energisaprev

POLÍTICA

De Gestão de Riscos

<table>
<tr><td rowspan="2">  </td><td colspan="3">POLÍTICA</td><td>Data da Publicação:

15/06/2026</td></tr>
<tr><td>Código:

POL-000001</td><td>Versão:

02</td><td>Página

02 de 11</td><td>Data Limite de Revisão:

14/06/2031</td></tr>
<tr><td colspan="4">Título:

Política de Gestão de Riscos</td><td>Classificação:

Pública</td></tr>
<tr><td colspan="3">Processo:

Gestão de Riscos</td><td colspan="2">Responsável Técnico:

Administração Corporativa e Governança</td></tr>
<tr><td>Elaborador:

JCM - Junqueira de Carvalho e Murgel Consultores Associados</td><td>Revisor:

Administração Corporativa e Governança</td><td colspan="3">Aprovador:

Diretoria Executiva
Conselho Deliberativo</td></tr>
</table>

Versão	Data	Descrição	Elaborador/Revisor
00	27/04/2022	Aprovado na 171ª Reunião Extraordinária do Conselho Deliberativo o Programa de Gestão de Risco	Gilberto Santos
01	31/03/2023	Revisão da Política com inclusão dos itens: Documento de referência, diretrizes, conteúdo específico, aprovação e controle do processo de aprovação e ciência.	Gilberto Santos Veronica Nascimento
02	15/06/2026	Revisão da Política e ajuste do nome para “política de Gestão de Riscos”	JCM - Junqueira de Carvalho e Murgel Consultores Associados

Sumário

1. OBJETIVO

Esta Política tem por objetivo estabelecer as diretrizes para executar o processo de Gestão de Riscos da EnergisaPrev - Fundação Energisa de Previdência, além de atender as exigências legais e os normativos internos vigentes.

A Gestão de Riscos é de responsabilidade de todos na Entidade e conta com o apoio do Conselho Deliberativo e da Diretoria Executiva, que incentivam a disseminação de cultura da gestão baseada em risco entre os colaboradores da EnergisaPrev para que os riscos sejam identificados, avaliados e monitorados continuamente, visando o alcance dos objetivos operacionais e estratégicos da Entidade, bem como o fortalecimento do ambiente de governança corporativa e a aderência dos controles internos aos normativos vigentes.

2. ABRANGÊNCIA

Esta Política aplica-se aos diretores, conselheiros, patrocinadores e instituidores da EnergisaPrev, bem como aos colaboradores e prestadores de serviços envolvidos no processo de gestão de riscos.

3. FORUM DE APROVAÇÃO

Esta Política foi aprovada na 237ª Reunião Extraordinária do Conselho Deliberativo da EnergisaPrev, realizada em 27/05/2026, e vigora a partir da sua aprovação.

4. DEFINIÇÕES

Gestão de Riscos: processo para identificar, avaliar, administrar, monitorar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos da Entidade.

Risco: possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos.

Apetite ao Risco: é o nível de risco que a Entidade deseja assumir para alcançar os seus objetivos.

Tolerância ao Risco: é o limite específico de variação aceitável acima ou abaixo do apetite do risco, antes que ações corretivas sejam tomadas.

Controles Internos: conjunto de processos, políticas e procedimentos operacionalizados para fazer frente aos riscos e fornecer segurança razoável quanto ao alcance de objetivos da Entidade.

Avaliação de Riscos: processo sistemático de identificar e mensurar os riscos, além de definir medidas de controle para eliminar ou reduzir riscos em atividades organizacionais.

5. RESPONSABILIDADES

5.1. Conselho Deliberativo

O Conselho Deliberativo desempenha papel fundamental no apoio ao fortalecimento de uma estrutura para a gestão dos riscos e de conformidade. Compete ao Conselho Deliberativo:

I. Aprovar a presente Política de Gestão de Riscos e suas atualizações;
II. Incentivar as ações de fortalecimento e disseminação da cultura de gestão de riscos e controles internos;
III. Compreender os principais riscos que a EnergisaPrev está exposta e definir os níveis de apetite e de tolerância aos riscos considerados aceitáveis para suas operações; e
IV. Avaliar e aprovar o posicionamento para os riscos relevantes, acompanhando o cumprimento das ações mitigatórias.

5.2. Conselho Fiscal

O Conselho Fiscal é responsável pela fiscalização das atividades da EnergisaPrev, certificando-se que os controles internos estejam adequados para manutenção dos riscos dentro dos limites aceitáveis segundo critérios legais, regulatórios e operacionais. Compete ao Conselho Fiscal:

I. Acompanhar as atividades decorrentes da Gestão de Riscos, manifestando-se a respeito das eventuais deficiências dos controles internos e ações corretivas;
II. Acompanhar as implementações dos planos de ação definidos para o alinhamento do apetite ao risco; e
III. Avaliar as análises emitidas pela Diretoria sobre o cumprimento dessas ações corretivas, assegurando um processo contínuo de aprimoramento dos controles internos.

5.3. Diretoria Executiva

A Diretoria Executiva deve zelar pela adequação da estrutura de Gestão de Riscos compatível com o porte da Entidade e com a natureza e complexidade dos seus respectivos planos de benefícios, em conformidade com as normas internas e as legislações pertinentes e vigentes. Compete a Diretoria:

I. Avaliar e encaminhar para aprovação do Conselho Deliberativo a presente Política de Gestão de Riscos e recomendações para atualização;
II. Propor e submeter ao Conselho Deliberativo os critérios para limites de riscos aceitáveis para a EnergisaPrev;
III. Aprovar a metodologia utilizada na gestão de riscos e controles, os objetivos e os níveis de tolerância em relação a cada risco identificado ou atividade suspeita desempenhada;
IV. Promover ambiente de controles internos que facilite a aplicação do processo de Gestão de Riscos e a disseminação da cultura de Gestão de Riscos e Controles Internos, inclusive quanto aos colaboradores e prestadores de serviços envolvidos nas atividades de identificação, avaliação, monitoramento de riscos, e demais critérios e ações necessárias para operacionalização deste instrumento;
V. Deliberar sobre as ações propostas, considerando os riscos mais relevantes;
VI. Avaliar a efetividade dos sistemas e dos processos estabelecidos para a Gestão de Riscos.

5.4. Funções de Gestão de Riscos, Controles Internos e Compliance

São atividades voltadas a Gestão de Riscos e controles internos a serem desempenhas por área, comitê ou profissional dedicado, conforme a seguir:

I. Coordenar o processo de Avaliação de Riscos junto às áreas de negócio;
II. Desenvolver, implementar e aprimorar continuamente as práticas de Gestão de Riscos e Controles Internos nos níveis de processos, sistemas e Entidade;
III. Apoiar na elaboração de relatórios periódicos para a Diretoria, Conselhos e Comitês;
IV. Ser contato com as auditorias interna e externa no que diz respeito a metodologia de gestão de riscos e controles internos;
V. Assegurar que as ações para Gestão de Riscos e controles internos planejadas e aprovadas sejam executadas adequadamente;
VI. Desenvolver processos de compliance que objetivam a conformidade com leis e regulamentos e aderência às políticas e normativos internos estabelecidos;
VII. Dar suporte aos demais órgãos quanto à metodologia para Avaliação de Riscos.

5.5. Gestores e Colaboradores

Os gestores e colaboradores são responsáveis pelos riscos inerentes às suas atividades e por isso devem agir ativamente na identificação, controle e mitigação dos riscos.

Compete aos colaboradores e gestores:

I. Participar ativamente dos ciclos de Avaliação de Riscos e Controles Internos para a identificação, avaliação, tratamento e monitoramento dos riscos, inclusive os riscos relativos aos serviços terceirizados;
II. Atualizar constantemente os dados referentes aos planos de benefícios e aderência ao risco de suas patrocinadoras, instituidores, clientes, beneficiários e assistidos;
III. Disponibilizar, sempre que solicitado, informações e acesso as bases de dados à Diretoria Executiva e à área responsável pelas funções da Gestão de Riscos e Controles Internos para elaboração de análises, estudos ou relatórios de gestão de risco.

6. PRINCIPIOS E DIRETRIZES

A Gestão de Riscos é responsabilidade de todos, quer sejam, conselheiros, diretores ou colaboradores, por isso é importante que os seguintes princípios e diretrizes sejam observados:

- Desenvolver e manter cultura interna que enfatize e demonstre a importância da Gestão de Riscos e controles internos em todos os níveis hierárquicos;
- Assegurar que a Gestão de Riscos esteja integrada em todos os processos e atividades da Entidade;
- Manter uma atuação dinâmica e formalizada por intermédio da aplicação de metodologias, estrutura e ferramentas reconhecidas pelo mercado e disseminadas no âmbito da Entidade;
- Garantir que a estrutura e o processo da Gestão de Riscos sejam proporcionais

aos contextos interno e externo e alinhados aos objetivos da EnergisaPrev;
- Estabelecer uma comunicação clara, transparente, tempestiva e baseada nas melhores informações disponíveis, apoiando a tomada de decisão.

6.1. Etapas do Gerenciamento de Riscos

O processo de Gestão de Riscos é realizado observando, no mínimo as seguintes etapas:

- Identificação dos riscos;
- Avaliação dos riscos;
- Tratamento dos riscos;
- Registro e Relato; e
- Monitoramento Contínuo.

6.1.1. Identificação dos Riscos

A identificação de riscos é realizada pelas áreas técnicas/gerências, devendo considerar os contextos interno e externo, os processos sob sua responsabilidade, os sistemas, a conformidade legal e regulatória.
Para cada risco, recomenda-se a definição dos controles internos que, após serem aplicados, possam reduzir o impacto e/ou a probabilidade de incidência do risco.

6.1.2. Avaliação de Riscos

Os riscos são mensurados de acordo com a magnitude do impacto financeiro e/ou os aspectos reputacionais, legais e relacionados a imagem da Entidade e pela probabilidade de incidência.

Para cada risco, os respectivos controles internos são avaliados quanto à sua aplicabilidade e eficácia para redução da exposição do risco. A partir desta avaliação é possível verificar o nível de risco resultante, ou seja, seu nível de exposição após a aplicação dos controles.

6.1.3. Tratamento dos Riscos

Posteriormente à etapa de avaliação dos riscos, deverá ser definido o tratamento que será dado aos riscos identificados, analisados e mensurados na fase anterior e como estes devem ser monitorados, comunicados às diversas partes envolvidas, e como se pode tirar proveito do risco encontrado. Tratar os riscos consiste em decidir entre evitá-los, mitigá-los, compartilhá-los ou aceitá-los. A decisão dos gestores depende, principalmente, do grau de tolerância ao risco da EnergisaPrev, previamente definido e aprovado pela Diretoria Executiva e Conselho Deliberativo.

- **EVITAR O RISCO:** consiste na eliminação total do risco, decidindo-se por descontinuar a atividade que seja fonte do risco. É necessário avaliar se, evitando se um risco, tal decisão não aumentaria a possibilidade de outro ocorrer.

- **MITIGAR O RISCO:** consiste em implementar ou aprimorar atividades de controles, com o objetivo de reduzir o impacto e a frequência da ocorrência do risco, de forma que o custo do controle não deva exceder seus benefícios.

- **COMPARTILHAR O RISCO:** consiste em compartilhar com outras partes os impactos provocados pelo risco, geralmente buscando a reparação das perdas, reduzindo o risco a um nível compatível com as tolerâncias aceitáveis pela EnergisaPrev.

- **ACEITAR O RISCO**: consiste na aceitação, sem tomada de ação, apenas mantendo o risco identificado e mensurado no plano de gerenciamento de riscos. Simplesmente aceita-se que o risco possa acontecer e se decidirá como lidar com ele caso ocorra.

Ao determinar respostas aos riscos, a EnergisaPrev deve considerar os efeitos do impacto da ocorrência do risco e que opções de resposta são compatíveis com as tolerâncias a risco, os custos em contrapartida aos benefícios do tratamento e as possíveis oportunidades da EnergisaPrev em alcançar seus objetivos.

6.1.4. Registro e Relato

O processo de Gestão de Riscos e seus resultados são documentados e relatados por meio de mecanismo apropriado. O registro e o relato visam:

- Comunicar atividades e resultados da Gestão de Riscos em toda a Entidade;
- Prover informações para a tomada de decisão;
- Melhorar as atividades de Gestão de riscos; e
- Auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e responsabilização por atividades de Gestão de Riscos.

O registro tem por finalidade documentar a lista dos riscos identificados, considerando potenciais ameaças e respectivos planos de resposta, ou seja, os riscos com maior exposição e o tratamento que será dado para estes riscos.

O relato por sua vez, compreende a divulgação dessas informações para monitoramento, conformidade e melhoria contínua. O relato é parte integrante da governança e convém que melhore a quantidade do diálogo com as partes interessadas e apoie os órgãos de governança e de supervisão a cumprirem suas responsabilidades.

Os planos de ação e relatórios resultantes da Avaliação de Riscos serão acompanhados pela área responsável pelas funções de Gestão de Riscos e Controles Internos, com apresentações dos resultados aos Conselheiros, Diretores e aos colaboradores da EnergisaPrev.

6.1.5. Monitoramento Contínuo

Visando ao aprimoramento contínuo da Gestão de Riscos, o processo de monitoramento consiste em acompanhar o desempenho dos indicadores de gestão, supervisionar a implantação e manutenção dos planos de ação, o alcance das metas estabelecidas para a EnergisaPrev, a eficácia e eficiência dos controles internos e atividades que não estejam em conformidade com os objetivos e interesses da Entidade.

Os resultados da Avaliação dos Riscos e dos Controles Internos, decorrente dos ciclos semestrais de avaliação, são registrados no sistema de gestão baseada em riscos, os quais deverão subsidiar os órgãos de governança da EnergisaPrev com informações para

tomada de decisão e monitoramento contínuo.

6.2. Comunicação e Consulta

A comunicação visa engajar as partes interessadas, tanto internas como externas, para aumentar a conscientização sobre riscos, fundamentar decisões, trocar informações oportunas e promover apropriação dos controles. A comunicação divulga informações, enquanto a consulta obtém feedback, garantindo que diferentes perspectivas sejam consideradas em todas as etapas (identificação, avaliação, tratamento e monitoramento).

6.3. Categorias de Riscos Adotados

Há várias maneiras de se classificar os riscos, as quais algumas classes de riscos possuem entendimento especializado para as entidades – EFPC's.
As categorias de riscos adotados na EnergisaPrev estão definidas no documento Dicionário de Riscos, o qual faz parte integrante desta Política.

6.4. Matriz de Riscos

Os riscos identificados e analisados são registrados em uma matriz de riscos, catalogados de acordo com as perdas associadas, conforme as métricas definidas no documento Métricas de Avaliação de Riscos, o qual faz parte integrante desta Política.

6.5. Estrutura da Gestão de Riscos

O processo de gestão de riscos da EnergisaPrev é estruturado de acordo com o Modelo de Três Linhas de Defesa, que define uma estrutura clara de responsabilidades relacionadas a identificação, avaliação e tratamento dos riscos, bem como de comunicação e monitoramento contínuo.

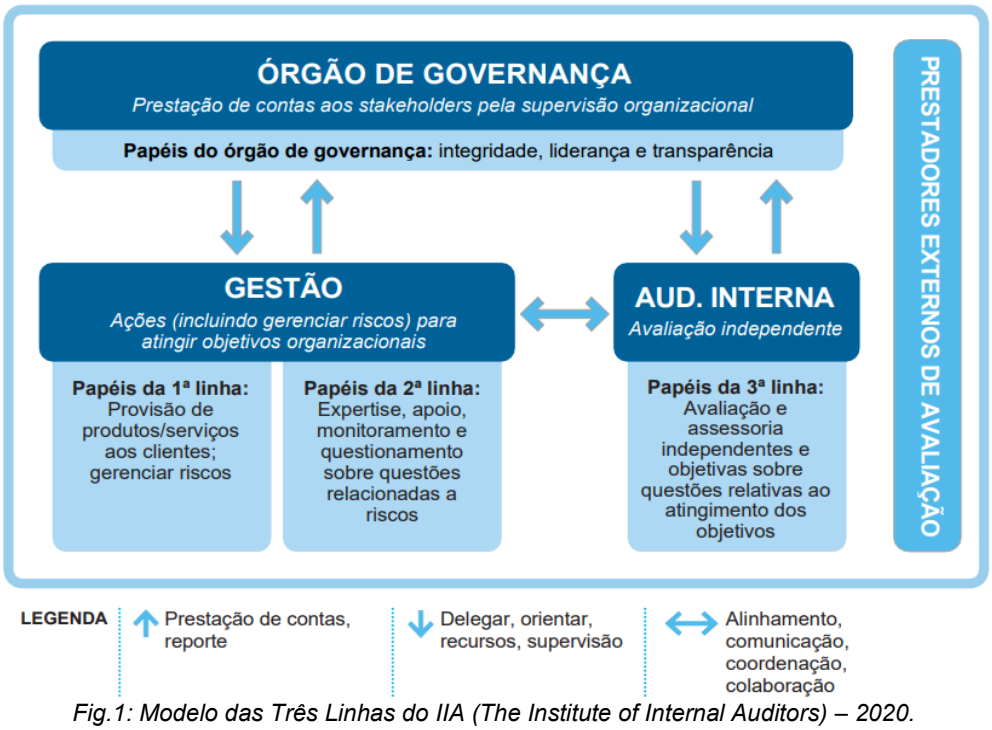

Fig.1: Modelo das Três Linhas do IIA (The Institute of Internal Auditors) – 2020.

1ª Linha de Defesa

Os papéis de primeira linha representam as funções proprietárias dos riscos, dotadas de responsabilidade e autoridade sobre os eles, representadas pelas Gerências e áreas técnicas.

A primeira linha deve implementar, manter, monitorar e revisar os controles internos, tendo por base a identificação, avaliação e o gerenciamento de riscos, visando propiciar com razoável segurança o alcance dos objetivos da Entidade, por meio dos processos conduzidos pelas áreas.

2ª Linha de Defesa

A segunda linha de defesa representa as Funções de Gestão de Riscos, Controles Internos e Compliance. Atua em conjunto com a primeira linha, visando garantir que ela tenha corretamente identificado, avaliado e reportado seus riscos. Deve atuar como facilitadora para a Gestão de Riscos, fornecendo expertise, apoio e monitoramento dos planos de ação para mitigação de riscos, bem como efetuar reportes dos resultados aos órgãos de governança da Entidade.

3ª Linha de Defesa

A terceira linha se refere às funções realizadas pelas Auditorias, as quais prestam avaliações independentes quanto à adequação e eficácia da estrutura e do processo de governança e gerenciamento de riscos implementados pela Entidade.

7. DOCUMENTOS DE REFERÊNCIA

Esta política baseou-se nos normativos vigentes que abordam gestão de riscos nas EFPC's:

- Resolução CGPC n°13, de 2004;
- Resolução CMN n° 4.994, de 2022 e atualizações;
- Recomendação MSP/CGPC n° 02, de 2009;
- Guias Previc de Melhores Práticas: Atuariais, Contábeis, Fundo de Pensão, Governança, Investimentos;
- Resolução Previc n° 23/2023 e atualizações;
- Metodologias de gestão baseada em riscos mais disseminadas no mercado;
- COSO ERM – Enterprise Risk Management – Integrating with Strategy and Performance (2017);
- COSO – Internal Control – Integrated Framework (2013);
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes;
- The Institute of Internal Auditors (IIA) - é uma associação profissional internacional organizada em 1941 para desenvolver a condição profissional da auditoria interna.

8. DISPOSIÇÕES GERAIS

Esta Política entra em vigor a partir da aprovação da Diretoria Executiva e do Conselho Deliberativo.

A Política de Gestão de Riscos deverá ser disponibilizada a todos os seus Conselheiros, Diretores e colaboradores e para todos os que atuem em nome da EnergisaPrev.

Esta Política deve ser acompanhada pelos Conselhos Deliberativo e Fiscal e pela Diretoria Executiva da EnergisaPrev, no que tange à aplicação dos procedimentos de acompanhamento e ao controle de suas diretrizes.

9. ANEXOS

- Dicionário de Riscos
- Métricas de Avaliação de Riscos

10. CONTROLE DO PROCESSO DE APROVAÇÃO E CIÊNCIA

CONTROLE SOBRE O PROCESSO DE APROVAÇÃO E CIÊNCIA		
Aprovação Diretoria Executiva	13/04/2026	8ª Reunião Extraordinária
Aprovação Conselho Deliberativo	27/05/2026	237ª Reunião Extraordinária
Ciência Conselho Fiscal	11/06/2026	22ª Reunião Extraordinária