| | |
|---|---|
| **GESTÃO TÍTULO** | Política de Riscos, Controles Internos e Conformidade |
| **CLASSIFICAÇÃO** | Documento Executivo |
| **REFERENCIAL NORMATIVO** | Lei Complementar nº 109, de 29 de maio de 2001<br>Resolução CGPC nº 13, de 1º de outubro de 2004<br>Lei nº 13.709, de 14 de agosto de 2018 |
| **ASSUNTO** | **[3]** Estabelecer as diretrizes para a gestão de risco, controles e conformidade da PREVIDÊNCIA BRB, objetivando fortalecer a governança corporativa e o cumprimento do referencial estratégico, primando pelos princípios éticos e de segurança na Entidade. |
| **ELABORADOR** | Área de Controle, Orçamento e Risco |
| **APROVAÇÃO** | **Revisão 00**<br>Aprovada na reunião 1050ª da Diretoria Executiva, de 12/12/2019<br>Aprovada na reunião 575ª do Conselho Deliberativo, de 27/01/2020 |
| | **Revisão 01**<br>Aprovada na reunião 1163ª da Diretoria Executiva, de 18/03/2022<br>Aprovada na reunião 612ª do Conselho Deliberativo, de 29/03/2022 |
| | **Revisão 02**<br>Aprovada na reunião 1233ª da Diretoria Executiva, de 31/05/2023<br>Aprovada na reunião 648ª do Conselho Deliberativo, de 27/06/2023 |
| | **Revisão 03**<br>Aprovada na reunião 1255ª da Diretoria Executiva, de 10/10/2023<br>Aprovada na reunião 654ª do Conselho Deliberativo, de 13/10/2023 |

**ÍNDICE**

## 1. CONSIDERAÇÕES INICIAIS

**[3]** A Política de Riscos, Controles Internos e Conformidade visará direcionamento para o desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos corporativos, controles internos e conformidade que terão o objetivo de identificar e tratar adequadamente os riscos inerentes à gestão da Entidade e dos Planos de Benefícios, estabelecer mecanismos que reforcem a boa conduta, a conformidade com a legislação e as normas internas e estimule o comportamento ético dos que se relacionam de forma direta ou indireta com a Previdência BRB, respeitando a fidúcia na administração de recursos dos Planos e a garantia ao contrato previdenciário, contribuindo, assim, para o alcance dos objetivos estratégicos e cumprimento do propósito institucional.

## 2. OBJETIVOS

**1.** Estabelecer as diretrizes e as principais atribuições associadas à função de gestão de riscos, controles e conformidade, observando as boas práticas de gestão e regulamentações aplicáveis.

**2. [3]** Aperfeiçoar a gestão de riscos, controles internos e conformidade, estabelecendo as boas práticas e fortalecendo a governança corporativa, com vistas a garantir segurança institucional, a rentabilidade e solvência dos Planos de Benefícios administrados.

**3. [3]** Prover a gestão dos riscos alicerçada na prevenção, identificação, monitoramento e controle dos fatores de riscos que impactam os objetivos da PREVIDÊNCIA BRB, em consonância com à missão e visão da Entidade.

**4.** Fortalecer a cultura de gestão de riscos, controle internos e conformidade com vistas à geração de valor agregado e à sustentabilidade do negócio e a perenidade da Entidade.

**5. [3]** Promover a ética e a integridade na Entidade e nas relações com a sociedade e com as partes relacionadas à PREVIDÊNCIA BRB.

**6.** Divulgar e promover o uso do canal de ética, principal ferramenta do sistema de *Compliance*, que produz indicadores para a gestão de riscos da Entidade.

**7. [3]** Monitorar o Programa de Integridade e *Compliance* e as ações do Plano de Integridade da Entidade, no intuito de detectar os riscos de integridade e aprimorar os processos para a prevenção de ilicitudes que favorecem a corrupção e a fraude.

## 3. DIRETRIZES

**[3]** A Gestão de Riscos, Controles Internos e Conformidade da PREVIDÊNCIA BRB deverá observar as seguintes diretrizes:

**1. [3]** Contribuir para a consecução da missão, visão e objetivos estratégicos;

**2. [3]** Salvaguardar os interesses, a reputação e a marca da PREVIDÊNCIA BRB;

**3. [3]** Gerar valor e proteger o ambiente interno;

**4. [3]** Promover a melhoria contínua dos processos organizacionais;

**5.** Subsidiar a tomada de decisões;

**6.** Garantir ambiente seguro para a tomada de decisão;

**7.** Tratar a incerteza;

**8.** Ser transparente, inclusiva e capaz de reagir a mudanças;

**9.** Considerar fatores humanos, culturais, valores éticos e de integridade;

**10.** Ter resiliência, capacidade de resposta eficaz e estar integrada às oportunidades e à inovação.

**11.** Promover a cultura ética dentro da Entidade;

**12.** Divulgar o canal de ética e demonstrar sua transparência e eficácia.

**4. CONCEITOS**

**Apetite ao Risco:** Nível de risco aceitável pela Entidade para atingir seus objetivos organizacionais.

**Auditoria:** Avaliações sobre a eficácia do gerenciamento de riscos e dos controles internos.

**Avaliação de Risco:** Processo de identificação e análise dos riscos relevantes para o alcance dos objetivos organizacionais e a determinação de resposta apropriada.

**Conformidade (*Compliance*):** Ato de verificar se condutas e práticas internas estão compatíveis com as regras, normativos e legislações.

**Integridade:** Característica da pessoa que é íntegra; qualidade de quem é honesto; que é incorruptível.

**Consequência do Risco:** Resultado de um evento que afeta positiva ou negativamente os objetivos da Entidade.

**Controles Internos:** Conjunto de regras, procedimentos, diretrizes, protocolos de atividades e de rotinas que versam sobre os sistemas informatizados ou não, conferências, trâmites de documentos e informações, operacionalizados de forma integrada destinados a enfrentar os riscos e fornecer segurança de que os objetivos organizacionais serão alcançados.

**Gerenciamento de Risco:** Processo que visa identificar, avaliar, administrar e controlar potenciais eventos ou situações de risco e fornecer segurança no alcance dos objetivos organizacionais.

**Gestão de Riscos:** Sistema institucionalizado e permanente, estruturado e monitorado pela administração e direcionado às atividades de identificar, analisar e avaliar riscos; decidir sobre estratégias de resposta e ações para tratamento de riscos corporativos; monitorar e comunicar sobre o processo de gerenciamento desses riscos, com vistas a apoiar a tomada de decisão, em todos os níveis, e ao efetivo alcance dos objetivos da empresa.

**Governança:** Combinação de processos e estruturas implantadas pela Entidade com objetivo de informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos institucionais e prestar contas dessas atividades para as partes interessadas.

**Identificação de Riscos:** Processo que busca a identificação, o reconhecimento e descrição dos riscos e envolve a identificação de suas fontes, causas e consequências.

**Incerteza:** Incapacidade de saber antecipadamente a probabilidade ou impacto de eventos futuros.

**[3] Matriz de Risco:** Ferramenta que permite aos gestores mensurar, avaliar e ordenar os eventos de riscos que podem afetar os objetivos dos processos vinculados à sua área de atuação e, consequentemente, os objetivos organizacionais, demonstrando a combinação da probabilidade *versus* impacto, que caracteriza o dimensionamento dos níveis de riscos e o tratamento em função do apetite a risco.

**Medida de controle:** Medida aplicada para tratar os riscos de forma a buscar que objetivos e as metas organizacionais sejam alcançados.

**Mitigação do Risco**: Atenuação dos impactos que um risco pode trazer para uma empresa. Isso ocorre quando não é possível eliminar totalmente um determinado tipo de risco, tornando a convivência com o risco de maneira mitigada, em uma ação de prudência para os gestores.

**Objetivo organizacional:** Situação que se deseja alcançar para ter êxito no cumprimento do propósito e no atingimento da visão de futuro da Entidade.

**Resposta ao Risco:** Qualquer ação adotada para lidar com risco. As respostas podem se enquadrar em um destes tipos de decisão:

a) aceitar o risco;

b) transferir/compartilhar o risco;

c) evitar o risco; ou

d) mitigar/reduzir o risco.

As ações adotadas visam diminuir a probabilidade de ocorrência ou minimizar as consequências do risco sobre os objetivos de Entidade.

**Risco:** Possibilidade de ocorrência de evento que tenha impacto na realização dos objetivos da Entidade.

**[3] Risco Inerente:** Risco a que Entidade está exposta, sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto. É o risco relacionado diretamente ao seu negócio.

**Risco Residual:** Risco remanescente depois de implementadas as medidas de controle para o tratamento do risco.

**Tolerância a Risco:** Nível aceitável de variação em relação à meta, para o cumprimento de um objetivo específico.

## 5. ABRANGÊNCIA

**[3]** Esta Política abrange todos os processos corporativos da PREVIDÊNCIA BRB, em consonância com as Melhores Práticas de Governança Corporativa, sendo aplicável às três linhas de defesa adotadas pela Entidade.

## 6. CATEGORIAS DOS RISCOS

A categorização de risco tem como objetivo direcionar a atribuição de responsabilidades, prover maior assertividade às ações de mitigação dos riscos e facilitar a identificação e/ou a definição de planos de ação integrados, considerando os principais riscos na gestão dos Planos de Benefícios e da Entidade.

**Riscos Atuariais:** Possibilidade de perdas decorrentes da não confirmação ou da pouca aderência das premissas adotadas nos cálculos de projeção dos compromissos dos Planos de Benefícios em relação aos participantes ativos e assistidos, tendo como base as regras regulamentares, risco de incapacidade de honrar o contrato previdenciário.

**Riscos de Contraparte:** Possibilidade de perda decorrente do não cumprimento de obrigação pela contraparte de uma operação ou contrato.

**Riscos de Crédito:** Possibilidade de perda associada à incerteza quanto ao cumprimento de obrigações por contraparte de contrato ou um emissor de título.

**Risco de Mercado:** Possibilidade de perda financeira decorrente da flutuação dos preços dos ativos financeiros em carteira, em função da volatilidade de mercado, causada por fatores adversos como por exemplo: alteração da conjuntura econômica.

**Risco de liquidez:** Possibilidade de perda por falta de capacidade de se desfazer imediatamente dos ativos mantidos em carteira, com perda de valor, devido às condições adversas de mercado para fazer frente às obrigações, em determinado horizonte de tempo.

**Riscos de Imagem:** Possibilidade de perda decorrente de quebra da confiança ou credibilidade de que a Entidade desfruta no seu ambiente de negócios. Essa adversidade resulta da interpretação de notícias veiculadas na imprensa, de atitudes e declarações dos representantes, bem como de eventos externos que possam afetar a reputação da Entidade.

**Riscos Legais e Judiciais:** Possibilidade de perdas decorrentes de penalidades ou decisões desfavoráveis em aspectos legais, judiciais e regulamentares que envolvam os contratos firmados e as obrigações previdenciárias, fiscais, trabalhistas e societárias da Entidade.

**Riscos Operacionais:** Possibilidade de perda decorrente da inadequação na especificação ou na condução de processos, pessoas e sistemas ou projetos, bem como de eventos externos que causem prejuízos às atividades ou danos aos ativos físicos.

**Risco Sistêmico:** Decorre da possibilidade de um choque a uma parte limitada do segmento se propagar por todo o sistema, levando a uma insolvência generalizada.

**Risco Socioambiental:** Possibilidade de perdas decorrentes de danos socioambientais decorrentes de danos à saúde humana, poluição, segurança, impactos em comunidades e ameaças à biodiversidade e podem provocar danos à reputação.

**Risco de terceirização:** Possibilidade de perdas decorrentes inadequação de contratos, relações trabalhistas, prestação de serviços e reputação de terceiros.

**Risco de Integridade:** Riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

## 7. PRINCÍPIOS

### 7.1. GESTÃO DE RISCOS

**[3]** A Gestão de Riscos visa a melhoria contínua nos processos organizacionais, promovendo segurança no cumprimento do propósito e no alcance dos objetivos organizacionais e deverá ser disseminada para todos os colaboradores da entidade.

**[3]** São objetivos da Gestão de Riscos:

**a)** Assegurar que os responsáveis pela tomada de decisão tenham acesso tempestivo a informações quanto aos riscos aos quais está exposta a Entidade;

**b)** Alocar e utilizar eficazmente os recursos da Entidade, inclusive para o tratamento de riscos corporativos;

**c)** Aumentar a probabilidade de alcance dos objetivos da Entidade, reduzindo os riscos a níveis aceitáveis; e

**d)** Agregar valor à Entidade, por meio da melhoria dos processos corporativos, de tomada de decisão e do adequado tratamento dos riscos corporativos e dos impactos negativos decorrentes da sua materialização.

Serão adotadas metodologias e ferramentas para a identificação, avaliação, monitoramento e controle dos riscos na entidade por meio de sistema de gestão baseada em riscos, com periodicidade definida e resultado tratado, por meio de ações de correção e ou de melhoria para o adequado tratamento dos riscos e de acordo com o grau de apetite a riscos, cuja operacionalização observará os componentes:

**Criação do ambiente interno:** O ambiente interno é a base e deve prover disciplina e presteza na gestão dos riscos. Cabe à administração preparar o ambiente interno da Entidade para propiciar o gerenciamento de riscos de forma célere e eficaz. A etapa de preparação consiste em um conjunto de convicções e atitudes que caracterizam a forma como a Entidade considera o risco no dia a dia, incluindo, entre outros elementos, integridade, valores éticos e competência das pessoas, papéis e responsabilidade, delegação de atribuições e de autoridade, a estrutura de governança organizacional e políticas e práticas adotadas.

**[3] Definição de objetivos:** Todas as unidades da Entidade devem ter objetivos fixados e publicizados. Esses objetivos devem estar alinhados ao propósito e à missão da Entidade e ser explicitados para permitir a identificação de eventos que potencialmente impeçam sua consecução e a extrapolação dos níveis de apetite a riscos.

**[3] Identificação de eventos de riscos:** Etapa em que são identificados e relacionados os riscos inerentes à própria atividade da Entidade, em seus diversos níveis. Fase em que devem ser definidos eventos, fontes, impactos e responsáveis por cada risco.

**Avaliação de riscos:** Etapa em que se avaliam os eventos sob a perspectiva de probabilidade e impacto de ocorrência. A avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas. Os riscos devem ser avaliados quanto à sua condição de inerentes e residuais.

**[3] Resposta a riscos:** Etapa em que se identifica qual estratégia (resposta) seguir (evitar, reduzir, compartilhar ou aceitar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de apetite a riscos, em confronto com a avaliação que se fez do risco.

**Priorização de riscos:** Consiste em comparar e classificar os riscos quanto aos seus respectivos níveis de probabilidade e impacto, identificando aqueles que necessitam de maior atenção e, em seguida, priorizar o tratamento daqueles considerados mais graves.

**Estabelecimento de atividades de controles internos:** Etapa em que serão avaliadas as políticas, os manuais e os procedimentos para mitigar os riscos que a Entidade tenha optado por tratar. Essas atividades são denominadas de procedimentos de controle e devem estar distribuídas por toda a Entidade, incluindo os controles internos preventivos e detectivos, e devem prever a preparação de planos de ação ou contingência e respostas à materialização dos riscos.

**[3] Comunicação:** Informações relevantes devem ser comunicadas, com a tempestividade necessária ao cumprimento das responsabilidades e devem inserir informações completas tais como: dados internos, informações sobre eventos, atividades e condições externas, para possibilitem o melhor gerenciamento de riscos e a tomada de decisão. A comunicação deve ser para toda a Entidade, por meio de canais que permitam acessibilidade e fluidez a todos os colaboradores.

**Monitoramento:** Tem o objetivo de avaliar a qualidade da gestão de riscos e dos controles internos, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com as mudanças nas condições que alterem o nível de exposição a riscos.

Serão estabelecidos nas Políticas de Investimentos os limites de riscos aceitáveis considerando as características de cada Plano de Benefícios e o nível de apetite aos riscos que a Entidade está disposta a aceitar para atingir suas metas e objetivos.

**[3]** Serão estabelecidas regras para a prevenção dos crimes financeiros e tratamento das pessoas consideradas como politicamente expostas no âmbito da Entidade, em conformidade com a legislação de regência e melhores práticas de gestão.

### 7.2. GESTÃO DE CONTROLES INTERNOS

Os Controles Internos devem ser estruturados para oferecer segurança de alcance dos objetivos da Entidade e devem ter objetivos claros e congregar todas as atividades materiais e formais implementadas pela gestão para assegurar que as respostas aos riscos sejam executadas com eficácia, possibilitando à Entidade o alcance dos objetivos estabelecidos.

Os Controles Internos devem observar os seguintes objetivos:

**1.** Dar suporte ao propósito, à continuidade e à sustentabilidade institucional, proporcionando garantia de atingimento dos objetivos estratégicos da Entidade;

**2.** Proporcionar eficiência, eficácia e efetividade operacional, mediante execução ordenada, ética e econômica das operações;

**3.** Assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisão, ao cumprimento de obrigações de transparência e à prestação de contas;

**4.** Assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos, procedimentos e diretrizes internas da Entidade; e

**5.** Estabelecer procedimentos de controles internos proporcionais aos riscos, observada a relação custo-benefício.

A gestão dos controles internos deverá propiciar a integração dos controles às rotinas, políticas, sistemas, recursos e deverá estar prevista em todos os processos corporativos, devendo, ainda, avaliar o impacto dos riscos inerentes a todos os processos e adotar controles compatíveis com vistas a mitigar seus efeitos, de forma a propiciar o cumprimento dos seus objetivos institucionais.

A operacionalização dos Controles Internos deverá observar os seguintes componentes:

**Ambiente de controle:** Compreende a base dos controles internos da gestão da Entidade que é formado pelas regras e estruturas que determinam a qualidade dos controles internos. Esse ambiente influenciará a forma pela qual se estabelecem as estratégias e os objetivos bem como, na maneira como os procedimentos de controle interno são estruturados.

**Avaliação de risco:** Processo permanente de identificação e análise de riscos que impactam o alcance dos objetivos da Entidade. Os riscos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência, por meio de análises qualitativas, quantitativas ou da combinação de ambas.

**Atividades de controle interno:** São atividades materiais e formais, como políticas, procedimentos, técnicas e ferramentas, implementadas pela gestão para diminuir os riscos e assegurar o alcance de objetivos organizacionais. Essas atividades podem ser preventivas (reduzem a ocorrência de eventos de risco) ou detectivas (possibilitam a identificação da ocorrência dos eventos de riscos), implementadas de forma manual ou automatizada. As atividades de controles internos devem ser apropriadas, funcionar consistentemente de acordo com um plano de longo prazo, ter custo adequado, ser abrangente, razoáveis e diretamente relacionadas aos objetivos de controle.

**[3] Comunicação:** As informações produzidas pela Entidade devem ser apropriadas, tempestivas, atuais, precisas e acessíveis, devendo ser comunicadas e armazenadas de forma que permitam que os empregados cumpram suas responsabilidades, inclusive a de execução dos procedimentos de controle interno. A Entidade deve comunicar, para todas as partes interessadas, as informações necessárias ao alcance dos objetivos traçados.

**Monitoramento:** Obtido por meio de avaliações específicas ou de monitoramento contínuo, independente ou não, realizados sobre todos os demais componentes de controles internos, com o fim de aferir sua eficácia, eficiência, efetividade, economicidade excelência ou execução na implementação dos seus componentes e corrigir tempestivamente as deficiências dos controles internos.

Os controles internos estabelecidos nas Políticas de Investimentos dos Planos serão incorporados aos demais normativos e executados pelas áreas responsáveis pelo gerenciamento.

**[3]** Os controles internos estabelecidos para a prevenção dos crimes financeiros e tratamento das pessoas impedidas e daquelas classificadas como politicamente expostas serão descritas em normativos internos e executadas em todas as unidades organizacionais da PREVIDÊNCIA BRB.

**[3]** A área de gestão de riscos, controle internos e conformidade, no que se refere ao monitoramento dos riscos e dos controles mitigadores, deverá primar pelo adequado gerenciamento dos riscos e controles dos processos executados pelas unidades, como uma segunda linha de defesa.

**[3]** Os gestores dos processos serão os responsáveis pela avaliação dos riscos no âmbito das unidades, dos processos e das atividades que lhes são afetos, portanto, todos os colaboradores devem adotar as boas práticas e cumprir regularmente a legislação de regência, as políticas, normas, manuais e procedimentos operacionais.

**[3]** Os colaboradores deverão adotar medidas de correção e de melhoria contínua, com vistas a adequar o nível dos controles, considerando os processos de relevantes da Entidade, que possam impactar a gestão dos Planos administrados.

### 7.3. GESTÃO DE CONFORMIDADE E INTEGRIDADE

Considerando que os riscos de integridade podem ter causa, evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem, é importante esclarecer que, a ocorrência de fraudes e atos de corrupção na gestão de riscos de integridade não devem ser entendidos apenas por infração de leis e normas, mas englobar outros aspectos, tais como: recebimento e oferta de propinas, desvio de verbas, fraudes, abuso de poder/influência, nepotismo, conflito de interesses, uso indevido de informações sigilosas e práticas antiéticas.

**[3]** A gestão dos processos de conformidade e integridade serão feitas pelo *Compliance Officer* através do Sistema de Gestão de Integridade e *Compliance* e das ações do Plano de Integridade da PREVIDÊNCIA BRB, em conformidade com as diretrizes do Programa de Integridade e *Compliance*.

**[3]** A área responsável pelo gerenciamento de riscos e *compliance* deverá prever as circunstâncias que podem ocasionar danos à Entidade e trabalhar na minimização de seus efeitos, entretanto, sempre existirá um grau de incerteza a ser administrado pelas equipes técnicas que atuam nesses processos.

## 8. SISTEMA DE GESTÃO DE RISCOS, CONTROLES INTERNOS E CONFORMIDADE

**[3]** A gestão de riscos, controles internos e conformidade é feita em três linhas de defesa para melhor estruturar a gestão dos processos corporativos e assegurar o cumprimento das diretrizes traçadas nesta Política. Atua na adoção de metodologia que visa identificar, avaliar, tratar e monitorar os riscos, estabelecendo uma estrutura de segurança nos processos, com vistas a assegurar que os objetivos da PREVIDÊNCIA BRB sejam alcançados e mitigar o risco de sanções legais ou regulatórias, de perdas financeiras ou de danos reputacionais, em virtude de falha no cumprimento da legislação de regência e normativos internos e externos, padrões técnicos, código de conduta e ética, dentre outros.

**[3] Primeira linha de defesa** – Representada pelas unidades de trabalho da PREVIDÊNCIA BRB, sendo seus colaboradores responsáveis diretos pela gestão dos riscos e atendimento às normas relacionadas às suas atividades, bem como pela execução dos controles e pela implementação de medidas preventivas e corretivas para o devido tratamento dos riscos.

**[3] Segunda linha de defesa** – Representada pelas áreas responsáveis pela gestão de riscos, controles e de conformidade, que tem independência no exercício de suas funções. Possui comunicação com os membros da Diretoria Executiva, Conselho Deliberativo e Conselho Fiscal, com os gestores e demais colaboradores da PREVIDÊNCIA BRB. Também tem acesso a quaisquer informações necessárias para a realização de suas atividades.

**[3] Terceira linha de defesa** – Representada pelo Comitê de Gestão de Riscos, pela Auditoria Interna, pelo Conselho Fiscal e pelas auditorias externas e das Patrocinadoras, permitindo à Diretoria Executiva aferir a adequação dos controles e efetividade do gerenciamento dos riscos, a confiabilidade das demonstrações contábeis e o cumprimento da legislação, normas e regulamentações.

## 9. RESPONSABILIDADES

**[3]** O Sistema de Gestão de Riscos, Controles Internos e Conformidade consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos corporativos em toda a Entidade.

São instâncias responsáveis pelo Sistema de Gestão de Riscos, Controles Internos e Conformidade no âmbito da PREVIDÊNCIA BRB:

**-** Conselho Deliberativo;

**-** Conselho Fiscal;

**-** Diretoria Executiva;

- **[3]** Área de Riscos, Controles e Conformidade;

**-** Gestores de processos;

- Colaboradores.

**[3]** O Comitê de Gestão de Riscos é órgão de assessoramento, responsável pelo Sistema de Gestão de Riscos, Controles Internos e Conformidade.

**[3]** A Auditoria Interna é responsável pelo assessoramento do Conselho Deliberativo quanto às atividades de auditoria, na forma definida e aprovada no Plano Anual de Auditoria Interna.

## 10. COMPETÊNCIAS

A gestão de riscos, controles internos e conformidade abrange todas as áreas da Entidade, cuja priorização se dará nos processos finalísticos e nos processos corporativos que possam impactar o atingimento dos objetivos estratégicos da Entidade.

### 10.1. CONSELHO DELIBERATIVO

Como órgão de direcionamento estratégico, sem prejuízo de outras competências previstas no Estatuto da Social:

I – Aprovar a Política de Gestão de Riscos, Controles Internos e Conformidade da Entidade;

II – Aprovar os níveis de apetite a riscos no processo de Gestão de Investimento, conforme disposto na Política de Investimentos de cada Plano e nos processos corporativos;

III – Acompanhar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas e as ações de conformidade;

IV – Acompanhar a gestão integrada de Governança, Riscos e *Compliance*;

V – Assegurar que os objetivos do Sistema de Gestão de Integridade e *Compliance* estão sendo atingidos, inclusive nas ações de divulgação e de incentivo do canal de ética;

VI – Acompanhar as ações do Sistema de Gestão de Integridade e *Compliance* estabelecidas nas reuniões de Análise Crítica da Alta Direção - ACAD. .

VII – Deliberar sobre a aplicação da penalidade proposta pelo Comitê de Ética e Disciplina em relação aos processos de investigação advindos dos relatos recebidos no Canal de Ética.

**10.2. CONSELHO FISCAL**

**[3]** Compete ao Conselho Fiscal da Entidade, como órgão de fiscalização da gestão, sem prejuízo de outras competências previstas no Estatuto da Entidade:

I – Supervisionar o processo de Gestão de Riscos, Controles Internos e Conformidade da Entidade;

II – Aferir a efetividade do gerenciamento de riscos e a adequação dos controles internos;

III – Analisar e produzir o relatório de Controles internos, conforme legislação pertinente;

IV – Reportar ao Conselho Deliberativo eventuais deficiências identificadas na gestão de riscos, controles internos e conformidade;

V – **[3]** Examinar e apresentar parecer acerca das demonstrações contábeis;

VI – Monitorar o nível de exposição aos riscos, a eficácia dos controles internos e ações de conformidade adotadas pela Diretoria Executiva.

VII – **[3]** Acompanhar as ações do Sistema de Gestão de Integridade e *Compliance* estabelecidas nas reuniões de Análise Crítica da Alta Direção - ACAD, incluindo aquelas voltadas ao incentivo da utilização do Canal de Ética para melhoria do processo de *compliance* (Integridade, ética e conformidade) da Entidade.

**10.3. DIRETORIA EXECUTIVA**

**[3]** Como órgão responsável pela Gestão da Entidade execução das Diretrizes aprovadas, sem prejuízo de outras competências previstas no Estatuto da Entidade:

I – Aprovar manuais, normas e diretrizes referentes à metodologia de gerenciamento de riscos, controles internos e conformidade;

II – Definir os níveis de apetite a riscos aceitos no âmbito da Entidade;

III – Monitorar os riscos estratégicos e respectivas medidas de mitigação;

IV – Monitorar a evolução dos níveis de riscos, a efetividade das medidas de controle implementadas e ações de conformidade;

V – Promover a cultura organizacional voltada para gestão de riscos, controle internos e conformidade de forma a ter atuação tempestiva na identificação e tratamento dos riscos, o constante aprimoramento dos controles e o estabelecimento de cultura da ética e de integridade na Entidade;

VI – Definir e acompanhar o processo de gestão de riscos, controles internos e conformidade, e disponibilizar os recursos necessários para implementação e aprimoramento constante dos programas de melhoria contínua e desenvolvimento e treinamento de pessoas;

VII – Assegurar a conformidade à legislação de regência, os normativos internos e externos, políticas, códigos e manuais;

VIII – Assegurar a atuação íntegra e respeitada da entidade, de seus colaboradores e terceiros;

IX – Aprovar o plano de capacitação e de educação continuada para os integrantes do sistema de gestão de riscos, controles internos e conformidade.

X – **[3]** Aprovar e apoiar o Programa de Integridade e *Compliance* da PREVIDÊNCIA BRB, e assegurar que os objetivos do Sistema de Gestão de Integridade e *Compliance* estão sendo atingidos.

XI – **[3]** Acompanhar trimestralmente o Plano de Integridade da Entidade.

XII **– [3]** Realizar a análise crítica do Sistema de Gestão de Integridade e *Compliance* da Entidade e acompanhar as ações estabelecidas

XIII – **[3]** Incentivar a utilização do Canal de Ética para melhoria do processo de *compliance* (Integridade, ética e conformidade) da Entidade.

### 10.4. ADMINISTRADOR RESPONSÁVEL PELA GESTÃO DE RISCOS [ARGR]

Compete ao Administrador Responsável pela Gestão de Riscos, sem prejuízo de outras competências:

**I.** Participação ativa nos processos de análise de investimentos, cabendo-lhe a responsabilidade pela avaliação prévia dos riscos das operações, possibilitando a emissão de pareceres com posicionamento técnico, bem como a plena manifestação nas instâncias decisórias;

**II.** Responsabilidade pela identificação, análise, avaliação, controle, monitoramento e comunicação à alta administração dos níveis de exposição aos riscos das carteiras de investimentos, bem como todos aqueles que possam afetar os resultados dos Planos de Benefícios, propondo ações mitigadoras, sempre que necessário;

**III**. **[3]** Manutenção permanente e tempestiva do fluxo de informações com as diversas instâncias da Entidade;

**IV.** Desenvolvimento de capacitação técnica e cultura de controle que estimule a disseminação dos princípios de gestão de riscos a todos os gestores internos e demais empregados.

O Administrador Responsável pela Gestão do Risco deve exercer suas funções com independência e sem qualquer subordinação hierárquica entre si, sopesadas questões do porte e da estrutura organizacional da EFPC.

### 10.5. COMITÊ DE GESTÃO DE RISCOS – CORIS

Compete ao CORIS, sem prejuízo de outras competências previstas no seu Regimento:

I – **[3]** Fornecer à Diretoria Executiva e aos Conselhos da Entidade avaliações abrangentes e independentes, conforme aprovado no Plano Anual de trabalho de avaliações de processos corporativos aprovado no âmbito da Entidade;

II – Avaliar as metas propostas para implementação de metodologias de Gestão de Riscos e avaliação/estabelecimento dos Controles Internos;

III – Avaliar se há mudanças nos níveis de apetite a risco da Entidade;

IV – Apoiar a implementação da Política de Gestão de Riscos, Controles Internos e de Conformidade na Entidade;

V – Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;

VI – Supervisionar a atuação dos gestores na Gestão de Riscos, Controles Internos e Conformidade.

### 10.6. [3] AUDITORIA INTERNA

**[3]** A Auditoria Interna é subordinada ao Conselho Deliberativo, competindo:

I – **[3]** Confeccionar o Plano Anual de Auditoria Interna e submetê-lo à aprovação do Conselho Deliberativo.

II – **[3]** Avaliar processos relevantes, sistema de informações, dos controles internos e do gerenciamento de riscos, tendo por base o Plano Anual de Auditoria Interna aprovado pelo Conselho Deliberativo.

III – **[3]** Avaliar a efetividade, a confiabilidade e a integridade dos processos e sistema de informações gerenciais dos processos auditados;

IV – **[3]** Acompanhar e assegurar o atendimento às solicitações das auditorias externas e internas, quando terceirizadas, e das auditorias das Patrocinadoras;

V – **[3]** Recomendar aprimoramentos de políticas, práticas e procedimentos.

VI – **[3]** Reunir-se com os Conselhos Deliberativo e Fiscal para tratar de situações e ou demandas especiais, que evidenciem riscos à integridade e imagem da Entidade.

VII – **[3]** Emitir relatório circunstanciado das auditorias realizadas, com as devidas recomendações de melhoria ou de correção de rotinas.

**10.7. [3] ÁREA DE CONTROLE, RISCO E CONFORMIDADE:**

**[3]** Compete à área de gestão de controle, risco e conformidade, sem prejuízo de outras competências atinentes à área:

I – Propor Política de Gestão de Riscos, Controles Internos para a Entidade, que deverá ser periodicamente revisada e aprovada em última instância pelo Conselho Deliberativo;

II – Propor metodologia de gerenciamento de riscos e controles internos, nos termos dos normativos internos da área;

III – Coordenar os processos de identificação, avaliação e respostas aos riscos a que está sujeita a Entidade, monitorando a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;

IV – Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;

V – Dar suporte aos gestores dos processos na identificação, avaliação, seleção de respostas e monitoramento dos riscos corporativos, bem como na avaliação/estabelecimento dos controles internos;

VI – Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva e Conselho Fiscal e com o acompanhamento do Conselho Deliberativo;

VII – Propor e promover a capacitação continuada em Gestão de Riscos, Controles Internos e Conformidade para os colaboradores da Entidade, fomentando, quando possível, a formação de multiplicadores;

VIII – **[3]** Aplicar os testes de verificação de riscos, controles internos e conformidade;

IX – Verificar a aderência da estrutura dos processos, produtos e serviços às leis, normativos, políticas e diretrizes internas e demais regulamentos aplicáveis;

X – Monitorar os riscos residuais e o tratamento das ações de melhoria e dos Registros de Não Conformidade com vistas à mitigação dos riscos e aprimoramento dos controles internos;

XI – Revisar e avaliar a eficácia da gestão de riscos e controles internos periodicamente;

XII – Agir preventivamente na mitigação dos riscos de maior relevância;

XIII – **[3]** Apoiar todas as unidades da Entidade na adoção de medidas de prevenção e controles dos riscos;

XIV – Promover a “internalização” de norma externa;

XV – Assegurar que todos atuem em conformidade com as normas estabelecidas pela Entidade;

XVI – Promover a fiscalização de atualização periódica dos normativos;

XVII – **[3]** Promover, integrar e controlar as atividades de *compliance*, em atuação conjunta com a área jurídica, sempre que necessário;

XVIII – **[3]** Zelar pelo Programa de Integridade de *Compliance* e se responsabilizar pelas ações propostas no Plano de Integridade da PREVIDÊNCIA BRB, inclusive propondo ajuste ou atualização;

XIX – Propor a atualização de normas e do Código de Conduta Ética;

XX – Conscientizar os integrantes da Entidade quanto aos padrões de conduta ética e de integridade, aos princípios socioambientais e ao combate à corrupção e terrorismo;

XXI –Identificar erros e propor aperfeiçoamento nas políticas e demais normas que tratam da conformidade;

XXII – **[3]** Disseminar a cultura de conformidade em todas as unidades organizacionais da Entidade;

XXIII – **[3]** Solicitar apoio da área jurídica com relação à interpretação de novas normas legais publicadas e a verificação de conformidades das normas, sempre que necessário;

XXIV – Incentivar o uso do Canal de Ética;

XXV – Fazer a gestão do Canal de Ética e orientar o Comitê de Ética e Disciplina no processo investigatório.

### 10.8. GESTORES DOS PROCESSOS

**[3]** Compete aos gestores dos processos, como responsáveis por implementar a gestão de riscos, controles internos e conformidade no âmbito dos processos corporativos sob sua responsabilidade:

I – Identificar, analisar e avaliar os riscos corporativos dos processos sob sua responsabilidade;

II – Propor respostas e respectivas medidas de controles internos a serem implementadas nos processos organizacionais sob sua responsabilidade, visando o tratamento dos riscos;

III – Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;

IV – **[3]** Manter os processos corporativos mapeados e com fluxogramas atualizados;

V – Implantar pontos de controles a fim de reduzir a probabilidade de que os riscos se materializem e de amenizar os seus efeitos, caso ocorram;

VI – Participar efetivamente das avaliações periódicas de riscos e controles feitas na Entidade, estabelecendo ações de melhoria e ou corretivas sempre que necessário;

VII – Assegurar que a legislação está sendo devidamente acompanhada e aplicada com regularidade nos processos organizacionais;

VIII – Disseminar a cultura de gestão de riscos, controles internos e conformidade em sua área de atuação;

XIX – Monitorar os mecanismos de controles internos, prevenindo posturas inadequadas e evitando desvios de qualquer natureza;

X – Estabelecer planos de contingência para os principais processos operacionais sob sua responsabilidade.

Compete a todos os colaboradores da Entidade, o monitoramento da evolução dos níveis de riscos corporativos, a efetividade das medidas de controles internos implantadas nos processos corporativos em que estiverem envolvidos ou que tiverem conhecimento e atuar em conformidade com a regras e conduta esperada de ética e integridade. E, ainda, caso sejam identificadas mudanças ou fragilidades nos processos corporativos, o empregado deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos corporativos do processo em questão.

## 11. TRATAMENTO DOS RISCOS

Os gestores devem adotar medidas mitigadoras de forma efetiva e tempestiva quando da identificação de riscos e de fragilidade nos controles internos empregados nos processos corporativos sob sua responsabilidade.

A área responsável pelo gerenciamento de riscos deverá recomendar medida corretiva, estabelecendo prazo para execução, em conjunto com o gestor, sempre que identificar extrapolação dos limites prudenciais, desenquadramento e desconformidade na operacionalização dos processos corporativos, a partir de todas as medidas de acompanhamento e verificação previstas nos normativos internos.

Na mesma linha de atuação, as demais estruturas de governança (Conselhos, Diretoria, Comitês) deverão manter vigilância quanto ao tratamento dos riscos inerentes à gestão da Entidade e dos Planos de Benefícios, registrando sempre que necessário recomendações a serem implementadas com vistas à mitigação dos riscos, fortalecimentos dos controles internos e da conformidade em todos os processos corporativos.

## 12. DISPOSIÇÕES GERAIS

**[3]** A implementação das diretrizes traçadas nesta Política será efetivada mediante a elaboração e atualização dos normativos internos de abrangência e da execução segura das rotinas operacionais, com observância da legislação de regência e das melhores práticas de gestão.

Os casos omissos e as dúvidas surgidas na aplicação desta Política serão avaliados pelo Comitê de Gestão de Riscos e decididos pelo Conselho Fiscal da Entidade.

**[3]** A presente Política deverá ser atualizada sempre que necessário, de modo a assegurar o efetivo gerenciamento de riscos, o fortalecimento do sistema de controles internos e o cumprimento das obrigações de conformidade, sendo que a revisão terá como limite 2 anos e entrará em vigor, a partir de sua aprovação pelo Conselho Deliberativo da Entidade.

**[3]** Os Conselheiros, Dirigentes e Colaboradores deverão assinar Termo de aceite e ateste de conhecimento da referida Política, observada a necessidade de divulgação das atualizações de forma regular para todos os colaboradores.