1. OBJETIVO

Estabelecer os princípios, objetivos e metodologia e diretrizes aplicáveis para o procedimento de gestão de riscos, com critérios que orientem na identificação, análise, avaliação, tratamento e monitoramento contínuo dos riscos que podem afetar a organização.
O procedimento suporta o sistema de gestão de segurança da informação estabelecendo os procedimentos de gestão de riscos para possíveis ameaças à confidencialidade, integridade e disponibilidade da informação.

2. ABRANGÊNCIA

Este procedimento se aplica aos planos, às metas, às estratégias, às ações, aos objetivos, aos programas, aos projetos, às atividades e a todos os processos do NEES, sejam da Governança ou dos Projetos.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO 31000 – Gestão de Risco.
- Norma ABNT NBR ISO 31010 – Gestão de Riscos - Técnicas para o processo de avaliação de riscos.
- Norma ABNT NBR ISO 27001 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos

4. DEFINIÇÕES

- Risco: é o efeito da incerteza nos objetivos impactando os resultados desejados de uma organização. Pode ser algo esperado ou inesperado e pode gerar consequências adversas ou oportunidades.
- Gerenciamento de riscos: processo dinâmico e contínuo efetuado por todos os membros da organização com o intuito de identificar, avaliar, tratar, comunicar e monitorar potenciais eventos ou situações para fornecer razoável certeza quanto ao alcance dos objetivos organizacionais.
- Classificação de riscos: é a classificação dos tipos de riscos definidos pelas organizações, observadas as características de sua área de atuação e as particularidades do setor de atuação.

- Causa: fatores que podem levar à ocorrência de um risco.
- Impacto: resultado ou efeito de um evento de risco.

5. DIRETRIZES

5.1 Princípios para a Gestão de Riscos no NEES

Os princípios são fundamentos essenciais que orientam o processo eficaz de gestão de riscos e garantem que a abordagem adotada seja estruturada, integrada e alinhada aos objetivos estratégicos, operacionais e de conformidade da organização.

a. universalidade: deve abranger todas as atividades organizacionais.

b. uniformidade: deve observar os mesmos conceitos, parâmetros e procedimentos em todas as unidades e níveis.

c. transparência: deve envolver todas as partes interessadas para melhor entendimento e tomada de decisão.

d. consistência: deve ser baseada nas melhores informações disponíveis utilizando dados confiáveis para análise e decisão.

5.2 Objetivos da Gestão de Riscos no Âmbito do NEES

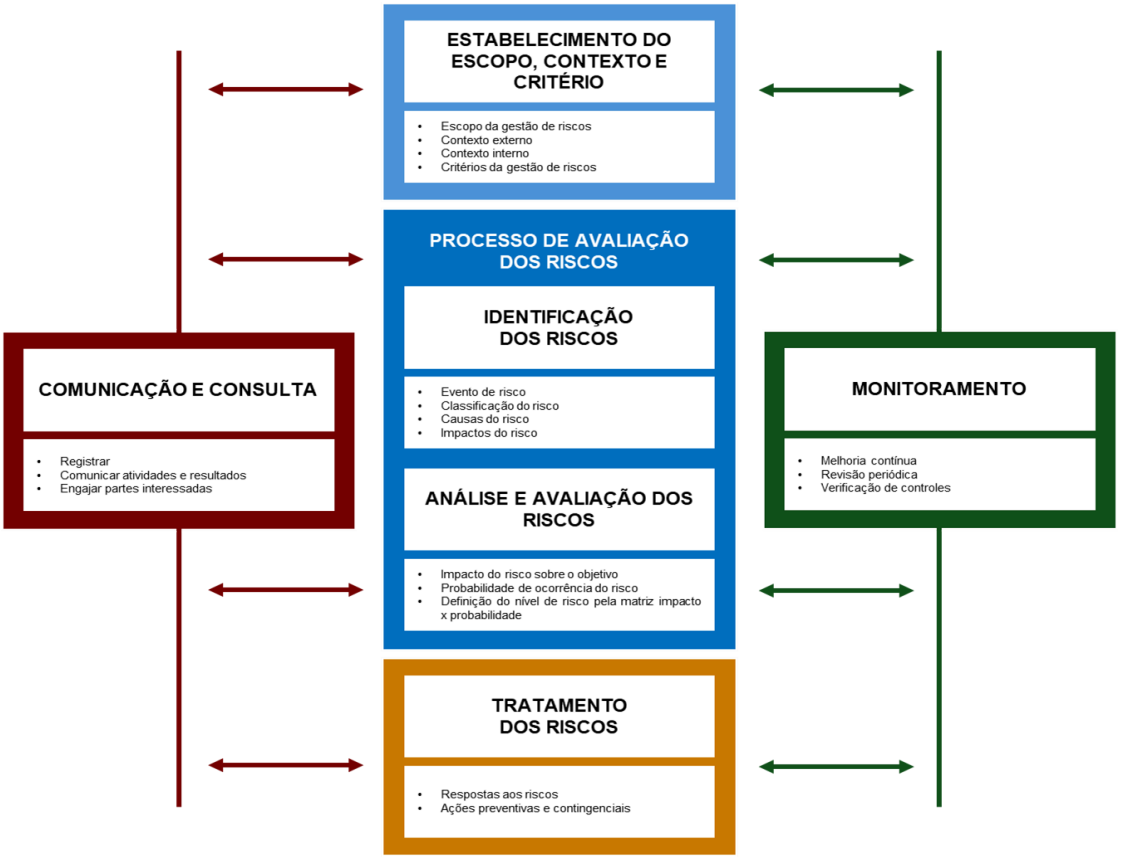
O principal objetivo é proteger e criar valor para a organização por meio do gerenciamento e controle de eventos que venham a interferir no cumprimento dos objetivos.

a. assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso à informações estruturadas suficientes quanto aos riscos aos quais estão expostos.
b. aumentar a probabilidade de alcance dos objetivos da organização, minimizando a severidade de eventos adversos e maximizando riscos positivos que possam gerar valor.
c. assegurar conformidade com requisitos legais e regulatórios.
d. proteger ativos, recursos e reputação, evitar prejuízos financeiros, danos à imagem e impactos na continuidade dos negócios.
e. promover a melhoria contínua das atividades da organização.
f. fortalecer a segurança da informação por meio de mecanismos de apoio à confidencialidade, integridade e disponibilidade das informações e promoção de uma cultura organizacional baseada na prevenção, monitoramento e resposta efetiva.

5.3 Metodologia para a Gestão de Risco no NEES

A metodologia para a gestão de riscos foi elaborada com base nas boas práticas existentes relativas aos métodos de gerenciamento de riscos e adaptada para atender a estrutura, contexto interno e externo e objetivos do NEES.

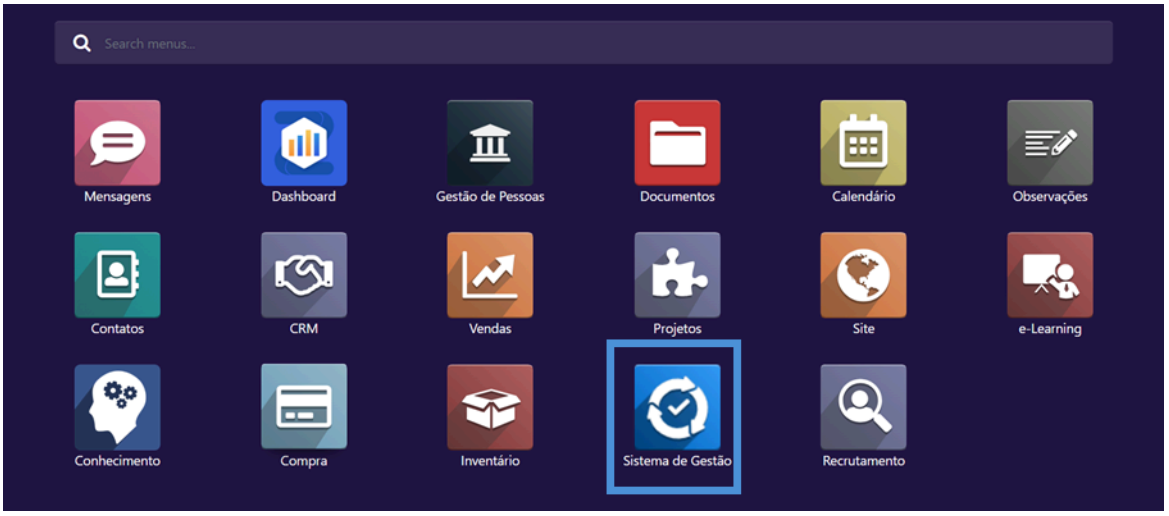
Figura 01 – Metodologia de Gestão de Riscos no NEES



5.4 Solução Tecnológica para a Gestão de Riscos no NEES

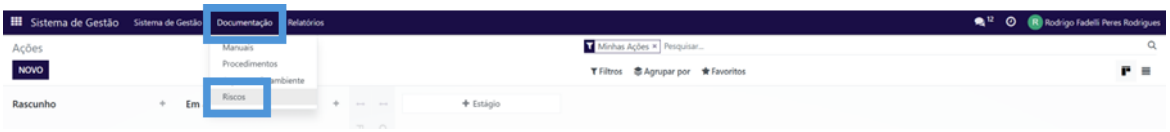
A gestão de riscos no NEES tem como instrumento de apoio o Sistema INTEGRA\ Módulo Riscos. O acesso ao módulo deve ser realizado por meio do painel inicial do sistema, conforme apresentado na fig. 02.

Figura 02 – Painel Inicial Sistema Integra



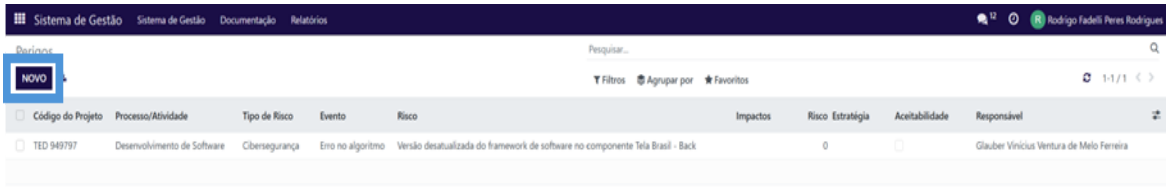
O próximo passo é acessar o Painel de Riscos na tela inicial dos Sistemas de Gestão.

Figura 03 – Painel Inicial Sistema de Gestão



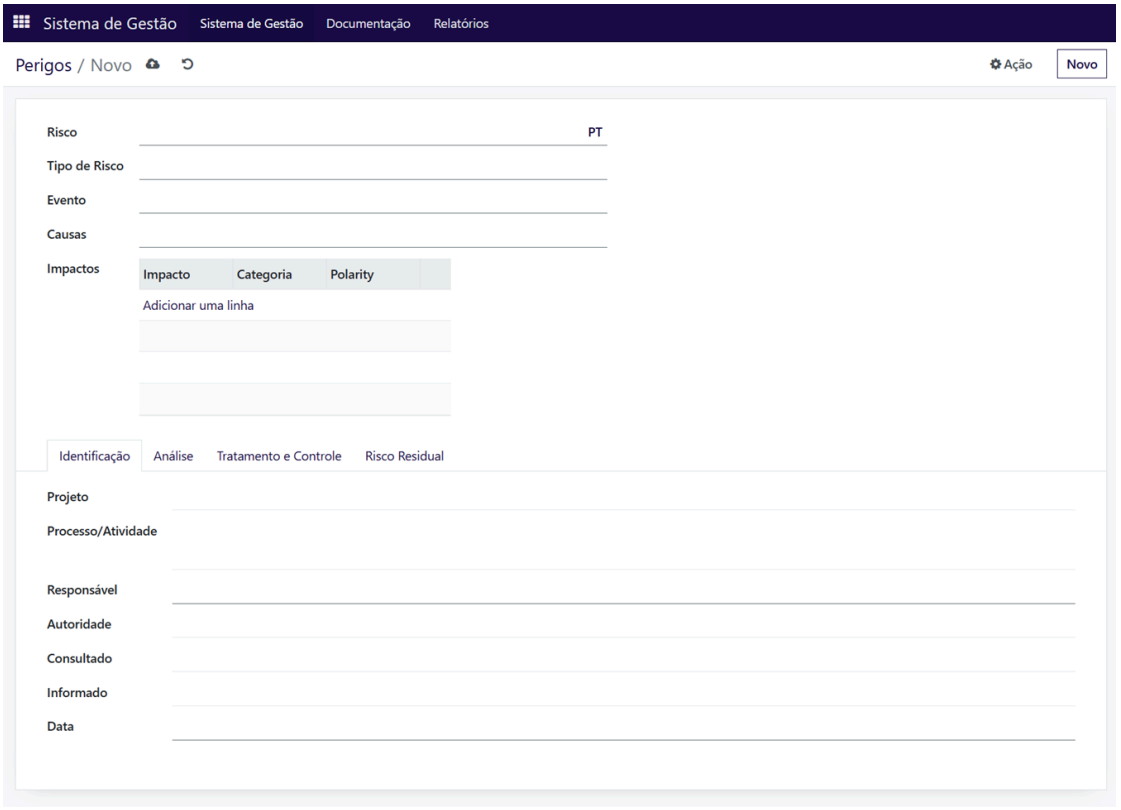
O passo a passo levará até a página inicial do módulo de Riscos, nesse ambiente estarão informações resumidas dos riscos que se relacionam de alguma forma com o indivíduo. O mesmo local é utilizado para iniciar a criação de um novo risco.

Figura 04 – Painel Inicial Módulo de Riscos



Por fim, o usuário é direcionado para o *card* com os campos necessários para inserção de informações que compõem o processo de gestão de riscos.

Figura 05 – *Card* para Inserção do Risco



5.5 Processo

A gestão de riscos do NEES segue um processo estruturado e cíclico que acontece em cinco etapas, conforme apresentadas:

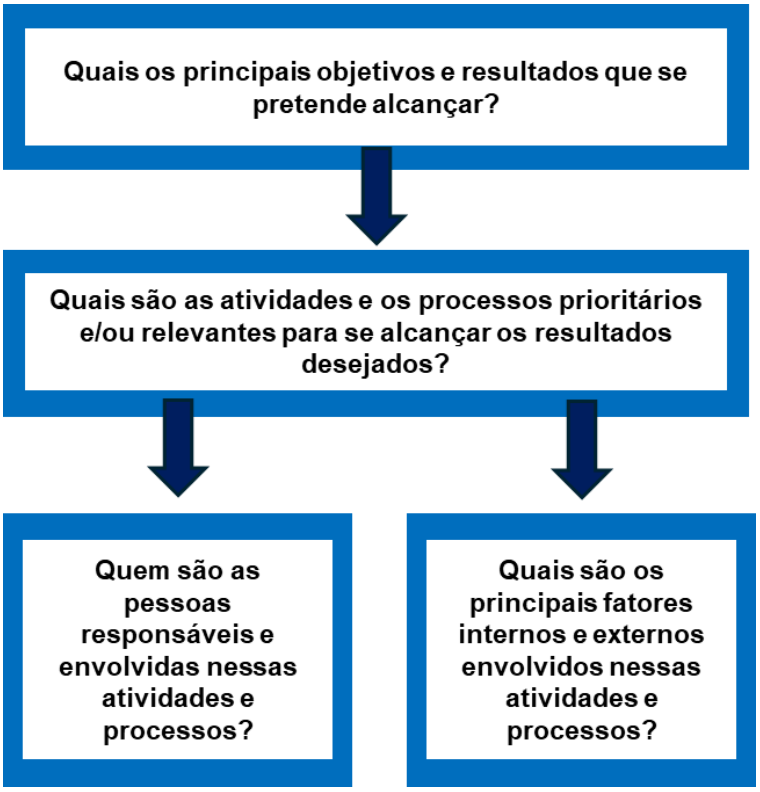
5.5.1 Identificação dos Riscos

5.5.1.1 Evento, Causas e Impactos

O processo de identificação dos riscos consiste em encontrar, reconhecer e descrever oportunidades ou ameaças que possam ajudar ou impedir que uma organização alcance seus objetivos. É uma atividade cíclica e constante que tem como objetivo realizar um levantamento dos eventos de riscos, determinando suas classificações, causas e potenciais impactos.

Um mapeamento do escopo e contexto da atividade, projeto ou processo é fundamental para suportar a identificação dos riscos. No contexto do NEES, essa é uma etapa norteadora, principalmente para atividades que estão passando pelo processo de gestão de riscos pela primeira vez.

Figura 06 – Mapeamento do Escopo e Contexto



Tendo como base o mapeamento realizado, a primeira etapa deve ser o levantamento dos eventos de riscos, que são incidentes, ocorrências ou mudanças que podem impactar ou alterar os fatores mapeados e, portanto, as chances de alcançar os objetivos. Após a identificação dos eventos, o foco deve ser compreender a causa do risco, ou seja, o motivo pelo qual o evento pode acontecer. O próximo passo deve ser a descrição dos impactos causados, caso o evento se concretize. A ocorrência de um evento pode gerar impactos diversos, inclusive com categorias e polaridades distintas, ou seja, o mesmo risco pode gerar uma oportunidade e uma ameaça que impactam âmbitos distintos do NEES.

5.5.1.2 Classificação dos Riscos

Os eventos de risco podem ser classificados por tipologias para organizar as informações e nortear a tomada de decisão. O NEES determinou a sua tipologia da seguinte forma:

Quadro 01 – Tipologia de Classificação de Riscos

CATEGORIAS DE RISCO		
CLASSES	**SUB-CLASSES**	**DESCRIÇÃO**
ADMINISTRATIVOS	**Riscos Estratégicos**	Riscos de longo prazo ou riscos de oportunidade relacionados aos objetivos estratégicos do NEES e às estratégias adotadas para alcançá-los.
	Riscos Operacionais	Riscos associados a processos inadequados, ineficientes ou inexistentes, problemas operacionais, questões de recursos humanos e infraestrutura que podem comprometer a eficiência e a continuidade das atividades do NEES.
	Riscos Técnicos	Riscos associados a problemas e falhas nos sistemas, serviços e infraestruturas de TIC, desenvolvimento tecnológico, compatibilidade de sistemas e obsolescência tecnológica.
	Riscos de Segurança da Informação	Riscos que podem ameaçar a confidencialidade, integridade e disponibilidade dos dados e sistemas da organização. Podem ser decorrentes de ataques cibernéticos, falhas humanas, vulnerabilidades técnicas, acessos não autorizados, configurações de redes, problemas em aplicativos, softwares que podem causar falhas futuras, etc. Os riscos de segurança da informação no NEES devem ser definidos respeitando os requisitos do Anexo A da ISO 27001 e os objetivos da organização.
	Riscos Orçamentários e Financeiros	Riscos que possam comprometer a capacidade do NEES em contar com recursos orçamentários e financeiros necessários à realização de suas atividades e projetos, incluindo eventos como atrasos no cronograma de licitações e cortes de financiamento.
	Riscos de Reputação	Riscos que possam comprometer a reputação e a confiança da sociedade e de outros stakeholders em relação à capacidade do NEES em cumprir sua missão institucional.
	Riscos Legais	Riscos de questões relacionadas à conformidade com leis, regulamentos e normas aplicáveis à organização. Podem incluir descumprimento de contratos, não observância de legislações setoriais e problemas regulatórios.
POLÍTICOS	**Riscos Políticos**	Riscos de intervenção política ou aqueles derivados de leis, decretos, portarias, resoluções etc., oriundos do Governo Federal, Estadual e Municipal, os quais podem ameaçar os interesses e objetivos da organização.
INOVAÇÃO	**Riscos de Inovação**	Riscos referente às incertezas decorrentes, normalmente, da introdução (oferta) de novos produtos ou serviços e da sua aceitação (demanda). Abordam as incertezas associadas à adoção de novas tecnologias, metodologias e modelos de negócio.

5.5.2 Análise e Avaliação dos Riscos

A análise de riscos é a fase em que os riscos identificados são examinados em profundidade para determinar a probabilidade de um evento de risco ocorrer e o seu possível impacto. A relação entre probabilidade e impacto serve como um guia para definir o grau de ameaça de cada risco.
O NEES adotou escalas compostas por 5 níveis tanto para a avaliação da probabilidade quanto do impacto.

Quadro 02 – Escala de Probabilidades

PESO	PROBABILIDADE	DESCRIÇÃO
1	Muito Baixa	Improvável, não é esperado que ocorra.
2	Baixa	Rara, pode ocorrer, mas é pouco provável.
3	Média	Possível, existe uma chance razoável de ocorrer.
4	Alta	Provável, altamente possível de ocorrer.
5	Muito Alta	Praticamente certo, as circunstâncias indicam claramente a possibilidade de ocorrer.

Quadro 03 – Escala de Impactos

PESO	IMPACTO	DESCRIÇÃO
1	Muito Baixo	Mínimo impacto, sem consequências relevantes.
2	Baixo	Pequeno impacto, com efeito localizado e recuperação rápida.
3	Médio	Impacto médio, afetando operações e exigindo correções.
4	Alto	Impacto significativo, afetando de forma ampla e com reversão difícil.
5	Muito Alto	Impacto extremo, podendo comprometer a viabilidade.

Após a definição da classificação da probabilidade e do impacto, a relação entre as duas dimensões posicionará o risco dentro da Matriz de Risco adotada pelo NEES. A ferramenta é importante para identificar quais são os riscos que devem receber mais atenção.

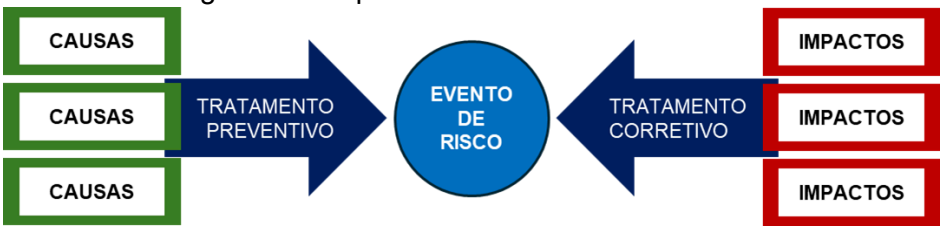
Figura 07 – Matriz de Risco (Impacto x Probabilidade)

		IMPACTO				
		1	2	3	4	5
PROBABILIDADE	1	Aceitável	Aceitável	Baixo	Moderado	Alto
	2	Aceitável	Baixo	Moderado	Alto	Alto
	3	Baixo	Moderado	Moderado	Alto	Intolerável
	4	Baixo	Moderado	Alto	Intolerável	Intolerável
	5	Moderado	Moderado	Alto	Intolerável	Intolerável

5.5.3 Tratamento dos Riscos

O planejamento de resposta aos riscos identificados e priorizados consiste no planejamento e na execução de ações para modificar o risco. As opções de tratamento dos riscos podem ter características e objetivos distintos, sendo assim podem ser preventivas ou corretivas. As ações preventivas têm como objetivo evitar que o risco se materialize, reduzindo sua probabilidade ou eliminando as causas antecipadamente, protegendo o NEES da exposição a esses riscos. Já as ações corretivas acontecem após a ocorrência do risco, atuando sobre os impactos buscando minimizar os danos.

Figura 08 – Tipos de Tratamentos dos Riscos



Convém que a seleção das estratégias de tratamento de risco seja realizada por meio de análise criteriosa balanceando os benefícios potenciais em contrapartida aos custos, esforços ou desvantagens da implementação. As estratégias possíveis adotadas pelo NEES são: evitar, mitigar, aceitar e transferir.

Quadro 04 – Estratégias de Tratamento dos Riscos

ESTRATÉGIA	DESCRIÇÃO
Evitar	Descontinuar as atividades que geram o risco. Ex. Suspender um produto ou uma atividade. Ex. suspender um produto ou uma atividade.
Mitigar	Adotar medidas para reduzir a probabilidade e/ou impacto dos riscos. Ex. implementa firewalls, autenticação multifator e monitoramento contínuo
Aceitar	Conviver com o evento de risco mantendo práticas e procedimentos existentes. Ex. aceitar que alguns clientes terão problemas técnicos
Transferir	Transferir ou compartilhar parte do risco, reduzindo a probabilidade e/ou impacto. Ex. seguro ou terceirização da atividade.

O plano deve trazer medidas para tratamento dos riscos que venham a se concretizar. Para isso, é necessário considerar exatamente qual tratamento o risco receberá, a medida de controle que será adotada, o prazo em que deve ser implementada, os responsáveis por isso, entre outras definições.

Para suportar o tratamento do risco é adotada a metodologia do Ciclo PDCA que permite a melhoria contínua da gestão de riscos. As ações delimitadas para tratamento e controle dos riscos são acompanhadas em seus diferentes estágios: Não iniciada, Concepção, Implementação e Executado. É um processo cíclico e dinâmico, o objetivo é garantir que as ações não sejam um esforço pontual, mas adotadas em um processo de evolução.

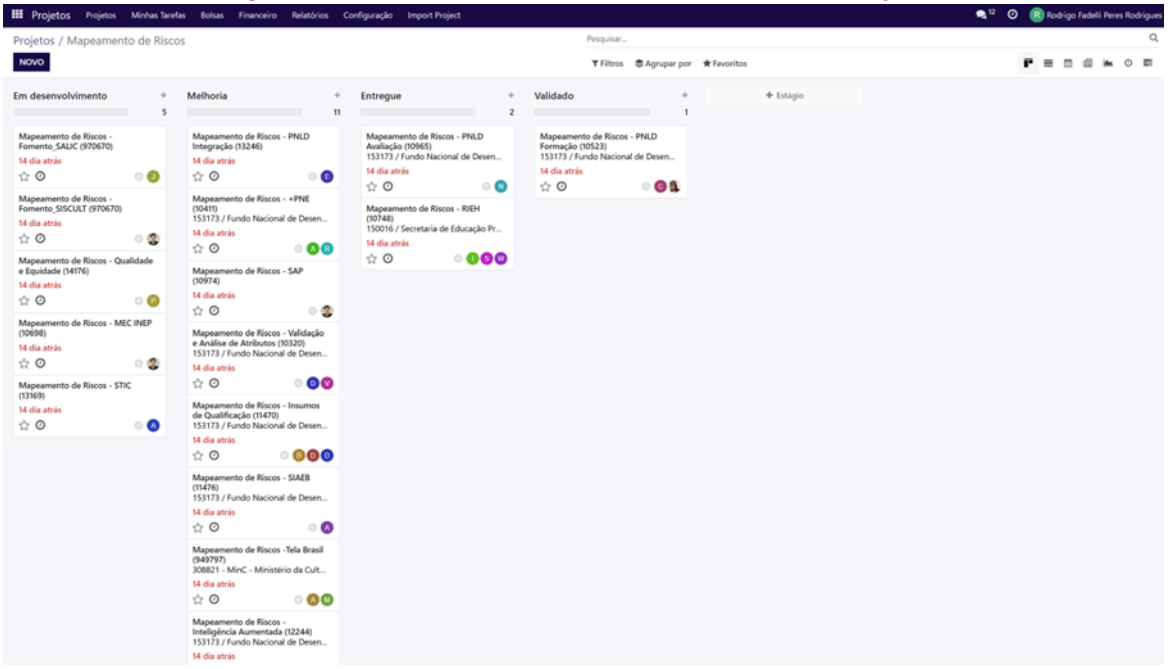
5.5.4 Monitoramento e Comunicação

O monitoramento e a Comunicação são etapas realizadas continuamente e com periodicidade para garantir que as estratégias de tratamento de riscos sejam eficazes e que novas ameaças sejam identificadas. Também contribui substancialmente para neutralizar ameaças aos objetivos institucionais e possibilita aproveitar as oportunidades. No âmbito do NEES, é determinado que os projetos e atividades essenciais sejam revisitados com periodicidade mensal.

No NEES as etapas de monitoramento e comunicação são apoiadas pelo Sistema Integra, que permite a visualização de todos os riscos e suas informações respectivas. A ferramenta possibilita que boas práticas de gestão de riscos sejam implementadas como regras sistêmicas e contribuam com a execução do monitoramento.

Para o monitoramento dos riscos no nível dos projetos do NEES é utilizado, adicionalmente, um painel no Sistema Integra para organizar o ciclo mensal adotado.

Figura 09 – Painel de Monitoramento Ciclo dos Projetos



- o responsável pelo registro do risco no sistema recebe aviso quando o prazo de alguma medida de tratamento e controle está próximo do fim.
- o responsável pela medida de tratamento e controle no sistema recebe aviso quando o prazo está próximo do fim.
- outras partes interessadas, caso existam, recebem aviso quando ocorre a criação de algum risco, alguma mudança de status das medidas de tratamento e controle ou prazo de alguma está próximo do fim.

A definição das partes interessadas é realizada por meio de processo que visa assegurar a participação das partes interessadas. Utilizando matriz estruturada considerando o papel do indivíduo, classificação e grau de ameaça do risco são determinados atores diferentes como partes interessadas de forma automática por meio de regra no Sistema Integra. Será habilitado ao responsável pela criação do risco inclua indivíduos nos campos de Classificação quando não houver determinação sistêmica.

Quadro 05 – Matriz de Partes Interessadas (Governança)

CLASSIFICAÇÃO	GRAU DE AMEAÇA				
	ACEITÁVEL	BAIXO	MODERADO	ALTO	INTOLERÁVEL
Riscos Estratégicos	-	-	Indicado Ger. Governança	Ger. Governança	Ger. Governança
Riscos Operacionais	-	-	Indicado Ger. Administrativo	Indicado Ger. Administrativo	Ger. Administrativo
Riscos Técnicos	-	Indicado Ger. Infraestrutura	Ger. Infraestrutura	Ger. Infraestrutura	Ger. Infraestrutura
Riscos de Segurança da Informação	-	Indicado Ger. Qualidade	Ger. Qualidade	Ger. Qualidade	Ger. Qualidade
Riscos Orçamentários e Financeiros	-	-	Indicado Ger. Administrativo	Ger. Administrativo	Ger. Administrativo
Riscos de Reputação	-	-	Indicado Ger. Administrativo	Indicado Ger. Administrativo	Ger. Administrativo
Riscos Legais	-	-	Indicado Ger. Administrativo	Ger. Administrativo	Ger. Administrativo
Riscos Políticos	-	-	Indicado Ger. Governança	Indicado Ger. Governança	Ger. Governança
Riscos de Inovação	-	-	Indicado Ger. Governança	Indicado Ger. Governança	Ger. Governança

Quadro 06 – Matriz de Partes Interessadas (Projetos)

CLASSIFICAÇÃO	GRAU DE AMEAÇA				
	ACEITÁVEL	BAIXO	MODERADO	ALTO	INTOLERÁVEL
Riscos Estratégicos	-	-	Gerente de Projetos	Vice-Coordenador	Coordenador
Riscos Operacionais	-	-	Gerente de Projetos	Gerente de Projetos	Coordenador
Riscos Técnicos	-	Gerente de Projetos	Vice-Coordenador	Coordenador	Coordenador
Riscos de Segurança da Informação	-	Gerente de Projetos	Vice-Coordenador	Coordenador	Coordenador
Riscos Orçamentários e Financeiros	-	-	Vice-Coordenador	Vice-Coordenador	Coordenador
Riscos de Reputação	-	-	Gerente de Projetos	Vice-Coordenador	Coordenador
Riscos Legais	-	Informado	Vice-Coordenador	Coordenador	Coordenador
Riscos Políticos	-	-	Gerente de Projetos	Vice-Coordenador	Coordenador
Riscos de Inovação	-	-	Gerente de Projetos	Gerente de Projetos	Coordenador

Para os riscos criados abordando a estrutura de governança serão acionados apenas os indivíduos do quadro de Governança, já os riscos envolvendo os projetos acionaram ambos.

6. REGISTROS

O registro relacionado com este procedimento é realizado no Sistema INTEGRA\ Módulo Riscos.

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO27001/Procedimentos.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	04/11/2024	Criação do documento.	Rodrigo Fadelli
02	10/03/2025	Padronização do procedimento para atender ao SGSI do NEES	Rodrigo Fadelli

Elaborador: Rodrigo Fadelli Peres Rodrigues, False, em 2025-05-14 10:16
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-14 10:29
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-14 13:55