

## **PORTARIA Nº 534, DE 08 DEZEMBRO DE 2014.**

Estabelece princípios e diretrizes para gestão de riscos no âmbito do Ministério da Previdência Social e de suas entidades vinculadas, dá outras providências.

O MINISTRO DE ESTADO DA PREVIDÊNCIA SOCIAL, no uso de suas atribuições, considerando o disposto no art. 87, parágrafo único, inciso II, da Constituição Federal, e o disposto no Decreto nº 6.944, de 21 de agosto de 2009, Decreto nº 7.078, de 26 de janeiro de 2010 e Decreto nº 3.505, de 13 de junho de 2000, resolve

Art. 1º Ficam estabelecidos, no âmbito do Ministério da Previdência Social e de suas entidades vinculadas, os princípios, diretrizes e responsabilidades da gestão de riscos, bem como as orientações dos processos de contexto, identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades, incorporando a visão de riscos à tomada de decisões estratégicas, em conformidade com as melhores práticas, nos termos desta Portaria.

### **CAPÍTULO I DAS DISPOSIÇÕES GERAIS**

Art. 2º A aplicação dos princípios e diretrizes descritas nesta Portaria deverão observar:

- I - a missão, a visão e os valores institucionais, assim como os direcionadores e objetivos constantes do Planejamento Estratégico Institucional - PEI;
- II - o Plano Plurianual - PPA;
- III - as diretrizes de gestão da inovação e de desenvolvimento institucionais;
- IV - os mecanismos de desempenho institucional;
- V - as diretrizes de gestão e segurança da informação e de comunicações; e
- VI - as competências e atribuições regimentais.

Parágrafo único. As diretrizes de gestão de riscos deverão refletir eventuais alterações realizadas nos documentos mencionados neste artigo.

Art. 3º Para a gestão de riscos que trata esta Portaria, considera-se:

- I - risco: efeito da incerteza nos objetivos;
- II - gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco;
- III - estrutura da gestão de riscos: conjunto de componentes que fornecem os fundamentos e metodologias para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização;
- IV - política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;
- V - atitude perante o risco: abordagem da organização para avaliar e tomar decisão no sentido de eliminar, reduzir, transferir ou reter o risco;
- VI - apetite pelo risco: riscos que uma organização está disposta a aceitar;

- VII - aversão ao risco: atitude de afastar-se de riscos;
- VIII - plano de gestão de riscos: esquema dentro da estrutura da gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;
- IX - proprietário do risco: pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;
- X - processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos;
- XI - estabelecimento do contexto: definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos;
- XII - contexto externo: ambiente externo no qual a organização busca atingir seus objetivos;
- XIII - contexto interno: ambiente interno no qual a organização busca atingir seus objetivos;
- XIV - comunicação e consulta: processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos;
- XV - parte interessada: pessoa ou organização que pode afetar, ser afetada, ou perceber se afetada por uma decisão ou atividade;
- XVI - processo de avaliação de riscos: processo global de identificação de riscos, análise de riscos e avaliação de riscos;
- XVII - identificação de riscos: processo de busca, reconhecimento e descrição de riscos;
- XVIII - fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;
- XIX - evento: ocorrência ou alteração em um conjunto específico de circunstâncias em que um risco acontece;
- XX - consequência: resultado de um evento que afeta os objetivos;
- XXI - probabilidade: chance de algo acontecer;
- XXII - perfil de risco: descrição de um conjunto qualquer de riscos;
- XXIII - análise de riscos: processo de compreender a natureza do risco e determinar o nível de risco;
- XXIV - critérios de risco: termos de referência contra a qual o significado de um risco é avaliado;
- XXV - nível de risco: magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades;
- XXVI - avaliação de riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável;
- XXVII - controle: medida que está modificando o risco;
- XXVIII - tratamento de riscos: são as ações tomadas para eliminar, reduzir, transferir ou aceitar os riscos;
- XXIX - risco residual: remanescente após o tratamento do risco;
- XXX - monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no

nível de desempenho requerido ou esperado; e

XXXI - análise crítica: atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos.

## CAPÍTULO II DOS OBJETIVOS

Art. 4º Os objetivos da gestão de riscos devem ser perseguidos pela organização e estão dispostos na forma de:

- I - aumentar a probabilidade de atingir os objetivos e metas organizacionais;
- II - fomentar uma gestão proativa;
- III - estar atento para a necessidade de identificar e tratar os riscos através de toda a organização;
- IV - melhorar a identificação de oportunidades e ameaças;
- V - atender às normas e requisitos legais e regulamentares pertinentes;
- VI - melhorar o reporte das informações institucionais;
- VII - melhorar a governança;
- VIII - fortalecer a confiança das partes interessadas;
- IX - estabelecer uma base confiável para a tomada de decisão e balizar o planejamento;
- X - alocar e utilizar eficazmente os recursos para o tratamento de riscos;
- XI - melhorar a eficácia e a eficiência tática e operacional;
- XII - melhorar o desempenho em saúde e segurança, bem como a proteção do meio ambiente;
- XIII - melhorar a prevenção de perdas e a gestão de incidentes;
- XIV - melhorar a aprendizagem organizacional;
- XV - aumentar a resiliência da organização; e
- XVI - subsidiar a continuidade de negócio.

## CAPÍTULO III DOS PRINCÍPIOS

Art. 5º Para o alcance da eficácia na gestão de riscos, o Ministério e suas entidades vinculadas deverão promover, em todos os seus níveis, os seguintes princípios:

- I - gestão de riscos como criação e proteção de valor, que contribui para a realização demonstrável dos objetivos estratégicos, a melhoria do desempenho institucional, a qualidade, a eficiência e efetividade dos processos e serviços, bem como a tomada de decisões baseada em riscos;
- II - adoção das melhores práticas de governança corporativa de forma sistemática, estruturada e oportuna, com o objetivo de alcançar e manter a transparência e a qualidade das informações;
- III - definição e adoção de uma linguagem comum e padrão de gestão de riscos, para melhor entendimento entre as partes interessadas e um processo livre de interferências;
- IV - estruturação da gestão integrada de riscos por meio de utilização de padrões e metodologias institucionalizadas e disseminadas para todos da instituição, capaz de

se adequar às estratégias, iniciativas e estrutura organizacional;

V - facilitação da melhoria contínua da organização, por meio da implementação de estratégias inovadoras e demais aspectos de desenvolvimento institucionais;

VI - gestão de riscos deve ser considerada transparente, inclusiva, dinâmica, iterativa e capaz de reagir a mudanças, com envolvimento das partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização, assegurando que a estruturação da gestão integrada de riscos permaneça pertinente e atualizada;

VII - promoção da gestão de riscos como parte integrante de todos os processos organizacionais, de forma a garantir a identificação de eventos de riscos inerentes a todas as áreas de negócio da instituição;

VIII - estabelecimento de papéis e responsabilidades definidas e comunicadas, de cada um dos colaboradores envolvidos no processo de gestão de riscos;

IX - definição de infraestrutura para gestão de riscos de forma integrada e eficiente, que envolva tecnologia, processos e pessoas, e estabeleça mecanismos de comunicação claros e objetivos;

X - considerar fatores humanos e culturais, que reconhece as capacidades, percepções e intenções das pessoas internas e externas;

XI - alinhamento com o contexto interno e externo da instituição e com o perfil do risco;

XII - identificação baseada nas melhores informações disponíveis, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas; e

XIII - estabelecimento de análise periódica mediante comitês de riscos e gestores de riscos, que assegurem a eficácia do gerenciamento de riscos por meio de revisões frequentes, favorecendo o cumprimento de seus objetivos estratégicos.

#### CAPÍTULO IV DAS DIRETRIZES

Art. 6º As diretrizes de gestão de riscos estão caracterizadas pelos processos:

I - de estabelecimento do contexto, pela qual a organização articula seus objetivos e define os parâmetros externos e internos a serem levados, estabelece o contexto dos processos de gestão de riscos e o escopo e definição dos critérios de risco;

II - de identificação dos riscos, que objetiva reconhecer e descrever as fontes de risco, as áreas de impactos, eventos, suas causas e consequências potenciais, com a finalidade de gerar uma lista abrangente de riscos baseada nos eventos que possam impactar na realização dos objetivos.

III - de análise de riscos, que envolve desenvolver a compreensão dos riscos qualitativos e quantitativos, visando à definição dos atributos de probabilidade e impacto, fornecendo entradas para a avaliação de riscos e para as decisões sobre a necessidade dos riscos serem tratados, bem como as estratégias e métodos mais adequados de tratamento de riscos;

IV - de avaliação de riscos, que tem a finalidade de auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento;

V - de tratamento de riscos, que envolve a seleção de uma ou mais opções, para modificar os riscos e a implementação dessas opções, com objetivo de evitá-los, mitigá-los, transferi-los, ou aceitá-los, por meio de planos de ação e controles internos; e

VI - de monitoramento de riscos, que envolve verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.

Parágrafo único. A comunicação dos riscos é permanente em todas as etapas do processo de gestão de riscos e atinge a todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança.

## CAPÍTULO V DAS DISPOSIÇÕES FINAIS

Art. 7º O processo de gestão de riscos deve assegurar a suficiência, a eficácia e a eficiência de quaisquer controles.

Art. 8º Convém que a organização assegure que haja responsabilização, autoridade e competência apropriada para gerenciar riscos, incluindo a implementação e manutenção do processo de gestão de riscos, por meio:

I - da identificação dos proprietários dos riscos que têm a responsabilidade e a autoridade para gerenciá-los;

II - da identificação dos responsáveis pelo desenvolvimento, implementação e manutenção da estrutura para gerenciar riscos;

III - da identificação de outras responsabilidades, em todos os níveis da organização no processo de gestão de riscos;

IV - do estabelecimento de medição de desempenho e processos de reporte internos ou externos em relação com os devidos escalões;

V - da deliberação, assegurando os níveis apropriados de reconhecimento; e

VI - dos riscos apontados com efeitos em diversas áreas, identificar os gestores com a responsabilidade e a autoridade para gerenciá-los.

Art. 9º Esta Portaria entra em vigor a partir da data de sua publicação.

GARIBALDI ALVES FILHO