema.

Demonstrando o compromisso do Banco com o aprimoramento de sua governança, é aprovado o Plano de Integridade para o ciclo de 2020-21 em conformidade com a Portaria nº 1.089, de 25 de abril de 2018, da Controladoria-Geral da União.

Nesse Plano a GR é um conjunto coordenado de ações destinadas a assegurar que os OE sejam alcançados dentro dos limites de risco aceitáveis. Esta metodologia envolve riscos estratégicos e riscos operacionais, sendo este último subdividido em diversas dimensões de impacto, como financeiro, reputacional e de negócio. Notavelmente, entre os tipos de risco operacional, podemos destacar aqueles que

afetam a integridade, envolvendo potenciais desvios éticos e de conduta, os quais comprometem os objetivos, valores ou imagem do Banco.

As informações derivadas da GR, incluindo aquelas relacionadas à integridade, são essenciais para embasar a tomada de decisões e fortalecer os processos. Em um contexto estratégico, a utilização das informações de risco constitui um suporte crucial para a tomada de decisões. No nível operacional, tais informações desempenham um papel fundamental na implementação adicional de medidas para mitigação no caso de materialização dos eventos de risco. No âmbito tático da organização, esses riscos servem como abordagens complementares entre as perspectivas decisória e defensiva. (BCB, 2021a)

Ainda pelo Plano de Integridade do BCB (2021a) a metodologia de GR para a integridade do BCB segue alinhada ao processo de identificação e avaliação de riscos da Autarquia, que se desenvolve através de resultados integrados analisados por meio de três modelos principais de informação:

a) Modelos de Percepção: baseados na avaliação de riscos e controles pelos gestores de cada processo, onde os riscos associados são identificados e classificados segundo uma taxonomia baseada em eventos;

b) Modelos de Confirmação: permitem a identificação de novos riscos, visualização de tendências e comportamento dos riscos ao longo do tempo, registrando sistematicamente eventos e quase eventos, independentemente da severidade da perda; e

c) Modelos de Reconhecimento: antecipam a evolução de exposições ao risco, utilizando técnicas de reconhecimento de padrões e aprendizado automático para identificar exposições atuais e tendências futuras de risco.

Os resultados da identificação e mensuração de riscos são consolidados em uma matriz de riscos, facilitando a compilação e visualização integrada dos processos e riscos associados. Esta matriz estabelece relações entre processos e riscos, oferecendo uma visão abrangente dos níveis de exposição ao risco, classificados nas escalas "I" (alta prioridade), "II" (prioridade média) e "III" (baixa prioridade), considerando impacto e probabilidade de ocorrência.

Com base na matriz de risco, os gestores de processo avaliam a resposta mais apropriada a cada risco, buscando ajustar a exposição ao risco a níveis aceitáveis. Quando há uma exposição significativa, mesmo com controles e recursos existentes, são implementadas ações de mitigação de riscos, avaliadas sob uma análise de custo-

benefício. As ações são formalizadas pelos departamentos em planos de mitigação, após validação do tratamento pela alta administração.

O processo de GR do BCB está bem estruturado na teoria, abrangendo todas as etapas essenciais: identificação, análise, avaliação, tratamento, comunicação e monitoramento. Cada uma dessas etapas é fundamental para garantir uma abordagem sistemática e abrangente na identificação e mitigação de riscos que possam impactar a organização.

No entanto, uma análise mais detalhada revela uma ausência significativa no que diz respeito à identificação e monitoramento de riscos de integridade. Riscos de integridade, que incluem fraudes, corrupção, e outras formas de conduta inadequada, são críticos para a manutenção da confiança e da reputação de uma instituição financeira.

A falta de identificação e monitoramento adequado desses riscos pode expor o BCB a sérias vulnerabilidades, comprometendo a eficácia geral do seu processo de GR. Os riscos de integridade são especialmente perniciosos, pois podem minar a confiança pública e a credibilidade da organização, além de trazer consequências legais e financeiras severas.

3.3.4 Gerenciamento de Riscos à Integridade do Programa de Integridade da Marinha do Brasil (MB)

Na MB define-se os riscos à integridade, como eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possam comprometer os valores e padrões preconizados pela Marinha e a realização de seus OE.

Segundo o Plano de Integridade da MB (2018), aprovado pela Portaria nº 336/2018 do EMA, foram identificados alguns riscos à integridade, relevantes e comuns, conforme a seguir:

-Abuso de posição ou de poder em favor de interesses privados;

-Conflito de interesses;

-Pressão ilegal ou antiética para influenciar agente público ou privado;

-Nepotismo;

-Solicitação ou recebimento de vantagem indevida;

-Utilização de recursos públicos em favor de interesses privados;

-Utilização/vazamento de informação privilegiada/restrita;

-Assédio Moral

-Assédio Sexual (Marinha, 2018).

A MB segue o Decreto nº 9.203/2017, onde a GR é o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

O processo de GR à Integridade seguirá o contido na SGM-107 Vol I, assim como a norma ISO 31000 – GR e a estrutura fornecida pelo *Committee of Sponsoring Organizationsof the Treadway Commission - Enterprise Risk Management* (COSO ERM) (Marinha, 2011).

As metodologias utilizadas pela MB consideram que o risco pode ser medido e quantificado, em termos de probabilidade de ocorrência e do impacto que pode causar.

Para que haja um tratamento adequado dos riscos identificados, deve haver um planejamento eficaz das respostas, ampliando as oportunidades e reduzindo as ameaças. Isso pode ser alcançado por meio de controles internos, considerando as causas, fontes, consequências e impactos, observando a relação custo-benefício. Os riscos aceitam os seguintes tipos de tratamento: aceitar, mitigar, transferir para terceiros e eliminar.

A MB adota para prevenção, detecção e correção de atos de corrupção, fraudes, irregularidades e desvios de conduta algumas publicações, como:

- Abuso de posição ou de poder, nepotismo, solicitação ou recebimento de vantagem indevida – EMA-136, DGPM-315 e DGPM-319;

- Sigilo de Informações – EMA-414;

- Utilização de Mídias e Redes Sociais – DGPM-319; e

- Prevenção e detecção de irregularidade em procedimentos administrativos EMA-130, SGM-601.

De acordo com a SGM-107 – Normas Gerais de Administração, é atribuição do Conselho de Gestão (CG) realizar a GR nas OM, efetuando a elaboração do registro de riscos, o planejamento das respostas aos riscos, sua implementação e controle. Cabe ressaltar que os riscos de integridade também estão inseridos na competência

do CG e devem ser levantados de acordo com a atividade desempenhada pela OM (Marinha, 2011).

A MB utiliza um modelo descrito no Plano de Gerenciamento e Planejamento de Respostas aos Riscos de Integridade da MB que deve ser apresentado ao EMA semestralmente pelos ODS, condensando os subsídios informados pelas OM subordinadas, em resposta às ações de monitoramento. Basicamente avaliando a probabilidade e o impacto, seguindo um critério quantitativo, onde são determinados níveis de riscos de 1 a 5 que definirão se o risco é baixo ou alto.

Fica evidenciado a importância que a MB destaca os riscos à integridade dentro do rol de riscos operacionais, financeiros, se foram estabelecidas estratégias, providências e ações (as respostas aos riscos) para aceitação, eliminação, mitigação ou transferência dos riscos à integridade mapeados na Avaliação de Riscos e para comunicação entre as partes, examinar se as respostas para eliminar ou mitigar os riscos à integridade mapeados e avaliados são claras, objetivas, necessárias e viáveis, observar se foram estabelecidos os prazos e responsáveis para acompanhar e implementar as respostas aos riscos e verificar a periodicidade com que o Plano de Integridade é atualizado para aperfeiçoamento do Programa e das Medidas de Integridade.

A Marinha se destaca pela sua transparência e comunicação eficaz através de publicações internas que abordam eventos relacionados à corrupção, fraudes, irregularidades e desvios éticos e de conduta. Essa prática fortalece a cultura organizacional de responsabilidade e integridade, permitindo que todos os membros da instituição estejam cientes dos riscos e das consequências de comportamentos inadequados.

A teoria de análise dos riscos na Marinha é robusta e bem escrita. Tanto a análise qualitativa quanto a quantitativa dos riscos são descritas corretamente, permitindo uma compreensão detalhada da natureza, probabilidade e impacto dos riscos identificados. Essa análise detalhada é importante para a realização de ações estratégicas de mitigação e tratamento dos riscos.

No entanto, a GR da Marinha enfrenta desafios significativos na **identificação dos riscos de integridade**. A ausência de uma estrutura lógica e sistemática para a identificação desses riscos compromete a eficácia geral do processo de gestão de riscos. Identificar riscos de integridade de forma precisa e completa é fundamental para proteger a instituição contra fraudes, corrupção e outras formas de má conduta.

3.4 MONITORAMENTO CONTÍNUO DOS ATRIBUTOS DO PROGRAMA DE INTEGRIDADE.

O monitoramento têm como objetivo acompanhar as ações delineadas no Plano de Integridade, aprovadas pela Alta Administração, que visa a avaliação dos resultados alcançados pelos Programas de cada organização. Este monitoramento requer medidas de tratamento dos riscos à integridade, capacitação de líderes, fortalecimento das instâncias, além da utilização dos meios de comunicação.

O Programa de Integridade implementa indicadores para avaliar periodicamente sua efetividade, com o intuito de identificar oportunidades de melhorias.

A CEF reporta de maneira oportuna às instâncias de governança competentes sobre as ações preventivas, detecções e penalidades aplicadas após a investigação de atos ilícitos cometidos por seus empregados e dirigentes. Esse processo visa avaliar a eficácia do programa, implementar melhorias e fortalecer o Ecossistema de Integridade (CAIXA, 2016).

No BNDES, o monitoramento do Programa de Integridade busca aprimorar a prevenção, detecção e combate à corrupção, desvios, fraudes, irregularidades e outros atos ilícitos.

No BCB é fato que ocorreram avanços na condução do tema Integridade, de forma a contribuir com a elevação do nível de maturidade da integridade pública, razão pela qual é intenção realizar uma auto avaliação de maturidade em Integridade Pública, conforme consta do atual Plano de Integridade (BCB,2021). No âmbito desses avanços, consta outra ação no referido plano, voltada para implantar painel de integridade de informações e indicadores relacionadas ao tema, para acompanhamento do Comitê de Integridade.

Por fim, o atual plano também prevê ação para promoção de interlocução do Comitê de Integridade com Unidades, visando ao compartilhamento de práticas de integridade adotadas nos processos meios e finalísticos das áreas.

A atividade de monitoramento possibilita o relato ágil de eventuais violações de limites operacionais, bem como das medidas adotadas para sua resolução. Esse monitoramento acompanha a evolução dos resultados das avaliações de risco e das decisões quanto ao tratamento desses riscos, incluindo a elaboração de planos de

mitigação. Além disso, o monitoramento facilita o registro das ações de gestão de continuidade de negócios. Por fim, os dados monitorados sobre os riscos alimentam relatórios direcionados tanto para as áreas de negócio quanto para a Diretoria Colegiada.

Tomando por base a Instrução Normativa Conjunta do MP/CGU, nº 1/2016 (2016), a qual dispõe sobre controles internos, GR e governança no âmbito do Poder Executivo Federal, o monitoramento na MB deve ser realizado sobre todos os componentes de controles internos, com o objetivo de medir sua eficácia, eficiência, efetividade, economicidade e excelência e corrigir as deficiências dos controles internos.

O CG é o fórum adequado para o monitoramento do grau de integridade nas OM, possibilitando aos titulares estabelecer diretrizes, verificar as atividades desenvolvidas e apresentar resultados, no intuito de elevar o nível de conhecimento da tripulação sobre o tema.

A disseminação da cultura de integridade deve ser pauta mensal das reuniões do CG, a fim de manter o tema em evidência, enaltecer as melhores práticas, promover a participação de militares e servidores civis em cursos, adestramentos, realização de palestras e estágios de capacitação.

Mensalmente é apresentada sugestões de temas para acompanhamento das atividades de integridade. O titular de OM e/ou os ordenadores de despesa deverão fomentar uma voga de integridade a bordo focando em ações voltadas para a prevenção, detecção e remediação de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta, incluindo a punição.

As ações de monitoramento do Programa de Integridade da MB são revisadas anualmente e estão disponíveis na página do Comando da Marinha, sendo encaminhadas para os Órgãos de Direção Setorial (ODS).

O modelo de relatório das ações de monitoramento deverá ser encaminhado anualmente, pelos ODS ao EMA (UGI).

3.4.1 Capacitação

As ações de capacitação dentro do Programa de Integridade serão formalizadas com base em iniciativas futuras delineadas no Plano de Integridade. O

propósito dessas medidas é fornecer orientação e treinamento para capacitar e conscientizar os Agentes de Integridade sobre diretrizes, políticas e procedimentos relacionados aos valores éticos e às práticas de integridade.

O Programa de Integridade da CEF oferece aos seus colaboradores e dirigentes oportunidades de capacitação por meio da Universidade CAIXA. O Portal da Universidade CAIXA facilita o acesso a atividades educacionais abrangendo temas como ética, conduta, integridade, regulamentos de pessoal, prevenção à lavagem de dinheiro, controles internos, riscos operacionais, gestão de bens e serviços, além do desenvolvimento de habilidades gerenciais (CAIXA, 2021).

Para reforçar o aprendizado e promover o debate entre os funcionários do Banco, também são implementadas estratégias interativas e participativas destinadas a compartilhar conteúdos educacionais.

Capacitações de interesse geral: capacitações que devem alcançar a todos os funcionários e dirigentes, como, por exemplo, capacitações relacionadas a códigos de ética e de conduta, implantação do Programa de Integridade, princípios e valores e uso de canais de denúncia;

Capacitações de interesse específico: são direcionadas para esclarecer temas ou políticas que se aplicam especialmente a grupos específicos de colaboradores ou dirigentes. Por exemplo, se uma nova política ou procedimento é implementado referente a verificações prévias para oferecimento de patrocínios, a equipe responsável pelos contratos de patrocínio deve receber treinamento sobre o conteúdo, importância e aplicação correta da política. O mesmo se aplica a políticas sobre investigações de irregularidades, aplicação de medidas disciplinares, conflitos de interesse, anticorrupção, gestão de riscos, entre outras políticas relacionadas ao Programa de Integridade.

Esse tipo de capacitação visa garantir que todos os envolvidos compreendam e possam aplicar adequadamente as políticas e procedimentos relevantes para suas funções específicas dentro da organização.

Quanto à capacitação do pessoal do BNDES é previsto na Política Corporativa de Risco Operacional que a Diretoria deverá garantir a adequada capacitação dos integrantes por meio de treinamentos periódicos e comunicação sobre o Programa de Integridade no intuito de mantê-lo adequado.

No inciso VII do artigo 16º da Resolução do BCB Nº 236, de 27 de julho de 2022 que divulga a Política de Conformidade (*Compliance*) do BCB, prevê a comunicação

e o treinamento, auxiliando na transmissão de informações e na capacitação dos funcionários e também dos prestadores de serviços terceirizados (BCB, 2022).

Na MB as ações de capacitação no âmbito da Integridade Naval foram implementadas para ampliar o conhecimento de militares e servidores civis que atuam nos temas: ética, integridade, liderança, ouvidoria, controles internos e GR.

Em cumprimento a Portaria nº 244/2020, do CM, as regras de conduta e convivência entre militares fazem parte da formação do pessoal da Marinha, abrangendo todos os círculos hierárquicos em cada etapa do ensino militar e em conjunto com a adoção dos princípios e costumes expressos na Rosa das Virtudes, contribuindo para a adoção de um ambiente livre de assédio e discriminação perfazendo expressão da ética militar (Marinha, 2020).

No tocante à liderança, o EMA-137 - Doutrina de Liderança da Marinha, define como “o processo de influenciação de um grupo, de forma a atingir os objetivos da instituição”. Este assunto está ligado a valores éticos e morais, os quais devem ser praticados pelos líderes navais, e transmitido a todos os que ingressam nas escolas de formação da MB (Marinha, 2018).

Na citada publicação, é apresentada a importância da capacitação como forma de manutenção da habilidade do ser humano perceber valores, tais como honra, dignidade e honestidade.

A integridade exige fomento contínuo e pessoal capacitado para disseminá-la. Sendo assim, todas as OM deverão designar membros de sua tripulação para se capacitarem, seja por palestras e adestramentos internos deste plano ou de assuntos convergentes ao mesmo, seja por matrícula nos cursos disponíveis para atuarem como multiplicadores da mentalidade de integridade.

O CG tem papel fundamental nesse processo, com a atribuição de examinar a quantidade e a qualificação do pessoal, e incentivar a participação em cursos, adestramentos, realização de palestras e estágios no intuito de elevar o nível de capacitação do nosso pessoal.

As principais ações de capacitação e divulgação desenvolvidas no Programa de Integridade da MB serão revisadas anualmente e estarão disponíveis na página do Comando da Marinha, bem como serão encaminhadas para os ODS para controle das ações e posterior consolidação no relatório das ações de monitoramento. As ações de capacitação não é um rol taxativo, sendo incentivadas outras iniciativas de qualificação de pessoal no tema integridade.

A capacitação deve alcançar a todos os colaboradores e dirigentes, como, por exemplo, capacitações relacionadas aos códigos de ética e de conduta, implantação do Programa de Integridade, princípios e valores e uso de canais de denúncia. Se a entidade implementa uma nova política ou procedimento, como por exemplo verificações prévias ao oferecimento de patrocínios, é fundamental que a equipe responsável pelos contratos de patrocínio seja capacitada sobre o conteúdo, importância e correta aplicação dessa política. O mesmo princípio se aplica a políticas envolvendo investigações de irregularidades, aplicação de medidas disciplinares, conflitos de interesses, anticorrupção, bem como políticas ou procedimentos relacionados à GR e outras políticas vinculadas a um Programa de Integridade.

Essas capacitações garantem que todos da organização compreendam e possam implementar eficazmente as políticas e procedimentos pertinentes às suas responsabilidades dentro da organização.

3.4.2 Canais de Comunicação

Neste item, será analisada a estratégia de comunicação e treinamento das organizações sobre temas relacionados à ética e ao Programa de Integridade. São iniciativas voltadas para seus colaboradores, dirigentes, clientes e terceiros vinculados ao Órgão, cujo objetivo é promover um ambiente íntegro e reforçar uma cultura focada em valores e padrões de conduta e ética.

Fazem parte da estratégia o estabelecimento da periodicidade das ações, o grau de integração das áreas que se responsabilizam por disseminá-las, o público-alvo, os meios e instrumentos utilizados, tais como, e-mails, jornais institucionais, cartazes, vídeos, campanhas internas, oficinas, palestras, capacitações presenciais, videoconferências e oficinas, proporcionando ao público-alvo a familiarização com os temas, para que eles se sintam coadjuvantes e confiantes na busca de soluções que propiciem um ambiente cada vez mais íntegro.

Os canais de comunicação do Programa de integridade voltado para o público, tem como objetivo o tratamento de qualquer denúncia que configure infrações aos princípios afetos à ética e à integridade, pode ser por meio de telefone para denúncias anônimas, e-mail ou por página na internet para denúncias escritas e anônimas.

A CEF adota estratégias de comunicação e treinamento fundamentais para o bom andamento do Programa de Integridade, fortalecendo a ética e promovendo a discursão sobre questões relacionadas à integridade.

Os valores e diretrizes principais de integridade da CEF são expressos no código de ética e conduta, políticas, procedimentos e outros, os quais são amplamente divulgados nos meios de comunicação do Banco. Essa divulgação visa disseminar conhecimento e fortalecer a cultura de integridade na organização.

As informações, consideradas ativos essenciais para a CEF, são críticas para a tomada de decisões empresariais, exigindo que sejam confiáveis, íntegras e disponibilizadas de forma tempestiva. Para facilitar, os funcionários têm à disposição canais de comunicação que permitem o fluxo das informações e que chegam aos conselheiros (Administrativo e Fiscal), dirigentes, colaboradores, parceiros e terceiros.

Para o público interno, a CEF disponibiliza conteúdos na intranet, como o Portal do Empregado, campanhas de *endomarketing*, entre outros meios de comunicação interna. Para o público externo, há uma página na internet que oferece informações sobre produtos, campanhas de marketing e conteúdos relacionados a ética, conduta e integridade, além de serviços como o SAC, Canal de Denúncias, e presença em redes sociais (CAIXA, 2021).

Essas iniciativas visam assegurar que todos os públicos envolvidos estejam informados e engajados no compromisso da CEF com a integridade e ética corporativa.

No BNDES, são realizados treinamentos periódicos e comunicações regulares sobre o Programa de Integridade, estabelecendo parâmetros primordiais para a implementação e a melhoria contínua do programa. A comunicação com autoridades em investigações relacionadas a atos ilícitos contra a administração pública nacional ou estrangeira são conduzidas de acordo com a legislação e normas internas do BNDES.

O BNDES dispõe de canais dedicados ao diálogo e denúncias, operando com autonomia, imparcialidade e independência. Qualquer pessoa pode contatar a Comissão de Ética no caso de denúncias relacionadas ao Código de Ética, ou a Ouvidoria para denúncias relacionadas a fraudes, com garantia de sigilo e proteção aos denunciantes de boa-fé.

Essas medidas visam assegurar que o BNDES promova um ambiente de integridade, transparência e responsabilidade, conforme seus compromissos éticos e legais.

No BCB, as iniciativas de comunicação e treinamento desempenham um papel crucial na conscientização sobre ética e integridade, além de contribuírem para o desenvolvimento de habilidades essenciais em situações cotidianas que envolvam questões e conflitos éticos. Essas ações têm como objetivo fornecer aos servidores e colaboradores o conhecimento necessário para aplicar adequadamente as diretrizes, políticas e procedimentos relacionados às medidas de integridade e ética no serviço público (BCB, 2021b).

Essas iniciativas visam promover um ambiente organizacional onde os valores de ética e integridade são internalizados e aplicados de maneira consistente em todas as atividades do BCB.

Na MB as reclamações e comunicações no âmbito da Lei nº 13.709 (2018), Lei Geral de Proteção de Dados (LGPD), devem ser encaminhadas, pelo titular, ao Encarregado pelo Tratamento de Dados Pessoais por meio da plataforma Fala.BR.

É importante que sejam evidenciadas as ações de comunicação e treinamento relacionadas aos temas do Programa de Integridade, para isso existem áreas competentes para realizar ações de comunicação e capacitação integradas e dotadas de instrumentos e meios adequados de divulgação. Periodicamente, a alta administração encaminha, comunicações sobre o tema integridade, e são utilizados meios de comunicação para a divulgação do Plano, tais como intranet.

3.4.3 Promoção da Transparência Ativa e do Acesso à Informação

Para apoiar um ambiente organizacional receptivo a preocupações de integridade, é necessário incentivar uma cultura aberta à discussão de dilemas éticos, em que erros, críticas construtivas e preocupações com os valores e padrões de conduta possam ser livremente abordados e também a liderança esteja comprometida em fornecer conselhos oportunos e resolver questões relevantes. Além disso, fornecer regras e procedimentos claros para denunciar suspeitas de violação de integridade e garantir, de acordo com os princípios fundamentais do direito interno, a proteção aos denunciantes com o intuito de favorecer um ambiente íntegro.

Uma das iniciativas provenientes do Programa de Integridade inclui o incentivo a denúncias e a institucionalização de mecanismos internos capazes de suportá-lo. É essencial, portanto, dotar de canais de denúncia com a devida proteção aos denunciantes, abertos para colaboradores e terceiros e amplamente divulgados, expandindo os meios para que violações à integridade sejam conhecidas e tratadas.

De acordo com o artigo 5º da Lei de acesso Nº 12.527, de 18 de novembro de 2011 (2011), é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.

Uma política de transparência não apenas incentiva dirigentes e empregados a agirem com responsabilidade em suas atribuições, mas também proporciona à sociedade informações essenciais para o controle das atividades governamentais. Isso se torna um instrumento crucial para o exercício da cidadania, fortalecimento da democracia e combate a fraude e corrupção (CAIXA,2021)

Neste contexto, os cidadãos têm o direito de conhecer como os recursos públicos estão sendo administrados. A transparência na divulgação de informações não se limita apenas à publicidade e acessibilidade das informações, mas também garante que o ambiente onde são geradas seja íntegro, livre de ações de corrupção, abusos e irregularidades (CAIXA, 2021).

A CEF adota várias iniciativas para promover a transparência ativa e garantir o acesso à informação, em conformidade com a Lei de Acesso à Informação (LAI) no Brasil. Mantém um Portal da Transparência acessível ao público, onde disponibiliza informações detalhadas sobre suas operações e atividades, publica regularmente uma série de documentos que são acessíveis no site e fornecem uma visão abrangente sobre suas atividades e resultados. Conforme a LAI, dispõe de canais específicos para atender às solicitações de informação dos cidadãos. Os pedidos podem ser feitos eletronicamente através do Serviço de Informação ao Cidadão (SIC) disponível no site da CEF, que tem prazos estipulados para fornecer as respostas. Disponibiliza bases de dados abertas para acesso público, promovendo a análise de informações por parte de pesquisadores, jornalistas e demais interessados. Essas bases incluem dados sobre operações de crédito, programas sociais, e outros serviços prestados. Possui informações detalhadas sobre processos licitatórios e contratos administrativos que também são publicadas no site. Isso inclui editais de licitação, resultados de processos seletivos, contratos firmados, aditivos e rescisões.

Sujeita a auditorias e fiscalizações por parte de órgãos de controle como o Tribunal de Contas da União (TCU) e a Controladoria-Geral da União (CGU). Os relatórios e resultados dessas auditorias são divulgados publicamente, aumentando a transparência sobre suas operações.

A CEF organiza e participa de eventos, seminários e *workshops* para divulgar suas atividades e prestar contas à sociedade. Esses eventos são oportunidades para que o público obtenha informações diretamente dos gestores e participe de discussões sobre temas relevantes. Participa de iniciativas de governo aberto, colaborando com outras instituições públicas para promover a transparência e a participação cidadã. Essas iniciativas visam fortalecer a governança e a responsabilidade pública. E por último, como agente financeiro de diversos programas sociais do governo federal, divulga amplamente informações sobre esses programas, incluindo critérios de elegibilidade, formas de acesso aos benefícios e resultados alcançados.

O BNDES, muito similar com a CEF, mantém altos padrões de transparência e de prestação de contas, tem implementado diversas iniciativas para promover a transparência ativa e garantir o acesso à informação, de acordo com os princípios estabelecidos pela Lei de Acesso à Informação (LAI) no Brasil. Algumas das principais ações e práticas adotadas:

- Mantém um Portal da Transparência, que é uma plataforma online onde são divulgadas diversas informações sobre suas operações e atividades. Neste portal, o público tem acesso a dados detalhados sobre empréstimos e financiamentos concedidos, incluindo valores, prazos e taxas de juros, informações sobre os beneficiários dos recursos e projetos apoiados pelo banco, com detalhes sobre os objetivos, investimentos e impactos esperados;

- Regularmente, publica relatórios de atividades, demonstrações financeiras, relatórios de sustentabilidade e outros documentos que fornecem uma visão abrangente sobre a atuação do banco. Esses relatórios são disponibilizados em seu site oficial e são acessíveis ao público em geral;

- Dispõe de canais específicos para atender às solicitações de informação dos cidadãos, conforme previsto pela LAI. Os pedidos podem ser feitos por meio de formulário eletrônico no site do banco, e o BNDES tem prazos estipulados para fornecer as respostas, garantindo a transparência e a acessibilidade das informações solicitadas;

- Para facilitar o acesso a informações e promover a análise de dados por pesquisadores, jornalistas e outros interessados, o BNDES disponibiliza bases de dados abertas. Essas bases contêm informações estruturadas sobre operações de crédito, projetos financiados e outras atividades do banco;

- O BNDES está sujeito a auditorias e fiscalizações por parte de órgãos de controle, como o Tribunal de Contas da União (TCU) e a Controladoria-Geral da União (CGU). Os relatórios e resultados dessas auditorias são publicamente divulgados, contribuindo para a transparência das operações do banco;

- Organiza e participa de eventos, seminários e *workshops* voltados para a divulgação de suas atividades e prestação de contas à sociedade;

- Todas as informações referentes a contratos, convênios, parcerias e licitações do BNDES são publicadas e atualizadas regularmente em seu site. Isso inclui os processos de contratação, resultados de licitações, termos de contratos e aditivos; e

- Participa ativamente de iniciativas de governo aberto, colaborando com outras instituições públicas para promover a transparência e a participação cidadã. Essas iniciativas são parte de um esforço mais amplo para fortalecer a governança e a responsabilidade pública.

Essas ações demonstram o compromisso do BNDES com a transparência e o acesso à informação, elementos fundamentais para a *accountability* e a confiança da sociedade nas instituições públicas. Através dessas práticas, o BNDES busca não apenas cumprir as exigências legais, mas também estabelecer um diálogo contínuo e aberto com a sociedade, promovendo a cultura da transparência e da responsabilidade social.

No BCB, a transparência e o acesso à informação são fundamentais para promover o interesse público e consolidar uma cultura de integridade. Dentro da instituição, a Ouvidoria desempenha um papel crucial ao monitorar o cumprimento da Lei de Acesso à Informação (LAI), Lei nº 12.527 de 18 de novembro de 2011. Os resultados desse monitoramento são detalhados no Relatório Anual da Ouvidoria, apresentado à Diretoria Colegiada do BCB e à Ouvidoria Geral da União e disponibilizado na internet (BCB, 2021b).

O relatório anual reflete os avanços recentes no aumento da transparência, especialmente por meio da transparência ativa, que envolve a divulgação proativa de informações. Além disso, o documento inclui uma análise das manifestações recebidas pela Ouvidoria e informações sobre a implementação de propostas de

aprimoramento geradas a partir das demandas registradas pelos cidadãos (BCB, 2021b).

Essas iniciativas não apenas fortalecem a confiança pública na gestão do BCB, mas também promovem a *accountability* e o engajamento cívico, elementos essenciais para uma administração pública transparente e eficaz.

Na MB as denúncias no tocante as condutas antiéticas efetivada por militares deverão seguir a cadeia de Comando a que estiver subordinado. A conduta antiética, não enquadrada como crime, praticada por terceirizados e estagiários deverá ser reportada pelos militares ao responsável pelo apoio administrativo da OM.

No tocante as denúncias referentes às condutas atentatórias contra a pessoa e à discriminação por razão de sexo, os militares devem observar o contido na PESSOALMARINST nº 1/2023, da DGPM, onde assevera que as mesmas devem ser feitas pessoalmente e individualmente ao órgão de execução do serviço de assistência social ao pessoal da marinha, que assiste a OM, uma vez ser este o canal para recebimento desse tipo de ocorrência (Marinha, 2023).

Denúncias efetuadas por servidores civis, prestadores de serviços e demais integrantes da MB e da sociedade, orienta-se a procurar o seu superior hierárquico ou a utilizar a Plataforma Integrada de Ouvidoria e Acesso à Informação – “Fala.BR”, o que lhe for mais conveniente.

Os demais cidadãos ao identificarem qualquer fato ou ato, independente de quem praticou, que atente contra os princípios éticos devem sempre denunciar por meio da Plataforma Integrada de Ouvidoria e Acesso à Informação – “Fala.BR”

Insta salientar, que em atendimento ao Decreto nº 9.492/2018, que instituiu o Sistema de Ouvidoria do Poder Executivo Federal (e-Ouv), o CCSM é o responsável pelas respostas às manifestações que deverão ser registradas na Plataforma Integrada de Ouvidoria e Acesso à Informação – Fala.BR.

Adicionalmente, como previsto no Decreto nº 10.153 (2019), as informações dos denunciantes de ilícitos e de irregularidades estão plenamente salvaguardadas, de modo a preservar o sigilo daquele que denuncia.

Por meio do EMA-138 - Normas para o Serviço de Informações ao Cidadão no âmbito da Marinha do Brasil (SIC-MB) foram definidas a estruturação do SIC-MB e a tramitação de demandas por informações, estabelecidas na Lei de Acesso à Informação (LAI) (EMA-138, 2020).

A estrutura do SIC-MB está configurada da seguinte forma:

I - O CCSM é a Unidade de Monitoramento e Gestão (UMG); e

II - Os Comandos de Distritos Navais são as Unidades de Atendimento ao Público (UAP) (EMA-138, 2020).

A tramitação das demandas por informações pode ocorrer de três formas:

I - Por meio da Internet, bastando acessar a página principal da Marinha (www.marinha.mil.br) e clicar no link “Serviço de Informação ao Cidadão – SIC”;

II - Por meio de atendimento nas Unidades de Atendimento ao Público; e

III - Por meio de Mídias Sociais (EMA-138, 2020).

A Marinha utiliza as redes sociais, em seus perfis institucionais nas seguintes mídias: Facebook, Twitter, Youtube e Flickr. As informações demandadas nestes canais são direcionadas ao SIC-MB para resposta da Força (EMA-138, 2020).

Mas ainda é preciso que a MB tenha normativos que disciplinem as atividades de recebimento, tratamento e acompanhamento de manifestações de ouvidoria (denúncias, reclamações, sugestões, solicitações e elogios) e de pedidos de acesso à informação pública pelos canais de acesso.

4 PRESCRIÇÃO DE UMA METODOLOGIA PARA GERENCIAMENTO DE RISCO À INTEGRIDADE

O GR tem como objetivo principal identificar e tratar os eventos de riscos que possam impactar a organização. As incertezas que afetem os objetivos da organização devem receber atenção no processo de GR, enquanto aquelas que não possam impactar os objetivos, sejam conhecidas ou desconhecidas, não necessitam de tratamento específico.

Diversos autores e instituições destacam o GR como uma abordagem proativa para lidar com as incertezas inerentes às atividades organizacionais. Esta prática visa a redução da probabilidade e do impacto dos eventos negativos.

É importante ressaltar que não é possível eliminar completamente os riscos sem alterar fundamentalmente a natureza das atividades dos bancos e da MB. Portanto, o gerenciamento de riscos visa administrá-los de forma a mitigar seus efeitos adversos.

A abordagem no Manual de Gestão de Riscos do Ministério do meio Ambiente é dividida em etapas sequenciais e cíclicas, uma metodologia robusta de Gestão de Integridade, Riscos e Controles Internos compreende diversas etapas, como análise de ambiente e fixação de objetivos, identificação e avaliação de eventos de riscos, resposta aos riscos, e informação, comunicação e monitoramento. Essas etapas são projetadas para alcançar os objetivos específicos do processo de gestão de integridade, riscos e controles internos, incorporando boas práticas reconhecidas, incluindo elementos da estrutura do COSO ERM (MMA, 2020).

Adicionalmente, essa metodologia está alinhada com normativas e políticas governamentais, como a Instrução Normativa Conjunta MP/CGU nº 01/2016 e a Política de Gestão de Integridade, Riscos e Controles Internos estabelecida pela Portaria nº 426/2016 do MPOG. Isso garante que a implementação da metodologia não apenas atenda aos padrões de *compliance*, mas também fortaleça a integridade organizacional.

4.1 ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS

A análise do ambiente desempenha um papel crucial no suporte à identificação de eventos de riscos e na escolha de ações estratégicas para alcançar os OE. Esses objetivos, são definidos pela alta administração, e devem ser comunicados a todos os membros da organização antes da identificação dos eventos, alinhados à missão e ao apetite a riscos estabelecido.

No contexto do ambiente interno, são verificados aspectos como integridade, competência das pessoas, valores éticos, responsabilidades pela gestão e delegação de autoridade, estrutura de governança, políticas e práticas de recursos humanos. Este ambiente interno serve como base para todas as outras etapas, fornecendo

disciplina e preparação para a gestão de integridade, riscos e controles internos da organização.

A clareza na definição dos objetivos, alinhados com a missão e visão da organização, é essencial para facilitar a identificação de eventos que possam impedir sua realização. As informações necessárias podem ser obtidas através de pesquisas no planejamento estratégico, regimento interno, orçamento e relatórios de órgãos de fiscalização e controle.

Para identificar forças e fraquezas internas, bem como analisar as influências do ambiente externo sobre os macroprocessos, recomenda-se a utilização da ferramenta SWOT (*Strengths, Weaknesses, Opportunities, Threats*) (Figura nº 2). Essa análise permite uma visão abrangente dos pontos fortes e fracos internos da organização, além de oportunidades e ameaças externas que possam impactar seus objetivos estratégicos. Essa abordagem integrada no gerenciamento de integridade, riscos e controles internos ajuda a fortalecer a capacidade da organização de antecipar e responder eficazmente às mudanças e desafios do ambiente operacional.

Figura 2 –Análise SWOT

Fonte: Tachizawa e Freitas, 2004

A utilização da análise SWOT é essencial para realizar uma análise de cenário, tanto do ambiente interno quanto externo de uma organização. As informações obtidas por meio desta análise são cruciais para identificar riscos e determinar as respostas adequadas a esses riscos.

As informações coletadas durante a análise SWOT, juntamente com dados do processo como normas, fluxogramas, descrições de tarefas e responsabilidades, são fundamentais para as etapas subsequentes do GR à integridade e controles internos

da gestão. Estas informações são tipicamente coletadas ao longo da cadeia de valor ou do mapeamento dos processos organizacionais, das leis, regulamentos e normas que afetam os macroprocessos, bem como dos sistemas de informação da organização.

A análise SWOT não só ajuda a identificar riscos potenciais, mas também a verificar a conformidade com leis, regulamentos e normas vigentes. Isso é crucial para adotar ações de controle que garantam o cumprimento das obrigações legais e regulatórias, mitigando assim os riscos associados à não conformidade.

Ao integrar a análise SWOT ao gerenciamento de integridade, riscos e controles internos, as organizações podem melhorar sua capacidade de antecipar, avaliar e responder eficazmente aos desafios e oportunidades presentes em seu ambiente operacional.

Essa abordagem sistemática e integrada contribui significativamente para fortalecer a governança corporativa e promover uma cultura organizacional fundamentada em práticas éticas e transparentes.

4.2 IDENTIFICAÇÃO DE EVENTOS DE RISCOS

O objetivo da identificação de riscos é encontrar e descrever as incertezas que podem tanto beneficiar quanto impedir uma organização de alcançar seus objetivos. É crucial que as informações utilizadas sejam apropriadas para uma identificação eficaz de riscos. Para esse fim, diversas técnicas podem ser empregadas pela organização, visando identificar incertezas que possam impactar os OE.

O processo de identificação de eventos de riscos é cíclico, pois novos eventos podem surgir ao longo da análise. Recomenda-se que todos os envolvidos sejam incentivados a contribuir na identificação de eventos de riscos, utilizando técnicas como *brainstorming* e entrevistas entre outras.

Autores como Miles; Wilson Junior (1998) destacam a necessidade de ferramentas objetivas para a identificação e análise de eventos de riscos, dado que muitas vezes esse aspecto pode não receber a devida atenção por parte dos tomadores de decisão, influenciados pelo ambiente organizacional.

Essa etapa visa identificar e registrar os eventos de riscos e suas causas e consequências. É fundamental considerar a análise do ambiente organizacional nesse processo.

Eventos são situações potenciais que, caso ocorram, podem impactar negativamente o alcance dos OE. Os eventos que representam impactos negativos são denominados riscos. A correta identificação desses eventos permite planejar estratégias de tratamento e determinar o tipo de resposta apropriada para mitigar esses riscos. É crucial compreender que os eventos de riscos devem ser analisados dentro de um escopo mais amplo, não isoladamente.

Recomenda-se que a descrição de um evento de risco seja estabelecida conforme essa estrutura (Figura nº3):

“Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS> impactando no/na <OBJETIVO DE PROCESSO >” (ENAP/2018).

Figura 3 - Estrutura da Identificação do Risco

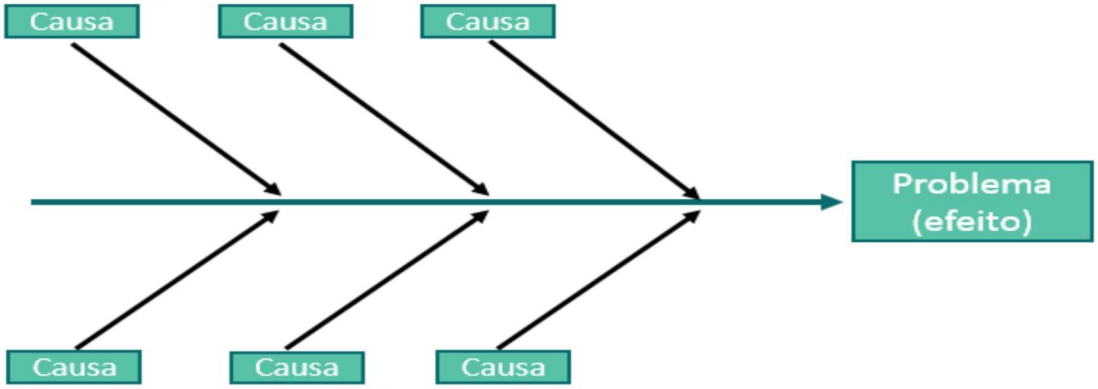
Fonte: ENAP, 2018

As causas são as condições que originam a ocorrência de um evento, também conhecidas como fatores de risco, podendo ter suas origens tanto no ambiente interno quanto externo. O risco é a probabilidade de um evento ocorrer e impactar negativamente o alcance dos OE, enquanto que a consequência representa o resultado de um evento de risco sobre os OE.

O processo de identificação de riscos prevê a aplicação de uma metodologia específica para identificar eventos de risco. Dentre as principais técnicas utilizadas estão os *workshops, brainstorming*, diagrama de causa e efeito, *bow-tie*, entre outras.

De maneira resumida, o diagrama de causa e efeito (Figura nº 4), também conhecido como diagrama de *Ishikawa* ou espinha de peixe, é uma técnica utilizada para identificar possíveis causas de um problema. Neste diagrama, cada "espinha" representa uma causa e a "cabeça" representa o problema causado por essas causas. Este método pode ser aplicado em *workshops* e sessões de *brainstorming*, começando pela identificação de um problema e, em seguida, explorando suas possíveis causas. Pode ser combinado também com o método dos "cinco porquês" para aprofundar a análise de cada causa, questionando repetidamente o motivo por trás de cada "espinha" (Falconi, 2004).

Figura 4 - Diagrama de Causa e Efeito

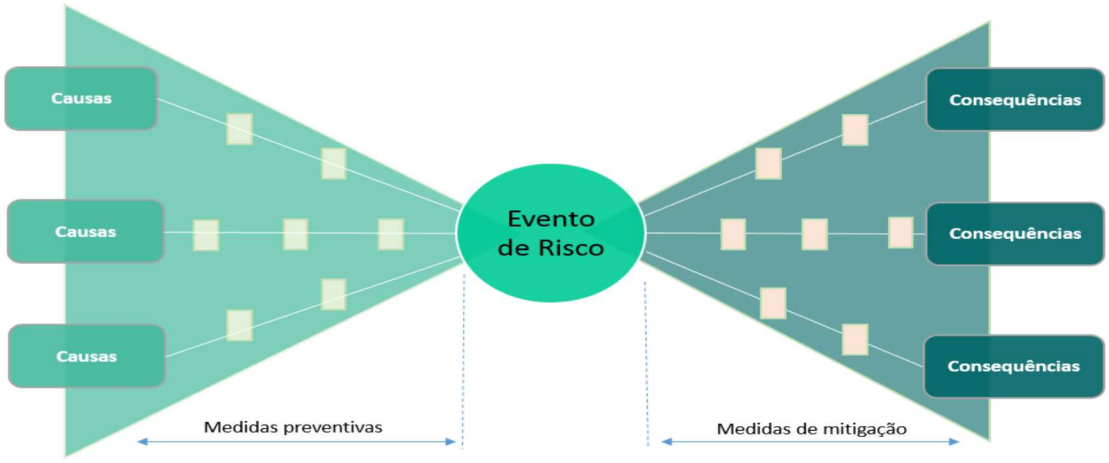


Fonte: Falconi, 2004

Outra técnica amplamente utilizada é o método *bow-tie* (Figura nº5), também conhecido como gravata borboleta. Este método é considerado uma evolução do diagrama de causa e efeito, pois permite identificar e analisar os diferentes caminhos que um evento de risco pode seguir. Isso ocorre porque um problema pode estar associado a diversas causas e consequências simultaneamente. Assim como no diagrama de causa e efeito, o processo começa com a identificação do problema, seguido pela análise das possíveis causas e consequências (ISO,2023).

Para concluir, é fundamental identificar estratégias para prevenir o risco e também mitigar as consequências. Essas medidas preventivas e mitigatórias são essenciais para garantir que os OE sejam alcançados, mesmo diante de possíveis eventos adversos.

Figura 5 - Método Bow-Tie



Fonte: ISO, 2023

Deve-se escolher a técnica mais favorável a identificação do risco à Integridade, mantendo a correção da gestão dos recursos e das atividades, reduzindo a desonestidade e desvios éticos.

Existem diversas abordagens para categorizar os eventos de risco. Alguns autores destacam a complexidade em definir categorias específicas para a natureza dos eventos. Por exemplo, Chapman (2001) menciona a dificuldade em estabelecer categorias claras de eventos de risco. Alguns modelos categorizam os riscos em quatro principais tipos: falha humana, falha organizacional, falha de projeto e falhas de planejamento. O *Project Management Institute* (2004) oferece um exemplo similar, dividindo os riscos em categorias como técnico, externo, organizacional e de gerenciamento de projetos.

Para efetivamente gerenciar os riscos, é crucial identificá-los e documentá-los de maneira adequada. Isso permite um acompanhamento contínuo, que deve ser uma prática habitual no processo de GR. Durante a identificação de um risco, deve-se registrar os eventos com suas causas e efeitos, considerando o resultado da análise do Ambiente, principalmente as ameaças e as fraquezas juntamente com os OE.

Alguns exemplos de riscos à integridade:

1) A Alta Administração ser influenciada por pressões externas, por abuso de poder, por tráfico de influência ou constrangimento ilegal, ocasionando a não consolidação da EGN como uma instituição de Altos Estudos e comprometendo as relações com outras instituições nacionais e estrangeiras (atrelar aos OE);

2) Contratação de familiar para ocupar cargo de confiança na EGN (atrelar aos OE);

3) Utilização de recursos públicos previstos na dotação orçamentária anual em desacordo com as atividades de Estudo e Pesquisa (atrelar aos OE);

4) Exercício de atividades incompatíveis com as atribuições do cargo, atuação como intermediário de interesses privados na EGN e recebimento de propina, presente ou pagamento indevido (atrelar aos OE); e

5) Divulgação de informações ou dados privilegiados, intencionalmente, de forma incorreta, em próprio proveito ou de terceiros, em razão das atividades exercidas na EGN (atrelar aos OE).

4.3 ANALÍSE DE EVENTOS DE RISCOS

O objetivo da análise de eventos de riscos é entender a natureza do risco e suas características de maneira abrangente, avaliando o nível de risco. Este processo analisa de forma detalhada as incertezas, as fontes de risco, as consequências potenciais, a probabilidade de ocorrência e a eficácia dos controles. É importante notar que um evento de risco pode ter múltiplas causas e consequências, afetando diversos OE.

A análise de riscos é conduzida em diferentes níveis de detalhamento e complexidade, dependendo dos objetivos estabelecidos, da disponibilidade e da confiabilidade das informações disponíveis, bem como dos recursos disponíveis para a análise. As técnicas utilizadas podem ser qualitativas, quantitativas ou uma combinação das duas, adaptadas de acordo com as circunstâncias específicas e os requisitos de uso. Para a análise dos eventos de risco identificados podem ser adotados os métodos qualitativos e quantitativos (Project Management Institute, 2004; Chapman, 2001).

Segundo o Project Management Institute (2004), a avaliação qualitativa é uma maneira rápida e econômica de estabelecer prioridades para o tratamento dos eventos de risco, identificando suas probabilidades de ocorrência e os impactos causados.

Na área de GR, as análises de probabilidades e impactos frequentemente são consideradas subjetivas em comparação com áreas como finanças, que possuem bancos de dados robustos e material estatístico para calcular probabilidades.

Enquanto o conceito de matriz de risco é amplamente utilizado, não há uma padronização evidente de tabelas para interpretar a probabilidade de ocorrência e os impactos para classificar riscos.

A análise de riscos muitas vezes se baseia em estatísticas e dados históricos, uma alternativa viável é consultar especialistas para obter informações quando os dados não estão prontamente disponíveis. Isso pode ajudar a mitigar a subjetividade e a aumentar a precisão na avaliação dos riscos organizacionais.

Para Kontovas (2005), há dois meios para determinar a probabilidade e o impacto ou consequência: por meio de estatística e de modelos. O primeiro, mais usado, é uma estimativa numérica que utiliza dados históricos, o segundo trabalha com índices de probabilidade.

Para identificar as práticas mais utilizadas, Lyons; Skitmore (2004) pesquisaram o GR em 44 (quarenta e quatro) empresas de engenharia na Austrália e constataram que a identificação e análise de riscos são as etapas mais frequentemente usadas, assim como o *brainstorming* é a técnica mais comumente empregada para a identificação de riscos, sendo a avaliação qualitativa o método mais utilizado para a etapa de avaliação de riscos.

Essa etapa visa avaliar os eventos de risco que foram identificados considerando os componentes principais, como causas e consequências. Sendo, as causas relacionadas à probabilidade de o evento ocorrer, enquanto as consequências o impacto que o evento pode ter caso se materialize.

A avaliação de riscos deve ser conduzida através de análises quantitativas, qualitativas ou uma combinação dessas abordagens. Além disso, é importante diferenciar os riscos inerentes, que são os riscos brutos sem considerar controles, dos riscos residuais, que já foram tratados por algum tipo de controle. Essas análises ajudam a entender melhor a natureza e a severidade dos riscos enfrentados pela organização.

Risco Inerente é o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto. (Art. 2º, XIV, IN Conjunta MP/CGU Nº 01/2016). Pode ser acompanhado por meio dessa matriz abaixo (Figura nº 6): (MP/CGU, 2016).

Figura 6 - Tabela de Acompanhamento de Risco Inerente

Objetivo:								
Identificação	**Análise**		**Avaliação**				**Tratamento**	
Risco Inerente	**Causa (fonte + vulnerabil)**	**Efeito (consequência)**	**P**	**I**	**(P)x(I)**	***Ranking***	**Medidas (Preventivas/ Corretivas**	**Plano Ação Quem/ Quando/ Como**
1								
2								
3								
...								

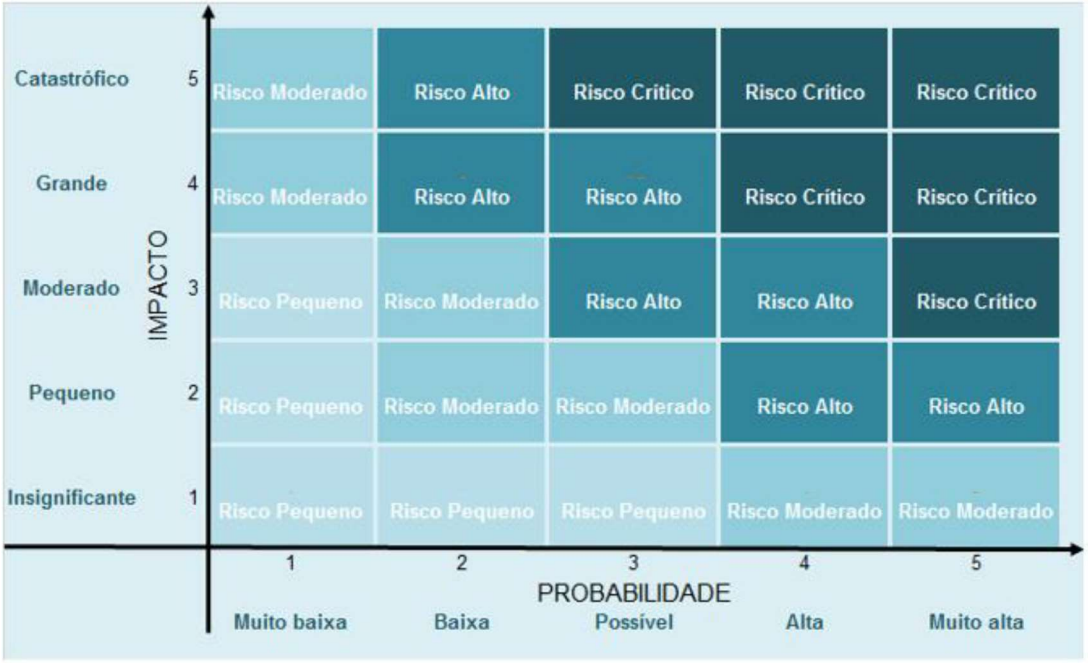
Fonte: ISO, 2023

Já o Risco Residual é o risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (MP/CGU, 2016).

As ações gerenciais correspondem aos controles internos da gestão, que compreendem um conjunto integrado de regras, procedimentos, diretrizes, protocolos, sistemas informatizados, conferências e tramitação de documentos e informações, entre outros. Esses controles são operacionalizados de forma coordenada pela direção e pelo corpo de servidores das organizações, visando enfrentar os riscos e proporcionar segurança razoável na realização da missão da entidade (MP/CGU, 2016).

Para calcular o Risco Inerente, realiza-se a mensuração com base na probabilidade e no impacto de ocorrência de cada evento de risco. Depois é crucial identificar, avaliar e descrever os controles que respondem aos eventos de riscos. Ao completar essas etapas, obtém-se o nível de risco para cada evento, conforme indicado na matriz de impacto e probabilidade (Figura nº 7).

Figura 7 – Matriz de Impacto e propabilidade



Fonte: TCU (2018a).

Os parâmetros são expressos por meio de adjetivos dispostos em escala categórica ordinal.

Probabilidade = representada por: Muito baixa (1), Baixa (2), Possível (3), Alta (4) e Muito Alta (5);

Impactos = insignificante (1), pequeno (2), moderado (3), grande (4) e catastrófico (5).

O resultado do produto da probabilidade X impacto define o valor do risco, conforme o apetite de risco da organização.

Ranking dos Riscos: 0<R<=3 Baixa; 3<R<6 Média; R=>7 Alta

4.4 AVALIAÇÃO DOS RISCOS

A avaliação de riscos tem como propósito fundamentar as decisões. Esse processo compara os resultados da análise com os critérios pré-estabelecidos para verificar se serão necessárias ações adicionais. Isso pode resultar em decisões de não fazer nada ou iniciar o tratamento de riscos, manter os controles ou até mesmo reconsiderar os OE. É importante que tais decisões considerem sempre as consequências reais para as organizações.

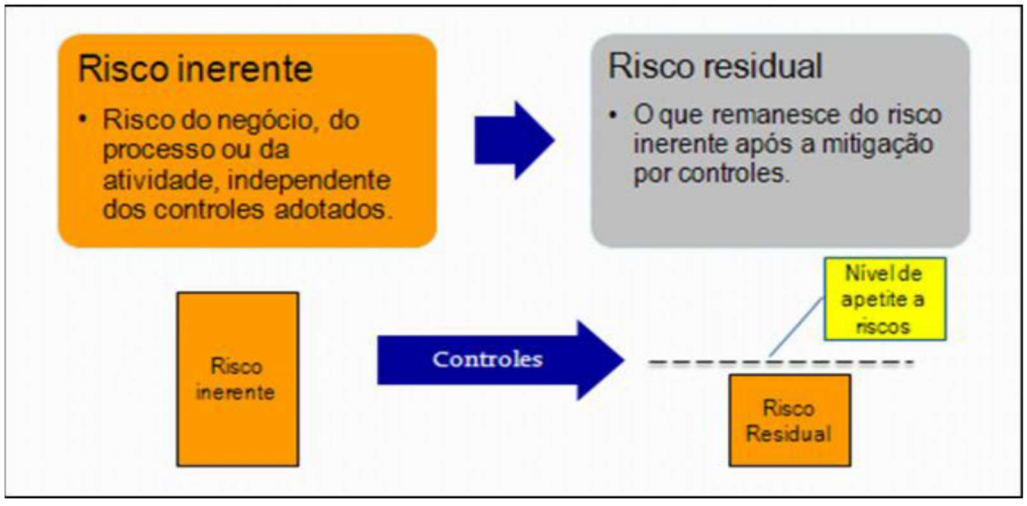
Todos os resultados devem ser registrados, comunicados e validados pela alta administração. Após a mensuração, uma prática recomendada é apresentar os eventos de risco em uma matriz para uma visualização clara. A matriz de risco é uma ferramenta que posiciona os eventos conforme sua frequência e impacto, facilitando a identificação dos eventos mais críticos. Vários autores têm adotado o conceito de matriz de risco, como Hewett et al. (2004); Garvey and Lansdowne (1998); Modarres (2006); Conrow (2003); Kerzner (2005); Project Management Institute (2004); entre outros.

4.5 RESPOSTA A RISCO

Referem-se às políticas e procedimentos estabelecidos e implementados para mitigar os riscos, também conhecidos como procedimentos de controle e com o objetivo de transformar um risco inerente para um risco residual. (Figura nº 8). Essas atividades devem ser aplicadas de maneira abrangente em toda a organização. Elas englobam uma variedade de controles internos, além da elaboração de planos de contingência antecipados para responder a ocorrências de eventos de risco.

Uma única atividade de controle pode abordar múltiplos riscos, enquanto em outros casos pode ser necessário implementar diversas atividades para responder a um único risco específico.

Figura 8 - Cálculo do Risco Residual



Fonte: ISO, 2023

Após determinar o nível de risco residual, é crucial selecionar a estratégia apropriada para a devida resposta ao evento de risco. Essa escolha depende da exposição aos riscos estabelecidos previamente, comparada à análise realizada na matriz.

A estratégia de resposta é definida em conjunto com a matriz de riscos. Com base no nível de risco residual, sugere-se uma ação correspondente para mitigação.

Todas as ações de respostas aos eventos de risco devem estar alinhadas ao apetite aos riscos, considerando a relação custo-benefício e como a resposta impactará a probabilidade e o impacto do evento. É essencial a designação de um responsável pelas respostas aos riscos, chamado de proprietário do risco.

Esse gestor do risco tem a prerrogativa de ajustar a resposta ao risco, seja para aceitar o risco sem adotar controle, ou para adotar uma ação de controle quando necessário, sempre validando com os níveis superiores.

Para tal, pode-se recorrer a controles, que são medidas para ajustar os níveis de risco, incluindo a implementação de novos controles ou a revisão dos controles existentes.

A escolha da ação mais apropriada para dar resposta aos riscos envolve equilibrar os potenciais benefícios com os OE, considerando os custos, esforços e eventuais desvantagens. As ações de tratamento de riscos não são exclusivas entre si e podem não ser adequadas em todas as circunstâncias. Dentre as ações para gerenciar o risco, pode-se incluir as seguintes estratégias:

- Eliminar: encerrar a atividade que representa a ameaça;
- Transferir: delegar para terceiros (por exemplo, através de contratações, Seguros);
- Mitigar: implementar ações de controle (como controles internos); e
- Aceitar: tolerar a exposição ao risco.

A justificativa para o tratamento de riscos vai além das considerações econômicas, abrangendo a reputação e considerando todas as obrigações, valores, objetivos estratégicos, percepções, compromissos voluntários e as opiniões das partes interessadas, buscando as formas mais adequadas de comunicação e consulta com elas.

Mesmo quando planejado e implementado, o tratamento de riscos pode não obter os resultados que eram esperados e também pode resultar em consequências não intencionais. Portanto, é essencial que o monitoramento e a análise crítica sejam

partes integrantes da implementação do tratamento de riscos, garantindo que as estratégias adotadas permaneçam eficazes ao longo do tempo.

A cultura organizacional relacionada ao tratamento de riscos também pode identificar novos riscos que exigem gestão adequada. Não havendo um tratamento viável ou se as estratégias adotadas não reduzirem o risco, é importante registrar e manter uma análise crítica contínua sobre o risco remanescente.

A alta administração das organizações deve estar plenamente ciente do risco remanescente após o tratamento. Esse risco residual deve ser documentado, monitorado e submetido a análise regular, considerando-se a aplicação de tratamentos adicionais, quando necessário.

4.6 INFORMAÇÃO, COMUNICAÇÃO E MONITORAMENTO

O acesso a informações confiáveis, tem um papel crucial na gestão eficaz da integridade, riscos e controles internos para alcançar os OE. Para tanto, é essencial que o fluxo de comunicação permita uma troca bidirecional de informações, garantindo que as diretrizes estratégicas do Comitê de Gestão Estratégica sejam disseminadas para todos da organização.

A comunicação externa também é importante para mitigar riscos de respostas inadequadas às necessidades da sociedade. O monitoramento abrangente da estrutura de governança e gestão de integridade, riscos e controles internos é fundamental para alinhar essa estrutura com os OE. Os planos são elaborados e submetidos à avaliação das instâncias. Ao identificar deficiências são formuladas recomendações pelas instâncias responsáveis.

A comunicação entre as instâncias de gestão de integridade, riscos e controles internos ocorre de acordo com os níveis de relacionamento estabelecidos. O Mapa de Risco assume um papel central no monitoramento da gestão de integridade, riscos e controles, juntamente com o Relatório do Plano de Controles, elaborado conforme a periodicidade definida pelas instâncias de supervisão, sendo essencial para acompanhar as atividades realizadas pela unidade.

Após a implementação, é crucial que os controles sejam continuamente avaliados quanto ao seu desenho e operação. Esta avaliação deve ser conduzida de forma contínua pelo gestor, garantindo que os controles estejam presentes e funcionando adequadamente. Durante o monitoramento, é essencial verificar se os

controles estão perdendo eficácia ou se tornando obsoletos. Também é possível que não estejam sendo aplicados conforme planejado, o que os tornaria desnecessários para mitigar o risco. Além dos testes realizados, se utiliza as reclamações, as denúncias levantadas na ouvidoria, relatórios, recomendações ou demandas de órgãos como o Ministério da Transparência e Controladoria Geral da União e o Tribunal de Contas da União, além de mudanças nos OE e nas normas e regulamentações vigentes.

As organizações devem estabelecer indicadores específicos para acompanhar e monitorar os controles existentes.

Pelo monitoramento haverá a garantia e o aprimoramento da qualidade e eficácia dos resultados do processo. É fundamental que seja contínuo e que haja uma análise crítica e seus resultados sejam planejados, com responsabilidades claramente definidas e aplicados em todas as fases. Isso engloba o planejamento, a análise das informações, o registro dos resultados, o feedback e sua integração em todas as atividades da gestão, medição e relatórios.

Para que a MB consiga implementar um GR à integridade, é necessário elaborar planos de comunicação e capacitação relacionados aos temas do Programa de Integridade e verificar se estes planos foram implementados, verificar se as ações desenvolvidas nos últimos dois exercícios contemplaram os seguintes temas:

a) Fomento à postura ética prevista no Código de Ética do Servidor Público do Poder Executivo Federal, no Código de Conduta do Servidor e em outros normativos;

b) Compromisso da alta administração com o Programa de Integridade;

c) Conhecimento da estrutura e da importância do Programa de Integridade e de seu respectivo Plano;

d) Fomento à gestão de riscos à integridade;

e) Prevenção de situações de conduta profissional inadequada, conflito de interesses, ameaças à independência funcional, nepotismo, corrupção, fraude e emprego irregular de verbas públicas, desvio de pessoa ou de recursos materiais, uso indevido ou manipulação de informações obtidas em razão das atividades exercidas; recebimento e oferecimento indevido de brindes e presentes;

f) Incentivo à integridade em contratações;

g) Incentivo ao monitoramento das medidas de controle estabelecidas no Plano de Integridade com o objetivo de mitigar a possibilidade de ocorrência de violações de integridade;

h) Incentivo à realização de denúncias e divulgação das medidas de proteção ao denunciante; e

i) Acompanhamento das medidas disciplinares.

5 CONCLUSÃO

Risco à Integridade refere-se à probabilidade de ocorrência de eventos incertos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, os quais têm o potencial de comprometer os valores e os padrões estabelecidos pela Instituição, assim como a consecução de seus OE.

Conforme instruções emanadas pela Portaria nº 1.089, de 25 de abril de 2018, do Ministério da Transparência e Controladoria-Geral da União (CGU) (2018), que, por sua vez, estabelece os procedimentos necessários à estruturação, à execução e ao monitoramento dos Programas de Integridade preconizados no Decreto nº 9.203, de 22 de novembro de 2017, foram apresentados os Programas de Integridade da Caixa Econômica Federal, do Banco de Desenvolvimento (BNDES), do Banco Central do Brasil e da Marinha do Brasil com o objetivo de verificar quais eram as similaridades e as singularidades e que se combinados poderia gerar um conhecimento a ser implementado na Marinha do Brasil.

Em consonância com as boas práticas de governança da gestão pública, o estudo focou nos quatro eixos de atuação do Programa:

- Comprometimento e Apoio da Alta Administração;
- Unidade Responsável e Instâncias de Integridade;
- Gerenciamento dos Riscos à Integridade; e
- Estratégias de Monitoramento Contínuo.

Adicionalmente e fazendo parte da estrutura de governança foi verificado:

- Promoção da ética, de regras de conduta e procedimentos de responsabilização;
- Promoção da transparência e do acesso à informação;
- Tratamento de denúncias e conflitos de interesse;
- Aprimoramento da GR e do controle interno; e
- Administração de pessoal, bens e valores.

Na primeira seção foi apresentado todo o arcabouço teórico dos principais conceitos utilizados na pesquisa. Foi utilizado o COSO ERM, referência no gerenciamento de riscos empresarial, os conceitos direcionados à Integridade e suas respectivas derivadas e os conceitos que envolvem a GR.

Na segunda seção de texto apresentamos os Programas de Integridade de forma comparativa, confrontando as estruturas dos Bancos com a Marinha do Brasil

e confrontando com a hipótese de não haver um gerenciamento de riscos estruturado na Marinha do Brasil.

Dessa comparação percebeu uma grande similaridade nas estruturas de governança, no cumprimento das fases de implementação dos Programas de Integridade, na prontificação do Plano de Integridade e seu monitoramento. Além disso, todas as instâncias estão consideradas e estruturadas para o acompanhamento do programa. Especificamente quanto a estrutura do gerenciamento de riscos, todos os bancos demonstraram uma fragilidade por não apresentarem todas as etapas do gerenciamento de riscos. Comparando com a Marinha do Brasil percebe-se que os resultados confirmam a hipótese.

Na terceira seção de texto foi apresentado uma prescrição de como a Marinha deve reforçar seu gerenciamento de riscos à integridade com a estruturação bem definida das etapas de identificação dos riscos, análise dos riscos, respostas aos riscos e monitoramento. Para cada risco identificado deverá ter um acompanhamento e respostas que reduzirão a probabilidade da ocorrência e se não for possível reduzir, verificar a possibilidade de eliminar. Comparando os resultados da pesquisa, confirmamos a hipótese e a possibilidade de adoção pela Marinha de um gerenciamento de riscos estruturado e acompanhado.

Os três bancos analisados permitiram estabelecer as relações centrais e os parâmetros de qualificação que orientaram avaliar a hipótese e a pesquisa. Permitiram também extrair proposições ao desenvolvimento da pesquisa. Os temas centrais estudados foram as seguintes: a estrutura de governança, bem registrada nos normativos, com apoio da alta administração, com a escolha de uma instância, com políticas de gerenciamento de riscos e monitoramento; e a prática ou ausência de prática quando se fala de gerenciamento de riscos.

A hipótese formulada foi a de que a Marinha não possui ainda uma metodologia bem estruturada de gerenciamento de riscos à integridade e que pode se tornar uma fragilidade e um comprometimento à sua imagem. A consequência da hipótese foi que a Marinha fica exposta aos riscos que envolvem conflito de interesse, nepotismo etc.

Os parâmetros de comparação que orientaram a estrutura de desenvolvimento da argumentação, foram: Estrutura da Governança, Apoio da Alta Administração, Criação de Instâncias, Gerenciamento de riscos, Monitoramento, capacitação, auditoria interna, Controle Interno, enfim toda a estrutura do Programa de Integridade com foco no gerenciamento de riscos.

Foi verificada a similaridade no que tange ao cumprimento das determinações emanadas pelos órgãos públicos competentes em relação a implantação do Programa de Integridade, por outro lado também confirmamos a hipótese. Vimos que tanto os bancos quanto a Marinha do Brasil podem aprofundar o estudo sobre o gerenciamento de riscos com suas etapas bem definidas.

A questão que colocamos foi: existe um gerenciamento de riscos a integridade bem estruturado? A pesquisa nos permitiu concluir contrariamente a hipótese, ou seja, que a Marinha ainda não possui de forma estruturada um gerenciamento de riscos à integridade, adequado ao tamanho da instituição.

Mas talvez tão importante quanto o que a pesquisa concluiu, ou até mais, é o que ela sugere. E ela sugere que a imagem da MB pode ser afetada por riscos de integridade.

O processo do gerenciamento de riscos da MB precisa de aprimoramentos, abrangendo todas as etapas essenciais: identificação, análise, avaliação, tratamento, comunicação e monitoramento. Cada uma dessas etapas é fundamental para garantir uma abordagem sistemática e abrangente na identificação e mitigação de riscos que possam impactar a instituição.

Identificação: possuir mecanismos estabelecidos para identificar riscos em diversas áreas de atuação. Esses mecanismos incluem a análise de processos internos, auditorias, feedback de *stakeholders* e monitoramento de mudanças no ambiente regulatório.

Análise: Os riscos identificados são analisados para compreender suas causas, impactos potenciais e a probabilidade de ocorrência. Essa análise detalhada permite uma compreensão aprofundada dos riscos, facilitando a priorização dos mesmos.

Avaliação: Após a análise, os riscos são avaliados para determinar seu nível de severidade. Essa avaliação considera tanto a probabilidade quanto o impacto potencial dos riscos, permitindo uma classificação clara e objetiva.

Tratamento: Com base na avaliação, são desenvolvidas e implementadas estratégias de tratamento de riscos. Essas estratégias podem ser a mitigação, aceitação, transferência ou eliminação dos riscos, dependendo de sua natureza e gravidade.

Comunicação: A comunicação eficaz é um pilar central na gestão de riscos. Que se tenha a garantia de que todas as partes interessadas, internas e externas,

sejam devidamente informadas sobre os riscos identificados e as ações tomadas para mitigá-los. Essa transparência é crucial para manter a confiança e a credibilidade da organização.

Monitoramento: Manter um sistema contínuo de monitoramento de riscos, revisando e atualizando regularmente suas avaliações e estratégias de mitigação. Esse monitoramento constante garante que a organização permaneça proativa na gestão de riscos, adaptando-se rapidamente a novos desafios e oportunidades.

No entanto, uma análise mais detalhada revela uma ausência significativa no que diz respeito à correta identificação e monitoramento de riscos de integridade. Riscos de integridade, que incluem fraudes, corrupção, e outras formas de conduta inadequada, são críticos para a manutenção da confiança e da reputação da MB.

A falta de identificação e monitoramento adequado desses riscos pode expor a MB a sérias vulnerabilidades, comprometendo a eficácia geral do seu processo de gestão de riscos. Riscos de integridade são especialmente perniciosos, pois podem minar a confiança pública e a credibilidade da instituição, além de trazer consequências legais e financeiras.

Para fortalecer sua gestão de riscos, é imperativo que a MB:

Desenvolva mecanismos específicos para a identificação de riscos de integridade, incluindo auditorias internas focadas em fraudes e corrupção, programas de denúncia anônima e treinamento regular para seu pessoal sobre ética e conformidade.

Implemente um sistema de monitoramento contínuo para riscos de integridade, assegurando que qualquer sinal de conduta inadequada seja rapidamente identificado e tratado.

Fortaleça a comunicação e a transparência em torno de questões de integridade, criando uma cultura organizacional que valorize a ética e a responsabilidade.

Ao integrar essas práticas na sua gestão de riscos, a MB poderá garantir uma abordagem mais completa e robusta, protegendo a instituição contra todas as formas de risco e assegurando o cumprimento da sua missão.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISSO/IEC 31000**: Gestão de Riscos: diretrizes. Rio de Janeiro, RJ: ABNT, 2018.

BAKER, S. and PONNIAH, D. and SMITH, S. (1999, July). **Survey of risk management in major U.K. companies.** Journal of Professional Issues in Engineering Education and Practice, 125(3), 94-102. Disponível em: http://dx.doi.org/10.1061/(ASCE)1052-3928(1999)125:3(94)

BCB - Banco Central do Brasil. **Gestão Integrada de Riscos no Banco Central do Brasil**. Brasília, DF: Banco Central do Brasil, 2017a.

BCB - Banco Central do Brasil. **Portaria nº 93.608, de 29 de maio de 2017**. Constitui o Comitê de Governança, Riscos e Controles do Banco Central do Brasil. Brasília, DF: Banco Central do Brasil, 2017b.

BCB - Banco Central do Brasil. (2019). **Portaria nº 104.238, de 9 de agosto de 2019**. Cria o Comitê de Integridade do Banco Central do Brasil. Brasília, DF: Banco Central do Brasil, 2019.

BCB - Banco Central do Brasil. **Plano de Integridade**. Banco Central do Brasília, DF: Banco Central do Brasil, 2021a.

BCB - Banco Central do Brasil. Resolução **BCB nº 165, de 23 de novembro de 2021**. Dispõe sobre o Regimento Interno da Comissão de Ética do Banco Central do Brasil (CEBCB). Brasília, DF: Banco Central do Brasil, 2021b.

BCB - Banco Central do Brasil. Resolução **BCB nº 236, de 27 de julho de 2022**. Política de Conformidade (*Compliance*) do Banco Central do Brasil. Brasília, DF: Banco Central do Brasil, 2022.

BCB - Banco Central do Brasil. Resolução **BCB nº 333, de 10 de agosto de 2023**. Divulga a Política de Controles Internos da Gestão do Banco Central do Brasil. Brasília, DF: Banco Central do Brasil, 2023a.

BCB - Banco Central do Brasil. Resolução **BACEN nº 5.076,** de 18 de maio de 2023 que altera a Resolução **BACEN nº4.557**, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital. Brasília, DF: Banco Central do Brasil, 2023b.

BNDES - BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL**.** **Política Corporativa de Integridade do Sistema BNDES**. Rio de Janeiro, RJ: Banco Nacional de Desenvolvimento Econômico e Social, 2020.

BNDES - BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL**.** **Resolução CA BNDES nº 12, de 2023**. Política corporativa de gestão de risco operacional e controle interno do sistema BNDES (PROCI) Rio de Janeiro, RJ: Banco Nacional de Desenvolvimento Econômico e Social, 2023.

BRASIL. Congresso Nacional, **Lei nº 6.880, de 09 de dezembro de 1980**. **Estatuto dos Militares**. Promulgada em 9 de dezembro de 1980. Brasília, DF: Congresso Nacional, 1980.

BRASIL. Congresso Nacional, **Lei Nº 12.527, de 18 de novembro de 2011**. **Lei de Acesso à Informação**. Promulgada em 18 de novembro de 2011. Brasilia, DF: Congresso Nacional, 2011.

BRASIL. Congresso Nacional **Lei nº 12.846, de 1º de agosto de 2013. Lei Anticorrupção**. Promulgada em 30 de novembro de 2022. Brasília, DF: Congresso Nacional, 2013a.

BRASIL. Congresso Nacional**. Lei nº 12.813, de 16 de maio de 2013.** Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego publicada em Diário Oficial da União. Brasília, DF: Congresso Nacional, 2013b.

BRASIL. Congresso Nacional. **Lei nº 13.303, de 30 de junho de 2016.** Lei das Estatais. Promulgada em 30 de junho de 2016. Brasília, DF: Congresso Nacional, 2016.

BRASIL. Congresso Nacional. **Lei nº 13.709, 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Promulgada em 14 de agosto de 2018. Brasília, DF: Congresso Nacional, 2018.

BRASIL. Controladoria-Geral da União. **Instrução Normativa CGU nº 03, de 9 de junho de 2017**. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Brasília, DF: Controladoria-Geral da União, 2017a.

BRASIL. Controladoria-Geral da União. **Instrução Normativa CGU nº 08, de 6 de dezembro de 2017**. Aprova o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Brasília, DF: Controladoria-Geral da União, 2017b.

BRASIL. Marinha do Brasil. **Portaria nº 244/MB,** de 12 de agosto de 2020. Aprova diretrizes para a incorporação e integração da mulher nos meios operativos e as regras de conduta e convivência entre militares da Marinha. Rio de Janeiro, RJ: Marinha do Brasil, 2020.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **EMA 136**: Normas a respeito das tradições Navais, do comportamento pessoal e dos cuidados marinheiros. Brasília, DF: Marinha do Brasil, 2021. Disponível em: http://www.ema.mb/publicações. Acesso em: 12 jun. 2024.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **EMA 130**: Manual de visitas, inspeções e reuniões funcionais da marinha - Vol. I e II. Brasília, DF: Marinha do Brasil, 2022. Disponível em: http://www.ema.mb/publicações. Acesso em: 18 jun. 2024.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **EMA 137**: Doutrina de Liderança da Marinha. Brasília, DF: Marinha do Brasil, 2018. Disponível em: http://www.ema.mb/publicações. Acesso em: 08 jul. 2024.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **EMA 138**: Normas para o serviço de informações ao cidadão no âmbito da Marinha do Brasil (SIC-MB). Brasília, DF: Marinha do Brasil, 2020. Disponível em: http://www.ema.mb/publicações. Acesso em: 18 jul. 2024.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **EMA 414**: normas para a salvaguarda de materiais controlados, dados, informações, documentos e materiais Sigiloso na Marinha. Brasília, DF: Marinha do Brasil, 2005. Disponível em: http://www.ema.mb/publicações. Acesso em: 20 jul. 2024.

BRASIL. Marinha do Brasil. Secretaria Geral da Marinha. **SGM 107**: Normas gerais da administração - Vol. I. Brasília, DF: Marinha do Brasil, 2011. Disponível em: http://www.sgm.mb/?q=normas. Acesso em: 14 mai. 2024.

BRASIL. Marinha do Brasil. Secretaria Geral da Marinha. **SGM 601**: Normas sobre auditoria, análise e apresentação de contas. Brasília, DF: Marinha do Brasil 2014. Disponível em: http://www.sgm.mb/?q=normas. Acesso em: 20 mai. 2024.

BRASIL. Marinha do Brasil. Diretoria Geral de Pessoal da Marinha. **DGPM 315**: Normas sobre justiça e disciplina na Marinha. Brasília, DF: Marinha do Brasil, 2011. Disponível em: http://www.dgpm.mb/. Acesso em: 19 mai. 2024.

BRASIL. Marinha do Brasil. Diretoria Geral de Pessoal da Marinha. **DGPM 319**: Normas para a conduta ético-militar e atividades sociais no âmbito militar. Brasília, DF: Marinha do Brasil, 2022. Disponível em: http://www.dgpm.mb/. Acesso em: 19 mai. 2024

BRASIL. Marinha do Brasil. Diretoria Geral de Pessoal da Marinha. **PESSOALMARINST nº 1**: Normas para a conduta ético-militar e atividades sociais no âmbito militar. Brasília, DF: Marinha do Brasil, 2023.

BRASIL. Marinha do Brasil. **Decreto nº 88.545, de 26 de julho de 1983**. Aprova o Regulamento Disciplinar para a Marinha e dá outras providências. Brasília, DF: Marinha do Brasil, 1983. Disponível em :http://www.planalto.gov.br/decreto10000. Acesso 4 abr 2024

BRASIL. Marinha do Brasil. **Decreto nº 95.480, de 13 de dezembro de 1987**. Dá nova redação para a Ordenança Geral para o Serviço da Armada. Brasília, DF: Marinha do Brasil, 1987. Disponível em: http://www.planalto.gov.br/decreto10000

BRASIL. Marinha do Brasil. Diretoria Geral do Pessoal da Marinha. **Portaria nº 59/2021, da DGPM.** Comissão de Ética dos Servidores Civis da MB. Diretoria Geral do Pessoal da Marinha. Rio de Janeiro, RJ: Marinha do Brasil, 2021.

BRASIL. Marinha do Brasil. Estado Maior da Armada. **Portaria nº 336/2018 do EMA** Plano de Integridade da Marinha do Brasil. Brasília, DF: Marinha do Brasil, 2018.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União. **Instrução Normativa Conjunta MP/CGU n.º 01, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, DF: Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União, 2016.

BRASIL. Ministério da Transparência, Fiscalização e Controladoria-Geral da União. **Portaria nº 915, de 12 de abril de 2017**. Institui a Política de Gestão de Riscos – PGR do Ministério da Transparência, Fiscalização e Controladoria-Geral da União – CGU. Brasília, DF: Ministério da Transparência, Fiscalização e Controladoria-Geral da União, 2017. Disponível em: https://repositorio.cgu.gov.br/handle/1/41321

BRASIL. Ministério da Transparência, Fiscalização e Controladoria-Geral da União - CGU. **Portaria nº 1.089, de 25 de abril de 2018**. Brasília, DF: Ministério da Transparência, Fiscalização e Controladoria-Geral da União, 2018. Disponível em: https://repositorio.cgu.gov.br

BRASIL. Ministério da Transparência, Fiscalização e Controladoria-Geral da União - CGU. **Portaria nº 57, de 4 de janeiro de 2019**. Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. Brasília, DF: Ministério da Transparência, Fiscalização e Controladoria-Geral da União, 2019. Disponível em:https://repositorio.cgu.gov.br

BRASIL. Ministério do Meio Ambiente. **Manual de Gestão de Riscos e Controle Interno**. Instituto de Pesquisas Jardim Botânico do Rio de Janeiro – JBRJ. Rio de Janeiro, RJ: Ministério do Meio Ambiente, 2020.

BRASIL. Ministério do Planejamento, Orçamento e Gestão (MPOG). **Portaria nº 426, de 30 de dezembro de 2016**. Brasília, DF: Ministério do Planejamento, Orçamento e Gestão, 2016. Disponível em: http://www.gov.br> legislaçãogeral>portarias

BRASIL. Presidência da República**. Decreto nº 1.171, de 22 de junho de 1994**. Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal. Brasília, DF: Presidência da República, 1994. Disponível em: http://www.planalto.gov.br/decreto10000

BRASIL. Presidência da República**. Decreto nº 6.029, de 1º de fevereiro de 2007**. Define as atribuições dos órgãos do sistema de Ética do Executivo. Brasília, DF: Presidência da República, 2007. Disponível em: http://www.planalto.gov.br/decreto10000

BRASIL. Presidência da República**. Decreto nº 8.945, de 27 de dezembro de 2016**. Regulamenta, no âmbito da união, a lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da união, dos estados, do distrito federal e dos municípios. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/decreto10000

BRASIL. Presidência da República. **Decreto 9.203, de 22 de novembro de 2017**: Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, Brasília, DF: Presidência da República, 2017.

BRASIL. Presidência da República**. Decreto nº 9.492, de 5 de setembro de 2018**. Regulamenta a Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo federal, e altera o Decreto nº 8.910, de 22 de novembro de 2016, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Transparência, Fiscalização e Controladoria-Geral da União. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/decreto10000

BRASIL. Presidência da República**. Decreto nº 10.153, de 3 de dezembro de 2019**. Dispõe sobre as salvaguardas de proteção à identidade dos denunciantes de ilícitos e de irregularidades praticados contra a administração pública federal direta e indireta e altera o Decreto nº 9.492, de 5 de setembro de 2018. Brasília, DF: Presidência da República**,** 2019. Disponível em: http://www.planalto.gov.br/decreto10000

BRASIL. Presidência da República**. Decreto nº 11.529, de 16 de maio de 2023**. Instituiu o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF: Presidência da República, 2023. Disponível em: http://www.planalto.gov.br/decreto10000. Acesso em 15 maio 2024.

CEF - Caixa Econômica Federal. **Estatuto Social**. Brasília, DF: Caixa Econômica Federal, 2017.

CEF - Caixa Econômica Federal. **Programa de Integridade**. Brasília, DF: Caixa Econômica Federal, 2021.

CEF - Caixa Econômica Federal. **Política de Controle Interno, *Compliance* e Integridade**. Brasília, DF: Caixa Econômica Federal, 2023.

CEP - Comissão de Ética Pública. Resolução da **CEP nº 10, de 29 de setembro de 2008**. Brasília, DF: Comissão de Ética Pública, 2008.

CHAPMAN, R. J. (2001). **The controlling influences on effective risk identification and assessment for construction design management**. International Journal of Project Management, 19, 147-160. Disponível em: http://dx.doi.org/10.1016/S0263-7863(99)00070-8.

CLARK, R. C. and PLEDGER, M. and NEEDLER, H. M. J. (1990, Feb.). **Risk analysis in the evaluation of non-aerospace projects**. International Journal of Project Management, 8(1), 14-24. Disponível em: http://dx.doi.org/10.1016/0263-7863(90)90004-U

CMN - Conselho Monetário Nacional. Resolução **CMN nº 4.943, de 23 de fevereiro de 2017**. Brasília, DF: Comissão de Ética Pública, 2017.

CMN - Conselho Monetário Nacional. Resolução **CMN nº 4.557, de 23 de fevereiro de 2017**. Brasília, DF: Comissão de Ética Pública, 2017.

CMN - Conselho Monetário Nacional. Resolução **CMN nº 4.968, de 25 de novembro de 2021**. Brasília, DF: Conselho Monetário Nacional, 2021.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework: Executive Summary. New York: COSO, 2004.Disponível em: https://www.coso.org/_files/ugd/3059fc_ae81f45d98474c9188045cbacbd510bf.pdf. Acesso em: 17 mar.2024

CONROW, E. H. **Effective risk management: some Keys to success**. 2nd. Reston: American Institute of Aeronautics and Astronautics, Inc, 2003.
CPC - Conselho de Prevenção da Corrupção. **Resolução de 8 de janeiro de 2020**. Sobre gestão de conflitos de interesses no setor público. Disponível em: https://www.cpc.tcontas.pt/index.html. Acesso em: 02 ago. 2024.

ENAP- Escola Nacional de Administração Pública. **Implementando a Gestão de Riscos no Setor Público**. Brasília, DF: Escola Nacional de Administração Pública, 2018.

FALCONI, Vicente. ***Gestão da Qualidade Total****: da estratégia à operação*. 1. ed. Nova Lima: INDG Tecnologia e Serviços Ltda., 2004.

GARVEY, P. R. and LANSDOWNE, Z. F. (1998, June). **Risk matrix: an approach for identifying, assessing,and ranking program risks.** Air Force Journal of Logistics, 22(1), 18-21 and 31.

HEWETT, C. J. M. et al. (2004). **Towards a nutrient export risk matrix approach to managingagricultural pollution at source. Hydrology and Earth System Sciences**, 8(4), 834-845. Disponível em: http://dx.doi.org/10.5194/hess-8-834-2004

ISO - International Organization for Standardization. NBR ISO/ TS 31000: **Risk management** - Principles and guidelines. Geneva: ISO. 2023.

KERZNER, H. (2005). **Project management: a systems approach to planning, scheduling, and controlling**. 9th. New Jersey: John Wiley & Sons, Inc.

Kontovas, C. A. (2005). **Formal safety assessment: critical review and future role**. 163p. Thesis (Naval Archicteture and Marine Engineering) - National Technical University of Athens, Maritime Transport, Athens, Greece.

LYONS, T and **SKITMORE**, M. (2004). **Project risk management in the Queensland engineering construction industry: a survey.** International Journal of Project Management, 22, 51-61. Recuperado de http://dx.doi.org/10.1016/S0263-7863(03)00005-X

MILES, F. M. and Wilson Junior, T. G. (1998). **Managing project risk and the performance envelope**.In: Annual Applied Power Electronics Conference and Exposition, 13., 1998, Disneyland.Proceedings. Anaheim: IEEE.

MODARRES, M. (2006). **Risk analysis in engineering: techniques, tools, and trends**. Boca Raton: Taylor & Francis Group.

PMI - Project Management Institute (2004). Standards Committee. Conjunto de conhecimentos em gerenciamento de projetos (PMBOK). 3.ed. Newtonw Square: PMI.

TACHIZAWA, T.; FREITAS, A.A.V. **Estratégias de negócios**: lógica e estrutura do universo empresarial. Rio de Janeiro, Pontal, 2004.

TCU -Tribunal de Contas da União. **Referencial básico de gestão de riscos.** Brasília, DF: Tribunal de Contas da União, 2018.