



# **POLÍTICA DE GESTÃO DE RISCOS**

**APROVADO PELO CONSELHO DELIBERATIVO  
EM 27/09/2017.**



## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>3</b>
<b>2</b>	<b>OBJETIVO .....</b>	<b>3</b>
<b>3</b>	<b>PRINCÍPIOS.....</b>	<b>3</b>
<b>4</b>	<b>DIRETRIZES.....</b>	<b>4</b>
<b>5</b>	<b>PARÂMETROS NECESSÁRIOS PARA A GESTÃO DE RISCOS .....</b>	<b>4</b>
<b>6</b>	<b>METODOLOGIAS ADOTADAS.....</b>	<b>5</b>
<b>6.1</b>	<b>COMPONENTES DO GERENCIAMENTO DE RISCOS .....</b>	<b>6</b>
<b>6.1.1</b>	<b>AMBIENTE INTERNO .....</b>	<b>6</b>
<b>6.1.2</b>	<b>DEFINIÇÃO DOS OBJETIVOS .....</b>	<b>6</b>
<b>6.1.3</b>	<b>IDENTIFICAÇÃO DE RISCOS .....</b>	<b>6</b>
<b>6.1.4</b>	<b>AValiação DE RISCOS.....</b>	<b>7</b>
<b>6.1.5</b>	<b>RESPOSTA A RISCOS.....</b>	<b>7</b>
<b>6.1.6</b>	<b>ATIVIDADES DE CONTROLE.....</b>	<b>8</b>
<b>6.1.7</b>	<b>INFORMAÇÃO E COMUNICAÇÃO .....</b>	<b>8</b>
<b>6.1.8</b>	<b>MONITORAMENTO .....</b>	<b>8</b>
<b>7</b>	<b>RESPONSABILIDADES DA GESTÃO DE RISCOS.....</b>	<b>9</b>
<b>7.1.1</b>	<b>CONSELHO DELIBERATIVO .....</b>	<b>9</b>
<b>7.1.2</b>	<b>CONSELHO FISCAL .....</b>	<b>9</b>
<b>7.1.3</b>	<b>DIRETORIA EXECUTIVA.....</b>	<b>9</b>
<b>7.1.4</b>	<b>COMITÊ DE GESTÃO DE RISCOS.....</b>	<b>10</b>
<b>7.1.5</b>	<b>ÁREA DE GESTÃO DE RISCOS E SUPERVISÃO ATUARIAL .....</b>	<b>10</b>
<b>7.1.6</b>	<b>ÁREAS GESTORAS.....</b>	<b>11</b>
<b>8</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>11</b>



## **1 INTRODUÇÃO**

A gestão de uma Entidade Fechada de Previdência Complementar - EFPC, reveste-se de grande relevância, devendo seguir princípios, regras e práticas de gestão, governança e controles internos, de modo a assegurar o cumprimento de seus objetivos.

A adoção da Supervisão Baseada em Risco (SBR), no âmbito da Superintendência Nacional de Previdência Complementar – Previc, disposta na Recomendação CGPC N° 02/2009, visa supervisionar de forma direta e indireta o regime de previdência complementar operado pelas EFPC, quanto a sua exposição a riscos.

Para a Previc, a Gestão Integrada de Riscos deve estar alicerçada na identificação, monitoramento e controle dos fatores de risco que impactam os objetivos da EFPC, em conformidade com as boas práticas de governança corporativa.

De acordo com o Guia Previc de Melhores Práticas de Governança para EFPC, as Entidades devem constantemente monitorar os ambientes regulatório, econômico, financeiro e social, e, ao identificar eventuais tendências de desvio, corrigir imediatamente a trajetória, utilizando, dentre outras, a seguinte medida:

*“Formulação da política de gestão de riscos, alinhada à política de investimentos, definição de procedimentos internos, monitoramento e controles, registrados em códigos, regimentos e manuais”.*

A gestão integrada de riscos corporativos está diretamente relacionada ao crescimento sustentável e a criação de valor, dado que este processo permite a identificação não só de ameaças, como também de oportunidades de negócio, além da tomada de decisões baseada em riscos.

Nesse contexto, a política de gestão de riscos figura como o instrumento que define as intenções e diretrizes gerais, da Entidade, relacionadas à gestão de riscos.

## **2 OBJETIVO**

Esta política tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos, bem como orientar a identificação, avaliação, tratamento, monitoramento e comunicação de risco estratégico, atuarial, de crédito, de mercado, de liquidez, legal, de imagem, de terceirização e operacional, incorporando a visão de riscos à tomada de decisões estratégicas e em linha com as melhores práticas de governança.

## **3 PRINCÍPIOS**

O Cibrius – Instituto Conab de Seguridade Social - reconhece que a gestão de riscos é parte integrante de todos os seus processos organizacionais.



O Instituto tem como meta principal, atingir a estratégia definida e, para isto, é preciso acompanhar suas operações, garantir a veracidade e apresentação transparente das informações para os participantes, assistidos e patrocinadores, bem como zelar pelo desempenho da conformidade ou atendimento aos normativos internos e externos, comprovando a aderência das atividades e o entendimento das legislações ou normas internas.

Em atenção ao estabelecido no seu Código de Ética, os dirigentes, conselheiros, empregados e prestadores de serviços, no exercício de suas funções, deverão pautar-se pelos padrões da ética, sobretudo no que diz respeito à integridade, à moralidade, à clareza de posições, de modo a prevenir eventuais conflitos de interesses.

#### **4 DIRETRIZES**

Esta política está estruturada, considerando os parâmetros necessários para gestão de riscos, as metodologias adotadas, bem como as responsabilidades para a gestão de riscos.

Os parâmetros são os itens que devem ser elaborados e formalizados pelo Cibrius, para que seja possível disseminar a gestão de riscos de forma padronizada, fazendo parte de todos os processos e áreas do Instituto.

As metodologias definem de que forma será estruturado o processo de gestão de riscos e, como será o processo de identificação, mensuração, avaliação e monitoramento de riscos e controles.

As responsabilidades servem para definir as atribuições a respeito da política e do processo de gestão de riscos, no Cibrius.

#### **5 PARÂMETROS NECESSÁRIOS PARA A GESTÃO DE RISCOS**

O processo de gestão de riscos objetiva identificar, em todo o Instituto, potenciais eventos que são capazes de afetá-lo, possibilitando o conhecimento pela Administração, de modo a mantê-los compatíveis com o apetite de risco desejado.

Este processo habilita os colaboradores, em todos os níveis, a entender melhor os riscos aos quais seus processos estão expostos e gerenciá-los.

Para os fins desta Política, fica estabelecido que no Cibrius, será tratado como risco, a possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos.

Dessa forma, somente os aspectos negativos que podem impedir ou dificultar o alcance dos objetivos receberão atenção e tratamento.

Uma vez que muitos termos utilizados na gestão de riscos não estão totalmente incorporados ao dia-a-dia do Instituto e, que a padronização de termos pode facilitar a comunicação entre as pessoas participantes do processo, o Cibrius adotará um Dicionário de Riscos como base de dados para a definição, os critérios de mensuração (impacto e frequência), os tipos e as categorias de riscos, considerando os diversos produtos e serviços, processos, atividades e natureza dos riscos inerentes à sua atuação, como administradora de planos de benefícios previdenciários.



## 6 METODOLOGIAS ADOTADAS

Para realizar a gestão de riscos e controles internos na Entidade, serão adotadas as seguintes metodologias norteadoras:

- COSO ERM – Committee of Sponsoring Organizations of the Treadway Commission, Gerenciamento de Riscos Corporativos – Estrutura Integrada;
- RSA – Risk Self Assessment, Autoavaliação dos Riscos;
- CSA – Control Self Assessment, Autoavaliação de Controles.

O modelo COSO ERM, considerado como norma de referência internacional e, em linha com as normas AS/NZS 4360<sup>1</sup> e ABNT NBR ISO 31000:2009<sup>2</sup>, é uma técnica que enumera as finalidades de um gerenciamento de riscos corporativos em alinhar o apetite de risco com a estratégia adotada, fortalecer as decisões em resposta aos riscos, além de identificar e administrar riscos múltiplos.

Esse modelo apresenta uma matriz tridimensional como modelo para gerenciamento de riscos integrado, em categorias de objetivos, componentes do gerenciamento de riscos e as unidades de negócios abrangidas pelo processo de gestão de riscos.

O RSA - Autoavaliação de Riscos e Controles é uma metodologia utilizada para identificar os riscos inerentes às atividades e seus respectivos impactos e frequência de forma original, desconsiderando os controles existentes.

A autoavaliação de controles ou modelo CSA é uma metodologia utilizada para avaliar a adequação dos processos de gerenciamento de risco e controle, bem como da efetividade dos controles internos estabelecidos para minimizar os riscos do negócio.

---

<sup>1</sup> A norma AS/NZS 4360, de 2003, é um padrão de risco australiano-neozelandês desenvolvido pela *New Zealand Institute of Chartered Accountants Standards*, fonte teórica dos trabalhos do *Controller and Auditor-General Office* (OAG – Entidade de Fiscalização Superior da Nova Zelândia) considerado uma importante publicação que oferece orientações detalhadas sobre as práticas de gerenciamento de riscos.

<sup>2</sup> A norma ABNT NBR ISO 31000:2009 (Princípios e Diretrizes para o Gerenciamento de Riscos), elaborada com base na AS/NZS 4360, visa harmonizar padrões, regulamentações e *frameworks* publicados anteriormente sobre gerenciamento de riscos.



## **6.1 COMPONENTES DO GERENCIAMENTO DE RISCOS**

O processo de gestão de riscos, do Cibrius, será estruturado observando os componentes definidos no modelo COSO ERM, constituído por oito “frentes de atuação” integrados e inter-relacionados, quais sejam: ambiente interno; definição dos objetivos; identificação de riscos; avaliação de riscos; resposta a riscos; atividades de controle; informação e comunicação; monitoramento.

A seguir, estão descritos, cada um dos oito componentes.

### **6.1.1 AMBIENTE INTERNO**

O ambiente interno é a base da estrutura de controles internos, influenciando a consciência de controle nas pessoas. Possui relação imediata com a cultura organizacional, o grau de desenvolvimento institucional, as decisões e atitudes da administração, a cultura de riscos da organização e a forma como eles são encarados e gerenciados, influenciando a consciência de controle das pessoas.

Ele direciona a organização, orientando e disciplinando os demais componentes do gerenciamento de riscos.

Os elementos que compõem o ambiente interno são a integridade pessoal e profissional e os valores éticos da direção e do quadro de pessoal, o comprometimento com a competência, o perfil e estilo gerencial, a estrutura organizacional da Entidade, a atribuição de autoridade e responsabilidade e as políticas e práticas de recursos humanos.

### **6.1.2 DEFINIÇÃO DOS OBJETIVOS**

Os objetivos estratégicos são definidos pelo Conselho Deliberativo em linha com a missão, com a visão e com o apetite ao risco, o qual direciona o nível de tolerância ao risco nos processos e atividades executadas nos diversos níveis do Cibrius.

Em função desses objetivos, são definidos conjuntos de estratégias para o seu cumprimento.

### **6.1.3 IDENTIFICAÇÃO DE RISCOS**

É o processo de identificar os eventos de impacto negativo e estes deverão ser classificados de acordo com o Dicionário de Riscos do Cibrius.



Nessa identificação serão considerados os fatores externos (econômicos, de negócio, ambientais, políticos, sociais e tecnológicos) e os internos (infraestrutura, pessoas, processos e tecnologia).

#### **6.1.4 AVALIAÇÃO DE RISCOS**

A avaliação de riscos permite que a Administração considere até que ponto os eventos, em potencial identificados, poderão impactar a realização dos objetivos.

O objetivo da avaliação é formar uma base para o desenvolvimento de estratégias (resposta a risco) de como os riscos serão gerenciados, de modo a diminuir a probabilidade de ocorrência e/ou a magnitude do impacto.

A avaliação será realizada por intermédio de análises quantitativas e qualitativas, utilizando as metodologias RSA e CSA.

Os riscos serão avaliados quanto a sua condição de inerente (original) e residual (remanescente após a mitigação por controles).

#### **6.1.5 RESPOSTA A RISCOS**

É o processo de desenvolver e determinar estratégias para gerenciar os riscos identificados.

Após a avaliação dos riscos residuais, a Administração determinará qual resposta será dada a estes, considerando os seus efeitos (impacto e frequência do evento), nível de tolerância e custo-benefício.

As várias alternativas para tratamento dos riscos são descritas abaixo:

- **Evitar o Risco:** decisão de não se envolver ou agir de forma a se retirar de uma situação de risco.
- **Aceitar o Risco:** neste caso, apresentam-se três alternativas: reter, reduzir e transferir/compartilhar o risco.
- **Reter:** manter o risco no nível atual de impacto e probabilidade.
- **Reduzir:** ações são tomadas para minimizar a probabilidade (frequência) e/ou o impacto do risco.
- **Transferir e/ou Compartilhar:** atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco.



### **6.1.6 ATIVIDADES DE CONTROLE**

As atividades de controle compreendem as políticas e procedimentos que asseguram o alcance dos objetivos, diminuindo a exposição das atividades aos riscos.

Tais atividades acontecerão ao longo do processo organizacional, em todos os níveis e em todas as funções, incluindo aprovações, autorizações, verificações, reconciliações, limites de alçada, revisões de desempenho operacional, plano de continuidade do negócio, segurança de recursos e segregação de funções.

### **6.1.7 INFORMAÇÃO E COMUNICAÇÃO**

A habilidade da administração de tomar decisões apropriadas é afetada pela qualidade da informação, que deve ser útil, isto é, apropriada, tempestiva, atual e precisa.

A importância do controle interno para a gestão das organizações está no seu potencial informativo para suporte ao processo decisório.

Informações relevantes deverão ser identificadas, coletadas e comunicadas a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão.

A comunicação das informações produzidas deverá atingir todas as partes interessadas, incluindo dirigentes, conselheiros, colaboradores, participantes, assistidos e patrocinadores, por meio de canais claros e abertos, devendo ser abrangente, consistente e frequente.

### **6.1.8 MONITORAMENTO**

O monitoramento é o processo que avalia a qualidade do desempenho dos controles internos ao longo do tempo.

A atividade de monitoramento será realizada de forma contínua e ocorrerá no decurso das atividades do Cibrius, de acordo com periodicidade estabelecida pela Área de Gestão de Riscos e Supervisão Atuarial.

As principais atividades de monitoramento incluem conciliações, auditorias internas e externas, emissão de relatórios e autoavaliações.



## **7 RESPONSABILIDADES DA GESTÃO DE RISCOS**

Para que a Gestão de Riscos seja implementada adequadamente e, exista um aprimoramento constante, é necessário que sejam definidas as responsabilidades de todos os envolvidos.

### **7.1.1 CONSELHO DELIBERATIVO**

O Conselho Deliberativo é responsável pela aprovação das propostas enviadas pela Diretoria e o monitoramento permanente do tratamento que a Diretoria está aplicando aos riscos relevantes, devendo ter no mínimo, as seguintes atribuições:

- Definir diretrizes estratégicas para a gestão de riscos;
- Aprovar as metodologias utilizadas na gestão de riscos e controles;
- Aprovar os objetivos e políticas de riscos alinhadas às estratégias do Instituto;
- Patrocinar as ações de fortalecimento e disseminação da cultura de gestão de riscos e controles internos; e
- Conhecer os riscos mais significantes e monitorar se a administração está respondendo a estes de forma adequada.

### **7.1.2 CONSELHO FISCAL**

O Conselho Fiscal é responsável pela avaliação periódica e permanente do processo de gestão de riscos, devendo ter no mínimo, as seguintes atribuições:

- Avaliar e documentar o monitoramento do processo de gestão de riscos;
- Avaliar se a estrutura para gestão de riscos é suficiente e adequada para suportar o processo implementado no Instituto; e
- Conhecer os riscos mais significantes e monitorar se a administração está respondendo a estes de forma adequada.

### **7.1.3 DIRETORIA EXECUTIVA**

A Diretoria Executiva é responsável pela definição da estrutura e do processo de gestão de riscos, devendo ter as seguintes atribuições:



- Promover ambiente de controles internos favorável que facilite a aplicação do processo de gestão de riscos;
- Avaliar e encaminhar para aprovação do Conselho Deliberativo as políticas e parâmetros para implementação do processo de gestão de riscos;
- Elaborar e aprovar o Dicionário de Riscos;
- Definir o apetite de riscos da Entidade;
- Priorizar e monitorar os planos de ação necessários para mitigar os riscos avaliados que estejam acima do apetite desejado; e
- Disseminar a cultura de gestão de riscos e controles internos.

#### **7.1.4 COMITÊ DE GESTÃO DE RISCOS**

O Comitê de Gestão de Riscos é um colegiado de assessoramento à Diretoria Executiva do Cibrius, constituído com a finalidade de apoiá-la na aplicação da gestão de riscos na Fundação, tendo as seguintes atribuições:

- Acompanhar de forma sistemática, a gestão de riscos com o objetivo de assegurar a sua eficácia e o cumprimento de seus objetivos; e
- Avaliar a eficácia e efetividade dos controles internos e gerenciamento de riscos, da Entidade.

#### **7.1.5 ÁREA DE GESTÃO DE RISCOS E SUPERVISÃO ATUARIAL**

A Área Gestão de Riscos e Supervisão Atuarial é responsável pela adoção das metodologias para identificar, avaliar e tratar os riscos, com o objetivo de manter o Instituto no caminho para alcançar a estratégia definida, controlar a exatidão e confiabilidade das informações financeiras e não financeiras, promover a eficiência operacional e motivar a adesão às políticas de direção estabelecidas, além de assegurar, em conjunto com as demais áreas da Entidade, a adequação, fortalecimento e o funcionamento da estrutura de controles internos, devendo ter as seguintes atribuições:

- Definir e manter os conceitos e metodologias aplicadas na gestão de riscos;
- Estruturar e supervisionar o processo de gestão de riscos;
- Disseminar a cultura de gestão de riscos e controles internos;
- Acompanhar as avaliações periódicas dos riscos e dos respectivos controles aplicados na Entidade;
- Validar a qualidade e os resultados das avaliações de riscos e controles;
- Alinhar o apetite a riscos com a estratégia, otimizando as decisões de resposta a riscos;
- Acompanhar os planos de ação definidos;
- Gerir o sistema de informação de riscos e controles do Instituto;



- Elaborar e divulgar os relatórios de gestão de riscos e controles internos; e
- Assessorar os comitês e conselhos no que diz respeito ao processo de gestão de riscos e controles internos.

#### **7.1.6 ÁREAS GESTORAS**

As áreas gestoras são responsáveis pelo gerenciamento dos riscos relacionados aos objetivos das atividades de sua responsabilidade, devendo ter as seguintes atribuições:

- Aplicar, nas suas esferas de atuação, os conceitos e metodologias componentes da gestão de riscos e controles internos;
- Identificar e avaliar os riscos dos seus processos;
- Realizar a gestão dos riscos de forma aderente aos objetivos e políticas de riscos;
- Participar das avaliações periódicas de riscos e controles;
- Propor níveis de apetite e tolerância em relação aos riscos sob sua responsabilidade;
- Definir e implementar os planos de ação; e
- Assimilar e disseminar a cultura de gestão de riscos e controles internos na sua esfera de atuação.

## **8 CONSIDERAÇÕES FINAIS**

Esta política baseou-se no Guia Previc de Melhores Práticas de Governança para EFPC, da Previc, bem como na norma ABNT NBR ISO 31000:2009.

A qualquer momento, mas com periodicidade mínima anual, poderá ser revisto o teor desse documento.

Esta Política de Gestão de Riscos entra em vigor a partir da data de aprovação pelo Conselho Deliberativo.