

POLÍTICA DE GESTÃO DE RISCOS

1.	OBJETIVO	3
2.	BENEFÍCIOS	3
3.	RESPONSABILIDADES	3
3.1	Conselho Deliberativo.....	4
3.2	Conselho Fiscal	4
3.3	Diretoria Executiva.....	4
3.4	Funções de Gestão de Riscos e Controles Internos	5
3.5	Gestores e Colaboradores	6
3.6	Comitê Riscos	7
4.	ETAPAS DO GERENCIAMENTO DE RISCOS	8
4.1	Identificação dos Riscos	8
4.2	Avaliação dos Riscos e Controles	9
4.3	Tratamento dos Riscos	10
4.4	Monitoramento de Riscos	11
4.5	Exceções	12
5.	DISPOSIÇÕES GERAIS	12
	ANEXO I DEFINIÇÕES.....	13

1. OBJETIVO

Estabelecer 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, o propósito da gestão de riscos é a proteção e criação de valor e garantia da manutenção dos resultados dos planos de benefícios e da própria entidade.

Esse processo é de responsabilidade de todos na Entidade. Liderados pelo Conselho Deliberativo e Diretoria, os colaboradores no desempenho de suas atividades no dia a dia, tem como premissa que os riscos devem ser identificados, avaliados e monitorados continuamente, considerando a possibilidade de ocorrerem e os impactos sobre os negócios, caso se materializem.

A gestão de riscos, tem como função o apoio ao processo decisório de gerenciamento de recursos em ações estratégicas, além de mitigar eventuais riscos relativos a lavagem de dinheiro ou financiamento do terrorismo, fraude e corrupção para evitar que haja desvio das atividades sob gestão da EnergisaPrev para fins ilícitos.

2. BENEFÍCIOS

O gerenciamento de riscos proporciona à EnergisaPrev:

- ✓ Resguardar os seus recursos, minimizando o risco de perdas financeiras relevantes;
- ✓ Identificar oportunidades de melhoria e/ou mudanças nos processos e controles, garantindo assim a eficácia e eficiência operacional;
- ✓ Melhorar a conformidade com os normativos internos e externos; e,
- ✓ Aprimorar o processo de comunicação com as partes interessadas (internas e externas), com a transparência adequada das informações e de que forma vem assegurando o atingimento dos seus objetivos.

3. RESPONSABILIDADES

A gestão de risco é responsabilidade de todos, quer sejam, conselheiros, diretores ou colaboradores, por isso é importante:

- ✓ Desenvolver cultura interna que enfatize e demonstre a importância dos controles internos em conformidade com todos os níveis hierárquicos;
- ✓ Manter e promover conduta permanentemente pautada por elevados padrões éticos, orientando-se pela defesa dos direitos dos participantes e assistidos dos seus planos de benefícios e impedindo a utilização da EnergisaPrev em prol de interesses conflitantes com o alcance de seus objetivos; e,
- ✓ Manter altos padrões de integridade, transparência e valores éticos, por intermédio da disseminação da cultura de gestão de riscos e controles internos.

3.1 Conselho Deliberativo

O Conselho Deliberativo desempenha papel fundamental no apoio ao fortalecimento de uma estrutura para a gestão dos riscos e na conformidade da EnergisaPrev com esta Política.

Compete ao Conselho Deliberativo:

- ✓ Aprovar a presente Política de Gestão de Riscos e suas atualizações;
- ✓ Patrocinar as ações de fortalecimento e disseminação da cultura de gestão de riscos e controles internos;
- ✓ Compreender os principais riscos que a EnergisaPrev está exposta e definir os níveis de exposições considerados aceitáveis para as suas operações; e
- ✓ Avaliar e aprovar o posicionamento para os riscos relevantes.

3.2 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:

- ✓ Acompanhar as atividades decorrentes do gerenciamento de risco, manifestando-se a respeito das eventuais deficiências dos controles internos e ações corretivas;
- ✓ Acompanhar as implementações dos Planos de Ação definidos para o alinhamento dos riscos ao apetite; e
- ✓ Avaliar as análises emitidas pela Diretoria sobre o cumprimento dessas ações corretivas, assegurando um processo contínuo de aprimoramento dos controles internos.

3.3 Diretoria Executiva

A Diretoria Executiva deve zelar pela adequação da Estrutura de Gestão de Riscos compatível com a natureza e complexidade dos produtos, serviços, atividades, processos e sistemas, em conformidade com as normas internas e legislações pertinentes.

Compete à Diretoria:

- ✓ Avaliar e encaminhar para aprovação do Conselho Deliberativo a presente Política de Gestão de Riscos e recomendações para atualização;
- ✓ Propor e submeter ao Conselho Deliberativo os critérios para limites de riscos aceitáveis para a EnergisaPrev;
- ✓ Aprovar a metodologia (processo, dicionário e métricas) utilizada na gestão de riscos e controles, os objetivos e os níveis de tolerância em relação a cada risco identificado ou atividade suspeita desempenhada;
- ✓ Promover ambiente de controles internos que facilite a aplicação do processo de gestão de riscos e a disseminação da cultura de gerenciamento 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;
- ✓ Deliberar sobre as ações propostas, definindo o gerenciamento dos riscos mais relevantes;
 - ✓ Apresentar as avaliações periódicas dos riscos e controles;
 - ✓ Avaliar a efetividade dos sistemas e dos processos estabelecidos para a gestão de risco;
 - ✓ Promover a cultura organizacional da prevenção de riscos, contemplando funcionários, clientes, parceiros e terceirizados;

3.4 Funções de Gestão de Riscos e Controles Internos

São atividades voltadas a controles internos e gestão de riscos a serem desempenhados por área, comitê ou profissional dedicado:

- ✓ Participar na definição, manutenção e atualização da matriz de riscos;
- ✓ Propor e manter atualizada a metodologia (processo, dicionário e métricas) utilizada na gestão de riscos e controles;
- ✓ Coordenar o processo de autoavaliação;
- ✓ Ser contato com as auditorias interna e externa no que diz respeito a metodologia de gestão de riscos e controles internos;
- ✓ Assegurar que as ações para gestão de riscos e controles internos planejadas e aprovadas sejam executadas adequadamente;
- ✓ Acompanhar os planos de ação da EnergisaPrev;
- ✓ Desenvolver processos que objetivam a conformidade com leis e regulamentos e aderência às políticas e normativos internos estabelecidos;
- ✓ Dar suporte aos demais órgãos quanto à metodologia para elaboração da gestão e administração de risco;
- ✓ Monitorar a atualização de cadastros de pessoas expostas politicamente, nos termos da legislação aplicável, das operações, seus representantes, familiares e outras pessoas de relacionamento próximo; e
- ✓ Comunicar ao COAF, sem ciência do envolvido, no prazo de 24 (vinte e quatro) horas:
 - sempre que o resultado da análise de alguma operação ou situação indicar suspeita de lavagem de dinheiro ou financiamento de terrorismo;
 - todas as operações referentes a um mesmo participante ou assistido que superar o valor de R\$ 50.000,00 (cinquenta mil reais), exceto pagamento de benefícios, empréstimos, resgate ou portabilidade;
- ✓ Comunicar a Previc a não ocorrência de operações ou situações passíveis de comunicação a COAF relativamente ao exercício anterior;
- ✓ Implementar procedimentos, incluindo os que assegurem a devida diligência na identificação, qualificação e classificação de riscos, visando o conhecimento das patrocinadoras, os instituidores, dos participantes, dos beneficiários e dos assistidos

de planos de benefícios de caráter previdenciário administrados, parceiros, funcionários e prestadores de serviço.

Os procedimentos de devida diligência para conhecimento, qualificação e classificação de riscos devem incluir a avaliação quanto à capacidade financeira (renda ou faturamento) e manter compatibilidade com:

- (i) o perfil de risco das patrocinadoras, dos instituidores, dos participantes, dos beneficiários e dos assistidos de planos de benefícios, bem como de funcionários, parceiros e prestadores de serviços terceirizados, contemplando medidas reforçadas para clientes classificados em categorias de maior risco, de acordo com a avaliação interna de risco;
- (ii) a Norma de Prevenção e Combate à Fraude, Corrupção, Lavagem de Dinheiro e Financiamento ao Terrorismo; e
- (iii) a avaliação interna de risco.

Os cadastros dos participantes, dos beneficiários e dos assistidos de planos de benefícios devem ser atualizados permanentemente e refletir os dados necessários à sua identificação e qualificação, observados os níveis diferenciados de detalhamento, proporcionais às categorias de risco em que se enquadram, mesmo que necessárias diligências adicionais para obtenção e confirmação das informações.

3.5 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:

- ✓ Participar ativamente dos Ciclos de Autoavaliação de Riscos e Controles Internos para a identificação, avaliação, tratamento e monitoramento dos riscos; inclusive os riscos relativos aos serviços terceirizados;
- ✓ Atualizar constantemente os dados referentes aos planos de benefícios e aderência ao risco de suas patrocinadoras, instituidores, participantes, beneficiários e assistidos;
- ✓ Desenvolver e implementar, procedimentos de identificação e qualificação de clientes configurados como expostos politicamente, nos termos da legislação aplicável;
- ✓ Disponibilizar, sempre que solicitado, informações e acesso às bases de dados a Diretoria Executiva, Comitê de Riscos e Gestão de Riscos e Controles Internos para elaboração de análises, estudos ou relatórios de gestão de risco;
- ✓ Ter conhecimento dos procedimentos para denunciar conhecimento ou mera suspeita de lavagem de dinheiro, financiamento de terrorismo ou fraude de terceiros à membros da Diretoria Executiva;
- ✓ Dar conhecimento à área de Gestão de Riscos e Controles Internos das operações ativas e passivas e a identificação das pessoas físicas ou jurídicas com as quais

estabeleça qualquer tipo de relação jurídica cujo valor seja igual ou superior a R\$ 10.000,00 (dez mil reais).

No caso de pessoas expostas politicamente, residentes no exterior, para fins da identificação e qualificação, providências adicionais poderão ser adotadas como:

- (i) Solicitação de declaração expressa do cliente a respeito da sua classificação;
- (ii) Utilização de informações publicamente disponíveis; e
- (iii) Análise de bases de dados eletrônicos comerciais.

3.6 Comitê Riscos

O Comitê de Riscos é colegiado voltado ao controle e atividades descritas nesta Política. São membros Comitê:

Função	Cargo
Presidente	Diretor Administrativo e Financeiro AETQ
Membro	Coordenador de Contabilidade
Membro	Coordenador de Benefícios Previdenciários
Membro	Coordenador de TI
Membro	Assessor de Gestão DPO

São atribuições do Comitê de Riscos:

- ✓ Acompanhar a implementação e a aderência a esta política e à Norma de Prevenção e Combate à Fraude, Corrupção, Lavagem de Dinheiro e Financiamento ao Terrorismo;
- ✓ Avaliar as recomendações de melhoria da metodologia adotada e do sistema de gestão de riscos e controles internos;
- ✓ Analisar as propostas para ampliação do processo de gestão de riscos e controles internos;
- ✓ Validar as propostas de adequação das definições de riscos e controles internos utilizadas pela EnergisaPrev;
- ✓ Acompanhar o processo de autoavaliação;
- ✓ Analisar o resultado do processo de autoavaliação;
- ✓ Acompanhar a implementação dos planos de ação;
- ✓ Informar à Diretoria e ao Conselho Deliberativo sobre a análise dos resultados;
- ✓ Apreciar os relatórios e sugestões realizadas pelos órgãos reguladores e os auditores internos e externos; Fiscalizar os procedimentos internos a fim de identificar práticas de lavagem de dinheiro ou financiamento de terrorismo.
- ✓ Aprovar o calendário anual de reuniões do Comitê proposto pelo Presidente para o ano civil subsequente, até a última reunião do ano em curso;

Relatório de avaliação de efetividade anual do Comitê de Riscos com data-base de 31 de dezembro, deve ser encaminhado, para ciência, até 30 de junho do ano seguinte ao da data-base ao Conselho Fiscal e ao Conselho Deliberativo, contemplando, no mínimo:

- (i) os procedimentos destinados ao conhecimento de patrocinadoras, os instituidores, dos participantes, dos beneficiários e dos assistidos de planos de benefícios, incluindo a verificação e a validação das informações destes e a adequação dos dados cadastrais;
- (ii) os procedimentos de monitoramento, seleção, análise e comunicação ao COAF, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas;
- (iii) a governança da Norma de Prevenção e Combate à Fraude, Corrupção, Lavagem de Dinheiro e Financiamento ao Terrorismo;
- (iv) os procedimentos destinados ao conhecimento de funcionários, parceiros e prestadores de serviços terceirizados; e
- (v) as medidas de desenvolvimento da cultura organizacional voltadas à prevenção da lavagem de dinheiro e ao financiamento do terrorismo.

4. ETAPAS DO GERENCIAMENTO DE RISCOS

O processo de gestão de riscos deverá ser realizado observando, no mínimo as seguintes etapas:

- ✓ Identificação;
- ✓ Avaliação;
- ✓ Tratamento aos Riscos;
- ✓ Monitoramento.

4.1 Identificação dos Riscos

A identificação dos riscos tem o objetivo de reconhecer e descrever os riscos aos qual a **EnergisaPrev** está exposta, considerando que a classificação do risco deve ser feita, tanto quanto possível, em relação às causas da perda e não de suas consequências, uma vez que a eficácia das medidas de mitigação será maior se elas forem orientadas para as causas das ocorrências.

Considerando que podem ocorrer alterações no conjunto de exposições ao risco, trazidas por mudanças nos processos internos (seguridade, investimento, administrativo, contábeis etc.) ou pelo ambiente (regulamentação, patrocinadoras, fornecedores, participantes etc.), anualmente o dicionário de riscos será reavaliado.

4.1.1 Identificação dos Riscos de Lavagem de Dinheiro e do Financiamento do Terrorismo

A identificação e mensuração do risco de utilização de produtos e serviços da EnergisaPrev na prática da lavagem de dinheiro e do financiamento do terrorismo levará em consideração, adicionalmente, os perfis de risco:

- (i) das patrocinadoras, os instituidores, dos participantes, dos beneficiários e dos assistidos de planos de benefícios de caráter previdenciário administrados;
- (ii) da entidade;
- (iii) das operações, planos e produtos disponibilizados; e
- (iv) das atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados.

O risco identificado deve ser avaliado quanto à probabilidade de ocorrência e à magnitude dos impactos financeiro, jurídico e reputacional.

Sempre que possível, deverão ser utilizadas e comparadas as avaliações realizadas por entidades públicas do país relativas ao risco de lavagem de dinheiro e de financiamento do terrorismo.

4.2 Avaliação dos Riscos e Controles

A avaliação de risco pode ser realizada por metodologia quantitativa ou qualitativa. Em ambas, a mensuração é definida a partir do conhecimento das variáveis frequência (probabilidade de ocorrência) e severidade (impacto financeiro).

A entidade elabora a matriz de riscos por processo e área, que visa categorizar o risco e propiciar comparações entre os eventos de risco potencial, permitindo a priorização para tratamento preventivo dos riscos, o gerenciamento e de mitigação reforçados para as situações de maior risco e a adoção de controles simplificados nas situações de menor risco. São identificados os eventos de risco potencial, que são classificados conforme o dicionário de riscos e são mensurados de acordo com os critérios de impacto e frequência.

Nesta Política a abordagem é qualitativa, o nível de risco é avaliado a partir de atribuição de critérios de frequência e impacto.

É adotada como metodologia orientadora:

- ✓ COSO - *Committee of Sponsoring Organizations of the Treadway Commission* que define uma estrutura e um processo de gestão de riscos com objetivo de manter a

entidade em busca aos seus objetivos estratégicos, operacionais, compliance e transparência.

A classificação com base no perfil de risco das patrocinadoras, os instituidores, dos participantes, dos beneficiários e dos assistidos de planos de benefícios nas categorias de risco definidas na avaliação interna de risco, levará em consideração, ainda, as informações obtidas nos procedimentos de identificação e de qualificação de tais clientes fixados nesta política.

A avaliação para elaboração da matriz de riscos será documentada, preferencialmente, anual, denominada Ciclo de Autoavaliação, sendo conduzida pelo responsável pela Gestão de Riscos ou Comitê de Riscos com a participação dos gestores e colaboradores responsáveis pelos processos.

Concluída a avaliação de riscos, esta deverá ser aprovada pela Diretoria Executiva e encaminhada para ciência ao Conselho Fiscal e ao Conselho Deliberativo.

A avaliação será revisada a cada dois anos ou quando ocorrer alteração significativa nos perfis das patrocinadoras, dos instituidores, dos participantes, dos beneficiários e dos assistidos de planos de benefícios de caráter previdenciário administrados; da entidade; das operações ou das atividades exercidas pelos funcionários, com o intuito de manter atualizado o objetivo da EnergisaPrev.

Os planos de ação e relatórios resultantes da autoavaliação serão acompanhados pela área de Gestão ou Comitê de Riscos e serão apresentados aos Órgãos de Governança.

4.3 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, tal como, 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 pelo 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 de riscos que não podem ser eliminados, nos quais seu benefício deverá ser maior

do que seu custo.

- **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 em aceitar o risco atuando na implantação ou alteração de práticas de gestão e controle, de caráter preventivo, ou seja, reduzindo a frequência e o impacto das ocorrências do risco.

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.

As decisões tomadas a partir do tratamento de riscos, observarão os requisitos legais, regulatórios e demais normas internas.

4.4 Monitoramento de Riscos

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, interesses ou estejam sendo realizadas de forma ilícita.

O monitoramento, a seleção e a análise devem identificar, também, operações e situações que possam indicar suspeitas de lavagem de dinheiro e de financiamento do terrorismo, considerando a Norma de Prevenção e Combate à Fraude, Corrupção, Lavagem de Dinheiro e Financiamento ao Terrorismo, a avaliação interna de risco a condição de pessoa exposta politicamente, seu representante, familiar ou pessoas de seu relacionamento próximo, em especial:

- (i) contribuição ao plano de benefícios, pelo participante ou assistido, cujo valor seja incompatível com a sua ocupação profissional ou com seus rendimentos, considerado isoladamente ou em conjunto com outras contribuições do mesmo participante ou assistido;
- (ii) aporte ao plano de benefícios efetuado por terceiro que não a patrocinadora, cujo valor seja igual ou superior a R\$ 10.000,00 (dez mil reais);
- (iii) negociação com pagamento em espécie, a uma mesma pessoa física ou jurídica, cujo valor seja superior a R\$ 10.000,00 (dez mil reais);
- (iv) operações realizadas que, por sua habitualidade, valor ou forma, configurem artifício para evitar procedimentos de identificação, qualificação, registro,

- monitoramento e seleção de riscos segundo esta política; e
- (v) operações realizadas e os produtos e serviços contratados que, considerando as partes envolvidas, os valores, as formas de realização, os instrumentos utilizados ou a falta de fundamento econômico ou legal, possam configurar a existência de indícios de lavagem de dinheiro ou de financiamento do terrorismo.

Os resultados da identificação e avaliação dos riscos e dos controles internos, decorrente dos ciclos anuais de autoavaliação, deverão ser registrados em relatórios específicos, que subsidiarão aos órgãos de governança da EnergisaPrev.

4.5 Exceções

Os casos não previstos nesta política deverão ser avaliados após manifestação do Conselho Deliberativo, salvo expressamente previsto em determinação legal.

5. DISPOSIÇÕES GERAIS

Este documento tem efeito de Política e entra em vigor a partir da sua aprovação pelo 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 e 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.

A inobservância dos procedimentos estabelecidos nesta resolução por parte dos órgãos estatutários e colaboradores será avaliada pelo Comitê de Riscos.

Esta Política de Gestão de Riscos foi aprovada na 149ª Reunião Extraordinária do Conselho Deliberativo da EnergisaPrev, realizada no dia 8 de dezembro de 2020.

ANEXO I DEFINIÇÕES

Apetite ao risco: nível de risco aceitável pela Entidade na busca e realização de sua missão, visão e objetivos estratégicos.

Autoavaliação de controles (CSA): metodologia que avalia a adequação dos processos de gerenciamento de risco e a efetividade dos controles internos estabelecidos para minimizar os riscos do negócio.

Compliance: conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da EnergisaPrev, bem como prevenir, evitar, detectar e tratar qualquer desvio ou não conformidade que possa ocorrer.

Controles internos: conjunto de todas as políticas e boas práticas adotadas pela EnergisaPrev com intuito de mitigar riscos e melhorar processos.

Frequência: É a possibilidade de materialização do risco ocorrer.

Gestão de riscos: processo cujo objetivo é prevenir, identificar, mensurar e controlar o impacto de possíveis riscos.

Impacto: consequência resultante da ocorrência do evento de risco impactando sobre os objetivos traçados pela entidade.

Processos/projetos: conjunto de tarefas ou atividades desempenhadas pelas unidades/ áreas da EnergisaPrev.

Risco: é a probabilidade de perda ou a incerteza associada ao cumprimento de um objetivo, sendo inerente a qualquer atividade.

Risco original: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais (controles) que possam reduzir a frequência de sua ocorrência ou seu impacto.

Risco residual: risco remanescente após a implementação de atividades de controle que visam reduzir sua probabilidade de ocorrência e/ou impacto.

Tolerância a riscos: capacidade que a Entidade tem em suportar o impacto e/ou consequências de determinados riscos.