

Especificação Técnica para contratação de *Enterprise Risk Assessment*

1. Objetivo

Esta Especificação Técnica tem por objetivo estabelecer os requisitos para a contratação de empresa especializada na prestação de serviços de consultoria para a realização de uma Avaliação Corporativa de Riscos (*Enterprise Risk Assessment – ERA*) do Centro Nacional de Pesquisa em Energia e Materiais (CNPEM).

A contratação tem como finalidade identificar, analisar, avaliar e priorizar os principais riscos que possam impactar o alcance dos objetivos estratégicos, científicos, operacionais e institucionais do CNPEM, considerando seus processos, projetos, ativos, operações e o contexto de atuação da instituição.

O trabalho deverá contemplar a identificação e a avaliação dos riscos inerentes às atividades do CNPEM, a análise da efetividade dos controles existentes, a determinação do nível de exposição aos riscos, a identificação de oportunidades de aprimoramento da governança e da gestão corporativa de riscos, bem como a proposição de recomendações e de um plano estruturado de ações para mitigação, monitoramento e tratamento dos riscos identificados.

A avaliação deverá abranger, de forma integrada, os principais riscos estratégicos, operacionais, financeiros, científicos, tecnológicos, regulatórios, ambientais, de pessoas, de segurança, de continuidade de negócios e de integridade, observadas as particularidades do ambiente de pesquisa, desenvolvimento e inovação do CNPEM, incluindo a operação de infraestruturas científicas de grande porte, a gestão de projetos e recursos públicos, as relações com órgãos governamentais, agências de fomento, parceiros nacionais e internacionais, usuários e demais partes interessadas.

Como resultado, espera-se que a consultoria forneça uma visão estruturada da exposição ao risco da organização, subsidiando a alta administração na tomada de decisões, na definição de prioridades para tratamento dos riscos e no fortalecimento da governança, dos controles internos e da gestão corporativa de riscos.

2. Detalhamento do serviço a ser contratado

A empresa contratada será responsável pela execução de uma Avaliação Corporativa de Riscos (*Enterprise Risk Assessment – ERA*) no âmbito do Centro Nacional de Pesquisa em Energia e Materiais (CNPEM), contemplando todas as etapas necessárias à identificação, análise, avaliação, priorização e proposição de ações para tratamento dos riscos institucionais, de forma a subsidiar o fortalecimento da governança, dos controles internos e da gestão corporativa de riscos.

Os serviços deverão ser conduzidos de forma integrada e colaborativa, envolvendo as áreas técnicas, científicas, administrativas e de apoio do CNPEM, proporcionando uma visão abrangente dos riscos associados às atividades, processos, projetos, ativos, infraestrutura, pessoas e objetivos institucionais.

A execução dos serviços deverá contemplar, no mínimo, as seguintes atividades:

2.1 Planejamento do projeto

- a) Realizar reunião de abertura (*kick-off*) com os representantes designados pelo CNPEM;
- b) Elaborar Plano de Trabalho contendo metodologia, cronograma detalhado, etapas de execução, responsabilidades, produtos, estratégia de comunicação e forma de acompanhamento do projeto;
- c) Definir, em conjunto com o CNPEM, a governança do projeto, os interlocutores responsáveis e o fluxo de validação das informações produzidas.

2.2 Compreensão do contexto organizacional

- a) Analisar o contexto institucional do CNPEM, incluindo sua estratégia, missão, objetivos institucionais, estrutura organizacional, cadeia de valor, macroprocessos e ambiente interno e externo;
- b) Realizar levantamento e análise da documentação institucional relevante, incluindo políticas, normas, procedimentos, planejamento estratégico, regulamentos internos, estrutura de governança, processos, relatórios, indicadores e demais documentos necessários à execução dos trabalhos;
- c) Identificar as principais partes interessadas (*stakeholders*) e compreender suas interfaces com as atividades do CNPEM.

2.3 Identificação dos riscos

- a) Realizar entrevistas, *workshops*, reuniões técnicas, questionários, análise documental e demais técnicas de levantamento de informações consideradas necessárias. A estratégia de levantamento de informações deverá assegurar representatividade adequada da estrutura organizacional do CNPEM, contemplando, no mínimo, todas as Diretorias, os Laboratórios Nacionais, as áreas corporativas e demais unidades organizacionais abrangidas pelo escopo desta contratação. A definição do quantitativo de entrevistas, workshops, reuniões técnicas e demais atividades de levantamento será proposta pela Contratada no Plano de Trabalho e dependerá de aprovação prévia do CNPEM, devendo ser tecnicamente justificada e suficiente para garantir a adequada identificação, análise e avaliação dos riscos institucionais.
- b) Identificar os riscos associados aos processos, projetos, atividades, ativos, infraestrutura, pessoas e objetivos institucionais;
- c) Identificar causas, consequências, fatores de risco, vulnerabilidades, eventos de risco e controles existentes.

A identificação dos riscos deverá contemplar, no mínimo, os seguintes grupos:

- riscos estratégicos;
- riscos operacionais;
- riscos financeiros;
- riscos científicos;



- riscos tecnológicos;
- riscos regulatórios e legais;
- riscos ambientais;
- riscos relacionados às pessoas;
- riscos de segurança;
- riscos de continuidade dos negócios;
- riscos de integridade, incluindo aspectos relacionados à ética, fraude, corrupção, conflitos de interesses, desvios de conduta, transparência, relacionamento com terceiros, proteção da imagem institucional e demais fatores capazes de impactar a confiança, a credibilidade e a reputação do CNPEM.

2.4 Análise e Avaliação dos Riscos

- a) Avaliar a probabilidade de ocorrência e os impactos potenciais dos riscos identificados;
- b) Avaliar a efetividade dos controles existentes;
- c) Determinar o nível de risco inerente e, quando aplicável, o nível de risco residual;
- d) Classificar e priorizar os riscos de acordo com critérios previamente definidos e validados com o CNPEM;
- e) Identificar interdependências entre riscos, fatores agravantes e potenciais impactos sobre os objetivos institucionais.

2.5 Avaliação da estrutura de Gestão de Riscos

- a) Avaliar a estrutura atualmente adotada pelo CNPEM para gestão de riscos;
- b) Identificar oportunidades de aprimoramento da governança, dos processos de gestão de riscos e dos controles internos;
- c) Avaliar o grau de integração da gestão de riscos aos processos de planejamento, tomada de decisão e gestão institucional.

2.6 Consolidação dos resultados

- a) Elaborar o inventário corporativo de riscos;
- b) Consolidar a Matriz Corporativa de Riscos;
- c) Elaborar Mapa de Calor (*Heat Map*) e demais representações gráficas que facilitem a visualização da exposição institucional aos riscos;
- d) Consolidar os controles existentes, as vulnerabilidades identificadas e as oportunidades de melhoria.

2.7 Recomendações e Plano de Ação

- a) Propor recomendações para eliminação, mitigação, tratamento, monitoramento ou aceitação dos riscos identificados;
- b) Priorizar as ações propostas considerando criticidade, impacto, urgência, esforço de implementação e benefícios esperados;
- c) Elaborar plano estruturado para fortalecimento da gestão corporativa de riscos, contemplando recomendações para aprimoramento da governança, dos controles internos e dos mecanismos de monitoramento.

2.8 Apresentação dos resultados



- a) Realizar reuniões de validação dos resultados com as áreas envolvidas;
- b) Apresentar os resultados consolidados à Alta Administração do CNPEM;
- c) Entregar os produtos finais previstos nesta Especificação Técnica e realizar reunião de encerramento do projeto, contemplando a apresentação das principais conclusões e a transferência de conhecimento à equipe designada pelo CNPEM.

2.9 Diretrizes para execução dos serviços

A metodologia proposta pela empresa contratada deverá ser compatível com a complexidade institucional do CNPEM e utilizar diferentes técnicas de levantamento, coleta, análise e validação de informações, de modo a assegurar a consistência, a confiabilidade e a abrangência dos resultados.

A execução dos trabalhos não poderá se limitar à aplicação de questionários ou formulários eletrônicos como única técnica de coleta de informações. A consultoria deverá utilizar, de forma integrada e complementar, análise documental, entrevistas individuais, *workshops*, reuniões técnicas, validações com gestores, visitas técnicas e outros instrumentos que se mostrarem adequados à compreensão dos processos e à identificação dos riscos.

Sempre que necessário, deverão ser realizadas visitas técnicas às instalações do CNPEM, incluindo laboratórios, unidades de pesquisa, áreas administrativas e demais ambientes considerados relevantes para a adequada compreensão dos processos, operações e atividades institucionais.

A metodologia deverá assegurar a participação das áreas envolvidas, a validação das informações obtidas junto aos respectivos responsáveis e a consolidação de uma visão corporativa dos riscos, considerando as interdependências entre processos, unidades organizacionais, projetos e objetivos estratégicos.

Durante toda a execução do contrato, a empresa contratada deverá manter comunicação periódica com o gestor do contrato e com a equipe designada pelo CNPEM, apresentando a evolução das atividades, os resultados parciais, os riscos relacionados à execução do projeto, eventuais desvios de cronograma e as medidas adotadas para sua mitigação.

A Contratada deverá prever a realização de atividades presenciais e remotas durante a execução do projeto, conforme a natureza dos trabalhos e as diretrizes estabelecidas pelo CNPEM. Serão obrigatórias a realização da reunião de abertura (kick-off), das reuniões de validação dos resultados e da apresentação executiva final, podendo o CNPEM determinar a realização presencial dessas atividades, bem como de visitas técnicas e demais reuniões que entender necessárias para a adequada compreensão do ambiente institucional e para a execução dos serviços.

3. Metodologia e requisitos técnicos mínimos

A empresa contratada deverá apresentar e aplicar metodologia estruturada para a execução da Avaliação Corporativa de Riscos (*Enterprise Risk Assessment – ERA*),



compatível com as melhores práticas de gestão de riscos, governança e controles internos, contemplando todas as etapas necessárias ao desenvolvimento dos trabalhos.

A metodologia deverá ser fundamentada em referenciais reconhecidos nacional e internacionalmente, observando, sempre que aplicável, as diretrizes da ISO 31000 – Gestão de Riscos, do COSO Enterprise Risk Management (ERM) e de demais boas práticas relacionadas à gestão corporativa de riscos, sem prejuízo da utilização de métodos e ferramentas complementares que agreguem valor à execução do projeto.

A metodologia proposta deverá contemplar, no mínimo:

3.1 Planejamento e Governança

- a) definição das etapas de execução do projeto;
- b) definição dos mecanismos de governança, comunicação e acompanhamento;
- c) estabelecimento dos critérios para validação das informações e dos produtos.

3.2 Levantamento de informações

A coleta de informações deverá utilizar diferentes técnicas de levantamento, incluindo, sempre que necessário:

- análise documental;
- entrevistas individuais;
- *workshops*;
- reuniões técnicas;
- aplicação de questionários;
- visitas técnicas;
- validações junto aos gestores e especialistas das áreas.

A utilização exclusiva de questionários eletrônicos não será considerada suficiente para atendimento ao escopo desta contratação.

3.3 Identificação dos Riscos

A metodologia deverá possibilitar a identificação estruturada dos eventos de risco relacionados aos objetivos estratégicos, processos, projetos, ativos, infraestrutura e atividades institucionais do CNPEM.

Sempre que aplicável, os riscos deverão ser descritos considerando, no mínimo:

- evento de risco;
- causas;
- consequências;
- controles existentes;
- fatores de vulnerabilidade;
- áreas responsáveis.

3.4 Avaliação dos Riscos

A metodologia deverá prever critérios objetivos para avaliação e priorização dos riscos identificados, contemplando, no mínimo:

- probabilidade de ocorrência;
- impacto;
- efetividade dos controles existentes;
- nível de risco inerente;
- nível de risco residual, quando aplicável;
- critérios para priorização dos riscos.

Os critérios adotados deverão ser previamente apresentados e validados pelo CNPEM antes do início da etapa de avaliação.

3.5 Consolidação e Validação

Os resultados obtidos deverão ser consolidados e submetidos à validação junto às áreas envolvidas e aos representantes designados pelo CNPEM, assegurando consistência técnica, rastreabilidade das informações e alinhamento institucional.

3.6 Recomendações

Com base nos riscos identificados e avaliados, a empresa contratada deverá apresentar recomendações para seu tratamento, contemplando, sempre que possível:

- eliminação ou redução das causas do risco;
- fortalecimento dos controles internos;
- implementação de controles adicionais;
- compartilhamento ou transferência de riscos, quando aplicável;
- aceitação do risco, quando tecnicamente justificável;
- mecanismos de monitoramento e acompanhamento.

As recomendações deverão considerar a realidade operacional do CNPEM, sua capacidade de implementação, a relação custo-benefício das medidas propostas e sua contribuição para o fortalecimento da governança institucional.

3.7 Princípios gerais

Durante toda a execução do projeto, a metodologia deverá observar os seguintes princípios:

- abordagem corporativa e integrada da gestão de riscos;
- participação ativa das áreas envolvidas;
- independência técnica na condução dos trabalhos;
- objetividade e fundamentação das análises;
- rastreabilidade das informações utilizadas;
- transparência dos critérios empregados;
- confidencialidade das informações acessadas;
- foco na geração de valor para a gestão institucional e no fortalecimento da governança.

4. Qualificação da equipe técnica

A empresa contratada deverá possuir comprovada experiência na prestação de serviços compatíveis com o objeto desta contratação, demonstrando capacidade técnica para execução de projetos de Enterprise Risk Assessment (ERA), gestão corporativa de riscos, governança corporativa, controles internos ou serviços de natureza equivalente, desenvolvidos em organizações de médio ou grande porte, preferencialmente em instituições de elevada complexidade organizacional, científica, tecnológica ou com atuação em ambientes regulados.

A execução dos serviços deverá ser realizada por equipe técnica qualificada e compatível com a complexidade do projeto, composta por profissionais com experiência na condução de diagnósticos organizacionais, identificação, análise e avaliação de riscos corporativos, facilitação de entrevistas e workshops, elaboração de matrizes de riscos, proposição de planos de tratamento e fortalecimento de estruturas de governança, gestão de riscos e controles internos.

A Contratada deverá designar um Coordenador de Projeto responsável pela interlocução com o CNPEM, pelo planejamento, coordenação técnica, acompanhamento da execução dos trabalhos e garantia da qualidade dos produtos entregues, assegurando a disponibilidade dos profissionais necessários ao cumprimento do escopo contratual durante toda a vigência do projeto.

Será considerado desejável que a equipe técnica possua certificações ou qualificações reconhecidas nas áreas de gestão de riscos, governança, auditoria, controles internos ou gerenciamento de projetos, tais como ISO 31000, COSO Enterprise Risk Management (ERM), CRMA, CIA, CCSA, PMP ou equivalentes.

A substituição de qualquer integrante da equipe técnica durante a execução do contrato somente poderá ocorrer mediante prévia anuência do CNPEM, devendo o profissional substituto possuir qualificação e experiência iguais ou superiores às do profissional originalmente indicado, de modo a não comprometer a qualidade técnica dos serviços contratados.

Produtos e Entregáveis

A empresa contratada deverá entregar, no mínimo, os seguintes produtos, observando os prazos estabelecidos no cronograma executivo aprovado pelo CNPEM.

Produto 1 – Plano de Trabalho

Documento contendo:

- metodologia detalhada de execução;
- cronograma físico das atividades;
- plano de comunicação;
- governança do projeto;
- responsabilidades das partes;
- relação das informações e documentos necessários ao desenvolvimento dos trabalhos;
- cronograma de entrevistas, reuniões técnicas e oficinas.

O Plano de Trabalho deverá ser submetido à aprovação do CNPEM antes do início das atividades de diagnóstico.

**Produto 2 – Diagnóstico Institucional**

Relatório contendo a compreensão do contexto organizacional do CNPEM, incluindo:

- contexto institucional;
- estrutura organizacional;
- macroprocessos;
- cadeia de valor;
- principais processos críticos;
- ambiente interno e externo;
- principais partes interessadas;
- fatores internos e externos capazes de influenciar a exposição aos riscos.

Produto 3 – Inventário corporativo de Riscos

Documento contendo o registro estruturado dos riscos identificados durante o projeto.

Cada risco deverá conter, sempre que aplicável:

- identificação do risco;
- categoria;
- descrição;
- causa(s);
- consequência(s);
- área ou processo relacionado;
- controles existentes;
- avaliação do risco inerente;
- avaliação da efetividade dos controles;
- avaliação do risco residual, quando aplicável;
- classificação de criticidade.

Produto 4 – Matriz Corporativa de Riscos

Documento consolidando a avaliação dos riscos identificados, contendo, no mínimo:

- classificação dos riscos;
- critérios utilizados para avaliação;
- probabilidade;
- impacto;
- nível de risco;
- priorização;
- responsáveis pelas ações de tratamento, quando definidos.

Produto 5 – Mapa Corporativo de Riscos (*Heat Map*)

Representação gráfica da distribuição dos riscos identificados, permitindo visualizar:

- riscos críticos;
- riscos elevados;
- riscos moderados;
- riscos baixos;
- distribuição por categoria;
- distribuição por área ou macroprocesso, quando aplicável.

Produto 6 – Avaliação da Estrutura de Gestão de Riscos

Relatório contendo:



- avaliação da estrutura atual de gestão de riscos do CNPEM;
- análise dos controles existentes;
- identificação de lacunas;
- oportunidades de melhoria;
- recomendações para fortalecimento da governança e dos controles internos.

Produto 7 – Plano de Tratamento dos Riscos

Documento contendo recomendações para tratamento dos riscos priorizados, contemplando, sempre que possível:

- ação recomendada;
- objetivo da ação;
- benefício esperado;
- prioridade;
- prazo sugerido para implementação;
- área responsável;
- dependências para implementação.

Produto 8 – Relatório Executivo Final

Relatório consolidado contendo:

- resumo executivo;
- metodologia aplicada;
- principais atividades desenvolvidas;
- síntese dos riscos identificados;
- análise consolidada da exposição institucional aos riscos;
- principais vulnerabilidades;
- oportunidades de melhoria;
- recomendações estratégicas;
- conclusões do projeto.

O relatório deverá ser apresentado em linguagem executiva, permitindo sua utilização pela Alta Administração como instrumento de apoio à tomada de decisão.

Produto 9 – Apresentação Executiva

Apresentação institucional destinada à Alta Administração do CNPEM, contendo:

- visão geral do projeto;
- metodologia utilizada;
- principais riscos identificados;
- análise da exposição institucional;
- principais recomendações;
- prioridades para implementação das ações.

A apresentação deverá ser realizada presencialmente ou por videoconferência, conforme definição do CNPEM.

Produto 10 – Transferência de conhecimento

Ao término do projeto, a empresa contratada deverá realizar atividade de transferência de conhecimento para a equipe designada pelo CNPEM, contemplando:



- metodologia utilizada;
- critérios de avaliação dos riscos;
- estrutura dos produtos entregues;
- orientações para atualização periódica da matriz de riscos;
- recomendações para manutenção e evolução da gestão corporativa de riscos.

Todo o material produzido durante a execução do contrato, incluindo relatórios, matrizes, planilhas, apresentações, bases de dados, registros e demais documentos, deverá ser entregue ao CNPEM em formato editável e em formato PDF, passando a integrar o patrimônio informacional da instituição.

5. Critérios de aceite dos produtos

Os produtos previstos nesta Especificação Técnica serão submetidos à análise e ao aceite do CNPEM, que verificará sua conformidade com o escopo contratado, a metodologia aprovada e os requisitos técnicos estabelecidos neste documento.

O aceite dos produtos dependerá do atendimento, no mínimo, aos seguintes critérios:

- aderência ao escopo desta Especificação Técnica;
- conformidade com a metodologia aprovada pelo CNPEM;
- consistência técnica das análises e recomendações;
- cobertura adequada do escopo organizacional definido para o projeto;
- atendimento aos requisitos previstos para cada produto;
- entrega dos arquivos em formato editável e PDF.

Caso sejam identificadas inconsistências, omissões ou não conformidades, o CNPEM poderá solicitar os ajustes ou complementações necessárias, sem ônus adicional para a Contratante, somente sendo emitido o aceite após a regularização das pendências.

Escopo organizacional da avaliação

A Avaliação Corporativa de Riscos deverá contemplar o CNPEM de forma abrangente, considerando sua estrutura organizacional, seus processos de negócio, suas atividades de pesquisa, desenvolvimento e inovação, bem como suas atividades administrativas, de apoio e de governança.

A empresa contratada deverá adotar abordagem corporativa, considerando a interação entre processos, áreas, projetos, infraestrutura, ativos e objetivos institucionais, de forma a identificar riscos que possam impactar o desempenho e a sustentabilidade da organização.

A avaliação deverá contemplar, sempre que aplicável:

- unidades de pesquisa;
- laboratórios e infraestruturas científicas;
- áreas administrativas;
- áreas de apoio;
- processos corporativos;
- projetos estratégicos;
- programas institucionais;
- atividades relacionadas à gestão de recursos públicos;

- relacionamento com usuários, pesquisadores, parceiros, fornecedores, agências de fomento, órgãos governamentais e demais partes interessadas.

O escopo deverá abranger tanto os processos finalísticos quanto os processos de suporte, considerando suas interdependências e sua contribuição para o alcance dos objetivos institucionais.

A empresa contratada deverá identificar os processos e atividades críticas para o funcionamento do CNPEM, avaliando os riscos associados à sua execução e os respectivos mecanismos de controle existentes.

Caso, durante o desenvolvimento dos trabalhos, sejam identificados processos, unidades organizacionais ou atividades inicialmente não previstas, mas considerados relevantes para a adequada compreensão da exposição institucional aos riscos, a empresa contratada deverá comunicar formalmente o gestor do contrato e apresentar justificativa técnica para sua inclusão no escopo da avaliação.

A definição da abrangência definitiva dos trabalhos será validada pelo CNPEM durante a fase de planejamento do projeto, podendo ser ajustada de comum acordo entre as partes, desde que não implique redução do escopo originalmente previsto nesta Especificação Técnica.

6. Cronograma de Execução

A empresa contratada deverá apresentar, como parte do Plano de Trabalho, cronograma executivo detalhado contendo as atividades, os responsáveis, as dependências entre as etapas e os respectivos marcos de entrega, observando, no mínimo, as seguintes fases:

Fase	Atividades Principais
Fase 1 – Planejamento	Reunião de abertura (<i>kick-off</i>), definição da governança do projeto, elaboração e aprovação do Plano de Trabalho.
Fase 2 – Diagnóstico Institucional	Levantamento documental, compreensão do contexto organizacional, identificação dos macroprocessos e das partes interessadas.
Fase 3 – Levantamento e Identificação dos Riscos	Entrevistas, oficinas de trabalho (<i>workshops</i>), reuniões técnicas, visitas técnicas e demais atividades de levantamento de informações.
Fase 4 – Análise e Avaliação dos Riscos	Consolidação das informações, avaliação dos riscos, análise da efetividade dos controles, classificação e priorização dos riscos.
Fase 5 – Consolidação dos Resultados	Elaboração da Matriz Corporativa de Riscos, Inventário de Riscos, Mapa de Calor (<i>Heat Map</i>) e demais produtos previstos nesta Especificação Técnica.
Fase 6 – Recomendações e Plano de Tratamento	Elaboração das recomendações, do Plano de Tratamento dos Riscos e da Avaliação da Estrutura de Gestão de Riscos.
Fase 7 – Encerramento do Projeto	Apresentação executiva dos resultados, validação dos produtos finais, transferência de conhecimento e encerramento formal do projeto.



O cronograma executivo deverá prever reuniões periódicas de acompanhamento com o gestor do contrato e com a equipe designada pelo CNPEM, em periodicidade a ser definida durante a fase de planejamento.

Eventuais ajustes no cronograma poderão ser realizados durante a execução do contrato, desde que previamente justificados pela empresa contratada e aprovados pelo CNPEM, sem prejuízo do prazo global estabelecido para a execução dos serviços.

Os produtos previstos nesta Especificação Técnica somente serão considerados concluídos após análise e aceite formal do CNPEM, podendo ser solicitados ajustes ou complementações sempre que os documentos apresentados não atenderem aos requisitos técnicos estabelecidos.

7. Vigência

O contrato terá vigência de 240 (duzentos e quarenta) dias corridos, contados da data de sua assinatura, podendo ser prorrogado, mediante justificativa e interesse das partes, nos termos do Regulamento de Compras e Contratações do CNPEM.

Campinas, 15 de julho de 2026

Michelle Pereira Guimarães

Michelle Guimarães
Gerente de Compliance
Assessoria de Compliance

Antonio Jose Roque Da Silva

Antonio José Roque da Silva
Diretor-Geral
Diretoria-Geral