

**NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**  
**GOVERNANÇA CORPORATIVA**  
**Versão 5 de 28.03.2018**

## **1. FINALIDADE**

Definir princípios e diretrizes para a Gestão Integrada de Riscos Corporativos, no âmbito de atuação da Companhia Paranaense de Energia – Copel (Holding), de suas subsidiárias integrais (SIs), e controladas, respeitado seus trâmites societários.

A presente Política é aplicável, em caráter indicativo, às suas empresas controladas em conjunto, empresas coligadas e outras participações societárias.

Para efeito desta Política, o conjunto das empresas relacionadas no parágrafo anterior será doravante denominado Copel.

## **2. CONCEITOS**

### **2.1 - GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**

É um processo estruturado e contínuo, desenhado para identificar e responder proativamente a eventos em potencial capazes de afetar os objetivos da Copel, buscando a manutenção dos riscos em níveis adequados. O processo divide-se em cinco macro etapas: Identificação, Avaliação, Tratamento, Monitoramento e Comunicação. Na Copel, tal modelo tem como base o COSO - ERM (*Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management*) e o Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC.

### **2.2 - RISCO**

Possibilidade de que um evento venha a ocorrer e afete adversamente a realização dos objetivos, podendo gerar impacto negativo, positivo ou ambos, sendo risco quando o efeito é negativo e oportunidade quando o resultado é positivo.

O risco é medido em termos de impacto (ou consequência) e probabilidade e os tipos de risco considerados são os seguintes:

- a) risco inerente: é o risco existente antes da adoção de ações de tratamento que visem alterar a probabilidade ou o impacto da materialização do risco; e
- b) risco residual: é o risco remanescente após a adoção de ações de tratamento do risco inerente.

### **2.3 - EVENTO**

Incidente ou ocorrência gerada com base em fontes internas ou externas, que afeta a realização dos objetivos.

### **2.4 - PROBABILIDADE**

Indica a possibilidade de ocorrência de um dado evento.

Pode ser expressa em termos quantitativos, como: porcentagem, frequência de ocorrência, ou outra métrica numérica, ou em termos qualitativos, como: alto, médio, baixo.

### **2.5 - IMPACTO**

Resultado ou efeito de um evento que afeta os objetivos. Os impactos (ou as consequências) podem ser expressos qualitativa ou quantitativamente. O impacto de um evento poderá ser positivo ou negativo em relação aos objetivos da organização.

### **2.6 - INCIDENTE**

Evento imprevisto e indesejável com potencial para causar transtornos que podem inviabilizar o alcance dos objetivos gerando perdas financeiras, danos de imagem e impactos operacionais.

### **2.7 - CONTROLE INTERNO**

Conjunto de políticas e procedimentos que são desenvolvidos e operacionalizados para garantir razoável certeza

**NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**  
**GOVERNANÇA CORPORATIVA**  
**Versão 5 de 28.03.2018**

2/7

acerca do atingimento dos objetivos organizacionais relacionados a operações, divulgação e conformidade. A Copel adota a estrutura de controles internos do COSO 2013 - *Internal Control Integrated Framework*.

#### 2.8 - APETITE AO RISCO

Está associado ao nível de risco que a Copel está disposta a aceitar para alcançar a realização de sua missão e visão e gerar valor para os acionistas.

#### 2.9 - TOLERÂNCIA AO RISCO

A variação aceitável relativa à realização dos objetivos da Copel.

#### 2.10 - PAPÉIS DA GESTÃO DE RISCO

##### 2.10.1 - CONSELHO DE ADMINISTRAÇÃO - CAD

Órgão de deliberação colegiada responsável por:

- Fixar a orientação geral dos negócios da Copel;
- definir o grau de apetite aos riscos;
- estabelecer o papel das diretorias no gerenciamento de riscos;
- aprovar o plano anual de riscos estratégicos;
- aprovar a Política de Gestão Integrada de Riscos Corporativos;
- avaliar a efetividade do processo de gestão de riscos na Copel; e
- analisar semestralmente a Matriz de Riscos e os planos de mitigação decorrentes.

##### 2.10.2 - COMITÊ DE AUDITORIA ESTATUTÁRIO - CAE

Órgão independente, de caráter consultivo e permanente, subordinado ao Conselho de Administração, responsável por:

- Revisar e supervisionar o processo de apresentação de relatórios contábeis e financeiros;
- avaliar a efetividade do processo de gestão de riscos na Copel;
- supervisionar as atividades dos auditores internos e auditores externos independentes e;
- revisar Política de Gestão Integrada de Riscos Corporativos periodicamente; e
- analisar trimestralmente a Matriz de Riscos e os planos de mitigação decorrentes.

##### 2.10.3 - TRÊS LINHAS DE DEFESA

- 1ª linha de defesa: É formada pelas Diretorias Executivas, superintendentes e gerentes das áreas, além dos gestores de projetos e processos. Esta linha é responsável por identificar e avaliar os riscos e conduzir os procedimentos de controles rotineiramente a fim de mitigar as vulnerabilidades de suas atividades.
- 2ª linha de defesa: Fornece estruturas de gerenciamento de riscos, controles internos e *compliance*, auxiliando a 1ª linha de defesa no desenvolvimento de processos e controles eficazes. A Diretoria de Governança, Risco e *Compliance* atua na 2ª linha de defesa.
- 3ª linha de defesa: Realiza avaliações independentes sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a 1ª e a 2ª linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle. A Auditoria Interna integra a 3ª linha de defesa.

##### 2.10.3.1 – Diretorias (1ª Linha de Defesa)

São as estruturas responsáveis por:

---

*Diretoria de Gestão Empresarial – DGE*

*Coordenação de Desenvolvimento Organizacional e Processos – CDO*

**NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**  
**GOVERNANÇA CORPORATIVA**  
**Versão 5 de 28.03.2018**

- 
- Patrocinar a implantação da gestão de riscos no âmbito de sua atuação;
  - definir os gestores responsáveis pela identificação e avaliação dos riscos inerentes às suas atividades;
  - apoiar os gestores de riscos no estabelecimento das ações de tratamento e dos mecanismos de controles para os riscos identificados; e
  - apoiar a Diretoria de Governança, Risco e Compliance - DRC na elaboração do plano anual de riscos estratégicos.

**2.10.3.2 - Gestor de Riscos (1ª Linha de Defesa)**

É o indivíduo dentro da Copel responsável por:

- Identificar os riscos, as suas causas e o seus impactos para a Copel;
- estabelecer as ações de tratamento e os mecanismos de controles adequados para cada risco;
- realizar o monitoramento periódico dos riscos sob sua responsabilidade; e
- reportar, seguindo a metodologia e os padrões definidos, todos os riscos à Diretoria de Governança, Risco e Compliance.

**2.10.3.3 - Diretoria de Governança, Risco e Compliance - DRC (2ª Linha de Defesa)**

É a estrutura organizacional da Copel (Holding) responsável por:

- Definir e coordenar a implantação das diretrizes, políticas, metodologias e práticas de controles internos e gerenciamento de riscos corporativos na Copel;
- zelar pela efetiva disseminação e adequada aplicação das políticas e metodologias;
- elaborar, em conjunto com as Diretorias, o plano anual de riscos estratégicos;
- administrar o portfólio de riscos corporativos da Copel;
- monitorar as ações de tratamento e os mecanismos de controles para os riscos identificados; e
- reportar, periodicamente, as atividades de gestão de riscos ao Comitê de Auditoria Estatutário e ao CAD.

**2.10.3.4 - Auditoria Interna (3ª Linha de Defesa)**

É a estrutura organizacional independente responsável por:

- Avaliar a efetividade do processo de gestão de riscos na Copel;
- Avaliar a adequação das ações de tratamento e mecanismos de controles internos, recomendando, quando necessário, melhorias nos processos ao gestor de riscos; e
- Realizar reportes periódicos de suas avaliações ao Conselho de Administração e ao Comitê de Auditoria Estatutário.

**2.11 - MATRIZ DE RISCO**

Documento no qual são registrados os riscos, as causas, os impactos, os níveis de exposição, os gestores de risco, os processos, ações de tratamento e outras informações relevantes para monitoramento dos riscos identificados. A representação gráfica deste documento é realizada através do *Heatmap* (Mapa Térmico).

**3. PRINCÍPIOS**

**3.1 - PROTEÇÃO E GERAÇÃO DE VALOR PARA COPEL**

A gestão de riscos está diretamente relacionada com o crescimento sustentável da Copel, identificando as ameaças e fornecendo informações para tomada de decisões baseada em riscos.

## **NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**

### **GOVERNANÇA CORPORATIVA**

**Versão 5 de 28.03.2018**

4/7

---

#### **3.2 - INTEGRAÇÃO DA GESTÃO DE RISCOS COM A DEFINIÇÃO DAS ESTRATÉGIAS E MONITORAMENTO DE PERFORMANCE**

A gestão de riscos deve apoiar a Administração durante o processo de definição das estratégias e monitoramento de performance a fim de assegurar o alinhamento dos objetivos estratégicos com a missão, visão e valores da Copel.

#### **3.3 - ESTABELECIMENTO FORMAL DE PAPÉIS E RESPONSABILIDADES**

Cada papel durante o processo de gestão de risco precisa ser definido formalmente e os envolvidos devem ser comunicados e entender claramente as suas responsabilidades.

#### **3.4 - CONSTITUIÇÃO E MANUTENÇÃO DE INFRAESTRUTURA ADEQUADA**

É essencial que uma infraestrutura de gestão de riscos integrada de processos, tecnologia e pessoas seja constituída e avaliada periodicamente pelos órgãos de governança, a fim de que sua estrutura permaneça eficiente.

#### **3.5 - DEFINIÇÃO DE METODOLOGIA COMUM PARA TODA COMPANHIA**

Uma linguagem comum deve ser adotada no processo de gestão de riscos, utilizando metodologias e padrões reconhecidos, adaptados a perfil de negócios e estrutura organizacional da Copel.

### **4. DIRETRIZES**

4.1 - Manter a política de gestão de riscos alinhada com os objetivos e estratégias da Copel.

4.2 - Manter efetividade e conformidade no ambiente de controles internos.

4.3 - Assegurar que haja monitoramento de riscos de corrupção e de fraude no ambiente de controles internos.

4.4 - Integrar o processo de gestão de riscos nas relações comerciais com fornecedores e parceiros de negócio.

4.5 - Adotar indicadores de desempenho empresarial para o monitoramento da Gestão Integrada de Riscos Corporativos.

4.6 - Assegurar que os riscos severos com probabilidade de ocorrência muito baixa também sejam considerados na formulação de estratégias.

4.7 - Considerar aspectos socioambientais, de sustentabilidade empresarial, saúde e segurança, buscando antecipar, avaliar e reduzir os impactos de curto, médio e longo prazo das operações à sociedade.

4.8 - Integrar e manter os níveis de apetite ao risco alinhados com as dimensões de estratégia, negócios e finanças da Copel.

4.9 - Adotar práticas para reporte e controle de incidentes.

4.10 - Adotar critérios de apetite ao risco que, periodicamente, devem ser submetidos à apreciação do Conselho de Administração - CAD.

4.11 - Direcionar as oportunidades identificadas às áreas competentes para análise e implementação das ações necessárias à sua realização.

4.12 - Assegurar que os riscos e controles associados sejam revisados, no mínimo, anualmente, de acordo com os critérios relacionados à exposição de seu risco associado.

4.13 - Assegurar que os processos e atividades que envolvem a Gestão Integrada de Riscos Corporativos sejam exercidos pelas três linhas de defesa.

4.14 - Assegurar que haja o estabelecimento e manutenção de alçadas de aprovação e segregação de funções entre as atividades.

4.15 - Assegurar que o processo de identificação e análise geral de riscos seja monitorado e continuamente aprimorado para identificar os riscos eventualmente não conhecidos.

## **NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**

### **GOVERNANÇA CORPORATIVA**

**Versão 5 de 28.03.2018**

5/7

4.16 - Promover a cultura da gestão de riscos, em especial nas empresas controladas, controladas em conjunto e coligadas.

#### **5. CATEGORIAS DE RISCO**

A Copel definiu as categorias para classificação de seus riscos, considerando as quatro classes de objetivos do COSO – ERM, a natureza de suas operações e a relação com suas atividades:

##### **5.1 - RISCO ESTRATÉGICO**

- Estratégia - riscos que estão associados à tomada de decisão da alta administração e ao planejamento estratégico, podendo gerar perda substancial no valor econômico da Copel.
- Reputação - possibilidade de perdas decorrentes da deterioração da marca da Copel junto ao mercado, clientes e órgãos reguladores, em razão de publicidade negativa.

##### **5.2 - RISCO FINANCEIRO**

- Mercado - risco de que o valor justo ou os fluxos de caixa futuros de instrumento financeiro oscilem devido a mudanças nos preços de mercado, tais como as taxas de câmbio, taxas de juros e preços de ações.
- Liquidez - representado pela possibilidade de insuficiência de recursos, caixa ou outro ativo financeiro, para liquidar as obrigações nas datas previstas.
- Crédito - risco de incorrer em perdas decorrentes da dificuldade de recebimento de valores faturados a seus clientes ou de uma contraparte em um instrumento financeiro, resultantes da falha destes em cumprir com suas obrigações contratuais.
- Divulgação - risco associado à possibilidade de emissão de relatórios financeiros, gerenciais, regulatórios, fiscais, estatutários incompletos, inexatos ou intempestivos, expondo a Copel a multas, penalidades ou outras sanções.

##### **5.3 - RISCO OPERACIONAL**

- Processos - risco relacionado à eficácia e eficiência das operações da Copel, inclusive as metas de desempenho financeiro e operacional e a salvaguarda de perda de ativos e à possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.
- Tecnologia da Informação - riscos de acesso não autorizado a dados e informações da companhia, decorrente de vulnerabilidades de controles de acesso, falha de segregação de funções, violação de políticas, acarretando ataques externos, paradas no ambiente de TI, alteração ou divulgação indevida de informações.
- Socioambiental - riscos relacionados aos impactos das operações da Copel na sociedade e no meio ambiente, podendo afetar a reputação e gerar autuação dos órgãos fiscalizadores. Está relacionado, também, com o efeito das intempéries climáticas severas, escassez de recursos naturais ou mobilização de comunidades, podendo causar interrupção na prestação dos serviços ou prejuízo na produção de energia.
- Projetos - riscos relacionados aos projetos de transmissão, geração, distribuição, telecomunicações, pesquisa e desenvolvimento, entre outros, podendo implicar em custos adicionais, atraso na entrega do projeto e autuação por órgãos reguladores.

##### **5.4 - RISCO DE COMPLIANCE**

- Leis e normas - não conformidade com leis ambientais, trabalhistas, tributárias e regulatórias às quais a Copel está sujeita, incluindo políticas e normas internas, expondo a Companhia à autuação por órgãos reguladores.
- Fraude e corrupção - riscos relacionados ao roubo de ativos físicos, agenciamento de informações, desvios de recursos financeiros, conflito de interesses, tráfico de influência, suborno, propina, conluio com

**NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**  
**GOVERNANÇA CORPORATIVA**  
**Versão 5 de 28.03.2018**

6/7

---

fornecedores e clientes, entre outros, podendo implicar em perdas financeiras, multas, sanções e penalidades por órgãos fiscalizadores e deterioração da imagem da Copel.

**6. LEGISLAÇÃO E NORMAS RELACIONADAS AO ASSUNTO**

- a) Lei Federal nº 12.846/2013 (Lei Anticorrupção);
- b) Decreto Federal nº 8.420/2015 (Regulamenta a Lei Anticorrupção);
- c) Lei Federal 13.303/2016 (Lei das Estatais);
- d) Lei Federal nº 8.429/1992 (Lei da improbidade administrativa);
- e) Lei norte-americana Sarbanes-Oxley, de 2002, com destaque para as seções 302 e 404;
- f) Lei norte-americana Foreign Corrupt Practices Act (FCPA), de 1977;
- g) Norma ABNT NBR ISO 31000:2009;
- h) NPC 0101 - Política de Aplicação Financeira;
- i) NPC 0103 - Política de Divulgação de Informações relevantes e preservação de sigilo;
- j) NPC 0105 - Política de Relações com Investidores;
- k) NPC 0310 - Política de Comunicação;
- l) NPC 0303 - Política de Sustentabilidade;
- m) NPC 0301 - Política de Segurança da Informação;
- n) NPC 0106 - Política de Transação com Partes Relacionadas e Conflitos de Interesses;
- o) NPC 0308 - Política de Governança Corporativa;
- p) NAC 030901 - Gestão de Processos;
- q) NAC 030905 - Gerenciamento de Portfólio e de Projetos;
- r) COSO - ERM (*Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management*);
- s) Modelo de Gestão de Riscos publicado pela Fundação Nacional da Qualidade – FNQ;
- t) Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC; e
- u) Instrução CVM 586 – 08 de junho de 2017.

Atualiza a NPC 0104 de 19.09.2016.

---

Esta Política foi aprovada na 2.284ª Reunião de Diretoria - Redir em 22.01.2018 e na 174ª Reunião Ordinária do Conselho de Administração – CAD em 23.01.2018.

Documento original assinado por:

**ANTONIO SERGIO DE SOUZA GUETTER**  
Diretor Presidente

**NPC 0104 POLÍTICA DE GESTÃO INTEGRADA DE RISCOS CORPORATIVOS**  
**GOVERNANÇA CORPORATIVA**  
**Versão 5 de 28.03.2018**

Controle de alterações		
Data	Responsável	Descrição
19.09.2016	<p align="center">CIC Marco Antonio Biscaia Roberto Chylajenko Zarpelon</p> <p align="center">Analista de Gestão VPLO M<sup>a</sup> de Fátima</p>	<p>Inclusões:</p> <p>Impacto positivo e oportunidade no conceito de risco, item 2.6</p> <p>Cumprimento de normas e políticas internas como risco de <i>compliance</i>, alínea “d” do item 2.10 Perfil de Riscos.</p> <p>Diretriz 4.12 de submeter anualmente os critérios de apetite ao risco adotados ao Comitê de Auditoria, em substituição à tabela de parâmetro de apetite ao risco.</p> <p>Diretriz 4.13 relativa às oportunidades identificadas.</p>
28.03.2018	<p align="center">CIC/CRCC Felipe Borba da Silva</p> <p align="center">Analista de Gestão CDO M<sup>a</sup> de Fátima</p>	<p>Adequação à estrutura organizacional vigente.</p> <p>Alterações:</p> <ul style="list-style-type: none"> <li>• Atualização dos conceitos de Gestão Integrada de Riscos Corporativos, risco e evento para adequá-los ao COSO ERM, itens 2.1 a 2.3;</li> <li>• ajuste no item 4.5 para definir que monitoramento é para a gestão integrada de gestão de riscos e não apenas dos riscos;</li> <li>• acrescentados aspectos de saúde e segurança na diretriz 4.7; e</li> <li>• atualização da legislação relacionada ao assunto, tópico 6.</li> </ul> <p>Inclusões:</p> <ul style="list-style-type: none"> <li>• Conceitos de Papéis na Gestão de Riscos, Linha de Defesa e Matriz de Risco, item 2.10 e subitens; e</li> <li>• Diretrizes 4.12 a 4.16.</li> </ul> <p>Exclusões:</p> <ul style="list-style-type: none"> <li>• Conceitos de controladas e coligadas; e</li> <li>• conceitos de fraude e corrupção.</li> </ul>