NOTA TÉCNICA Nº 06/2025 – SECEX/TCE/RN

Comunica aos jurisdicionados, responsáveis e demais interessados sobre diretrizes para o gerenciamento de riscos corporativos e implementação de respostas adequadas aos eventos com potencial para influenciar negativamente a consecução dos objetivos estratégicos da organização, apresenta o SIAI – GR e dá outras providências.

O SECRETÁRIO DE CONTROLE EXTERNO, no uso das atribuições estabelecidas pelo artigo 163, inciso XII, do Regimento Interno do Tribunal de Contas do Estado do Rio Grande do Norte, aprovado pela Resolução nº 009, de 19 de abril de 2012, combinado com o artigo 3º, inciso XIV, da Resolução nº 042, de 18 de dezembro de 2024, e

CONSIDERANDO o disposto no texto da Resolução nº 008/2025 – TCE, de 28 de maio de 2025, que instituiu o Sistema Integrado de Auditoria Informatizada na área de Gestão de Riscos (SIAI – GR);

CONSIDERANDO que constitui um dos objetivos estratégicos do Tribunal de Contas do Estado, sob a perspectiva de resultados institucionais, contribuir para a melhoria do desempenho e transparência da gestão pública, através de ações de orientação sobre a prevenção de riscos capazes de comprometer a execução de programas governamentais e a implementação de políticas públicas;

CONSIDERANDO que a indução de boas práticas de gestão e a promoção da efetividade são compromissos inalienáveis para o fortalecimento institucional dos tribunais de contas;

CONSIDERANDO que o Tribunal de Contas do Estado, no exercício de sua função orientadora, pode expedir, por intermédio da sua Secretaria de Controle Externo, notas técnicas sobre conteúdo atinente ao controle externo,

FAZ SABER, PARA FINS DE AVALIAÇÃO DE CONFORMIDADE, QUE:

1. O Sistema Integrado de Auditoria Informatizada na área de Gestão de Riscos (SIAI – GR), instituído pela Resolução nº 008/2025 – TCE, de 28 de maio de 2025, constitui ferramenta eletrônica voltada ao apoio às rotinas de gerenciamento de riscos, disponível a todos os órgãos e unidades componentes do sistema de controle interno, jurisdicionados ao Tribunal de Contas do Estado, de acordo com os termos da Resolução nº 018/2022 – TCE, de 14 de julho de 2022.

2. As funcionalidades do SIAI – GR e as orientações gerais consignadas no Manual do Usuário, constante no Anexo Único a esta Nota Técnica, são acessíveis via Portal do Controle Interno, gerido pelo TCE, a partir do endereço https://pci.tce.rn.gov.br, ou através do *banner* disponível no Portal do TCE (https://www.tce.rn.gov.br), devendo-se observar, para a utilização do sistema, as regras para fornecimento de credenciais aos usuários designados pelos gestores das entidades e órgãos jurisdicionados, em observância ao regulamento pertinente à operacionalização do Portal do Gestor.

3. Os dados cadastrados na interface do SIAI – GR não substituem os papéis de trabalho próprios das atividades de gerenciamento de riscos e implementação de controles. A proposta do aplicativo é auxiliar na organização das informações pertinentes, sobretudo quanto ao cálculo dos riscos tratados.

4. A adequada utilização do SIAI – GR, de forma a extrair o máximo proveito das funcionalidades apresentadas por esta ferramenta de auxílio à gestão, pressupõe uma completa revisão dos processos de trabalho da organização, de forma a prepará-la para uma abordagem do controle a partir de uma política de gerenciamento de riscos corporativos e aplicação de controles eficientes, em um ciclo permanente de planejamento, execução, avaliação e, novamente, planejamento.

5. De acordo com o texto da NBASP 4000/131, os dados cadastrados na interface do SIAI – GR são aptos a fornecer indicadores sobre o nível de confiança do controle interno, de forma a subsidiar o planejamento de fiscalizações para aprofundar, quando necessário, as avaliações de conformidade, pela aplicação de procedimentos

substantivos complementares, com o fim de apurar o grau de desvio das informações prestadas pelos jurisdicionados, analisar os dados levantados, identificar evidências de eventuais achados ou mesmo testar o desenho, implementação e efetividade operacional dos controles, sujeitando os gestores omissos à aplicação da multa prevista no artigo 107, inciso II, alínea "d", da Lei Complementar Estadual nº 464, de 05 de janeiro de 2012, e no artigo 7º, § 3º, da Resolução nº 008/2025 – TCE, de 28 de maio de 2025.

Secretaria de Controle Externo do Tribunal de Contas do Estado do Rio Grande do Norte, em Natal, 7 de agosto de 2025.

MARCELO BERGANTIN OLIVEROS:03845708441

Assinado digitalmente por MARCELO BERGANTIN OLIVEROS:03845708441
ND: C=BR, O=ICP-Brasil, OU=Presencial, OU=08417107000141, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=MARCELO BERGANTIN OLIVEIROS, CN=MARCELO BERGANTIN OLIVEROS:03845708441
Razão: Eu sou o autor deste documento
Localização:
Data: 2025.08.07 11:39:27-03'00'
Foxit PDF Reader Versão: 2025.1.0

Marcelo Bergantin Oliveros

Secretário de Controle Externo

Mat.: 9.869-8

ANEXO ÚNICO

Manual para Operação do SIAI Gestão de Riscos (SIAI-GR)

TRIBUNAL DE CONTAS DO ESTADO
RIO GRANDE DO NORTE

SECEX
SECRETARIA DE CONTROLE EXTERNO

SIAI Gestão de Riscos (SIAI – GR) Manual do Usuário

Natal/RN
2025

HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Realização
30/05/2025	1.0	Elaboração do manual	Coordenadoria de Normas, Métodos e Qualidade para o Controle Externo

TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE
SECRETARIA DE CONTROLE EXTERNO
COORDENADORIA DE NORMAS, MÉTODOS E QUALIDADE PARA O CONTROLE EXTERNO

Manual para Operação do SIAI Gestão de Riscos
https://www.tce.rn.gov.br/#gsc.tab=0
https://pci.tce.rn.gov.br/#/

Avenida Presidente Getúlio Vargas, 690, Petrópolis.
CEP: 59012-360 – Natal/RN.
Email: cnmq@tce.rn.gov.br
Fone: (84) 3642-7332

Ficha Catalográfica

T822m

TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE (TCE-RN). Coordenadoria de Normas, Métodos e Qualidade para o Controle Externo.

Manual para Operação do SIAI Gestão de Riscos (SIAI-GR) / Tribunal de Contas do Estado do Rio Grande do Norte. – Natal/RN: TCE-RN, 2025.

55 p. il.:

1. Manual do usuário. 2. Operação do SIAI Gestão de Riscos. 3. Tribunal de Contas.

I. Título.

CDU 351.94 (021)

Michele Rodrigues Dias
Bibliotecária Documentalista
CRB/15 nº 780

COMPOSIÇÃO DO TCE – BIÊNIO 2025-2026

Presidente

Carlos Thompson Costa Fernandes

Vice-Presidente

Antônio Ed Souza Santana

Corregedor

Antônio Gilberto de Oliveira Jales

Diretor da Escola de Contas

George Montenegro Soares

Presidente da Primeira Câmara

Francisco Potiguar Cavalcanti Júnior

Presidente da Segunda Câmara

Renato Costa Dias

Ouvidor

Paulo Roberto Chaves Alves

Conselheiros Substitutos

Ana Paula de Oliveira Gomes

Marco Antônio de Moraes Rêgo Montenegro

Procurador-Geral do Ministério Público de Contas

Luciano Silva Costa Ramos

LISTA DE DIAGRAMAS, FIGURAS E FLUXOGRAMAS

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	**Associação Brasileira de Normas Técnicas**
AECI	**Assessoria Especial de Controles Internos do Ministério Planejamento, Desenvolvimento e Gestão**
COSO	***Committee of Sponsoring Organizations of the Treadway Commission***
DECRI	**Departamento de Compliance e Riscos da Empresa Brasileira de Correios e Telégrafos**
ENAP	**Escola Nacional de Administração Pública**
ERM	***Enterprise Risks Management***
IIA	***Institute of Internal Auditors***
IRB	**Instituto Rui Barbosa**
ISSAI	***International Standards of Supreme Audit Institutions***
NBASP	**Normas Brasileiras de Auditoria do Setor Público**
SIAI – GR	**Sistema Integrado de Auditoria Informatizada na área de Gestão de Riscos**
SWOT	**Strengths, Weaknesses, Opportunities and Threats**
TCE	**Tribunal de Contas do Estado do Rio Grande do Norte**
TCU	**Tribunal de Contas da União**

SUMÁRIO

1 INTRODUÇÃO

Promover, junto aos órgãos, entidades, unidades orçamentárias e fundos jurisdicionados a devida elucidação a respeito da missão do Tribunal de Contas do Estado, no âmbito do sistema de freios e contrapesos, de forma que a obtenção de informações aconteça espontaneamente e com níveis fidedignos de integridade e *compliance*. Este procedimento constitui diretriz fundamental e pré-requisito para uma atuação adequada aos padrões internacionais de auditoria, orientando a comunicação efetiva do órgão auxiliar do controle externo com as partes responsáveis e interessadas *(stakeholders)*, fomentando discussões em uma atmosfera de respeito e compreensão mútuos e contribuindo para o debate sobre o aperfeiçoamento da Administração Pública, por meio da proposição de soluções efetivamente benéficas (NBASP 12/40)[1].

Manter, junto às entidades sob sua jurisdição, elevados níveis de credibilidade, confiança e respeito, ancorados por objetividade, neutralidade, independência e imparcialidade, exige diligência e demanda a responsabilidade de apresentar, de maneira eficaz, a importância do Tribunal de Contas do Estado para os cidadãos, para o Legislativo e para outros órgãos e entidades governamentais.

Um caminho para demonstrar esta relevância é responder, apropriadamente, às expectativas das partes interessadas e manter uma boa comunicação no sentido

[1] As diretrizes e os princípios gerais estabelecidos pelas Normas Internacionais das Entidades Fiscalizadoras Superiores *(ISSAI)*, aprovadas pela Organização Internacional das Entidades Fiscalizadoras Superiores *(INTOSAI)*, foram adaptados e incorporados aos marcos normativos brasileiros através das Normas Brasileiras de Auditoria do Setor Público (NBASP), compiladas pelo Instituto Rui Barbosa (IRB) e adotadas pelos tribunais de contas brasileiros, mais especificamente no que reporta aos aspectos estruturais, de organização e planejamento, independência, transparência, *accountability*, ética e controle de qualidade, bem como no que se refere à escolha e utilização de métodos de avaliação de conformidade do objeto da auditoria, em suas dimensões qualitativa e quantitativa, às características verificadas em trabalhos de asseguração, ao entendimento sobre o ambiente de controle e gestão de riscos.

Em seu Nível 1, que discorre sobre os princípios basilares e pré-requisitos para o funcionamento dos tribunais de contas brasileiros, a NBASP 12 trata do valor agregado e dos benefícios gerados pela atuação dos tribunais de contas, no sentido de fazer a diferença na vida dos cidadãos.

de demonstrar que as ações de controle realizadas proporcionam o aperfeiçoamento da Administração Pública e agregam valor à gestão.

Os princípios e requisitos em torno da expectativa fundamental do Tribunal de Contas do Estado, no sentido de demonstrar o seu valor para a sociedade e de fazer a diferença na vida dos cidadãos, encontram-se divididos entre os seguintes objetivos: *(i)* fortalecer a *accountability*, a transparência e a integridade dos órgãos e entidades governamentais; *(ii)* demonstrar, continuamente, relevância para os cidadãos, para o Legislativo e para outras partes interessadas; e *(iii)* ser uma organização modelo, que lidera pelo exemplo.

Estes princípios e requisitos estão bem assentados na sua identidade institucional, a qual preconiza, para o exercício do controle externo, a orientação em igualdade de relevância com a fiscalização, assim como o bem maior da sociedade, visando o seu reconhecimento como referência em matéria de controle externo e como organização indispensável ao fortalecimento da cidadania.

A ampliação das funcionalidades aplicadas ao Sistema Integrado de Auditoria Informatizada, determinada pela Resolução nº 008/2025 – TCE, de 28 de maio de 2025, alcança a área da gestão de riscos, como ferramenta eletrônica de apoio às rotinas de trabalho das entidades e órgãos jurisdicionados (SIAI – GR), e foi conduzida nesta esteira do diálogo em alto nível, confiança e respeito mútuo entre as instâncias de controle (interna e externa), com ênfase na agregação de valor, sobretudo quanto aos seguintes objetivos:

1- Aprimorar o nível de consciência situacional sobre o ambiente de controle do órgão ou entidade, incentivando a consolidação da sua identidade institucional, a fixação dos seus objetivos estratégicos, a análise de contexto da organização e o planejamento;

2- Facilitar a identificação dos riscos, mediante o reconhecimento, descrição e registro dos eventos com potencial para influenciar, de forma negativa, a consecução dos objetivos estratégicos, com a caracterização de suas prováveis causas e consequências;

3- Definir o percentual de risco aceitável ou que não demandará mitigação ou transferência, com base em avaliação de custo-benefício (nível de apetite a risco);

4- Mensurar a probabilidade de materialização do evento, tendo em consideração as situações que podem ensejá-lo (causas);

5- Mensurar o impacto (potencial de repercussão ou consequências) do evento sobre os objetivos estratégicos, em caso de materialização;

6- Mensurar a interação entre probabilidade e impacto (intensidade do risco);

7- Definir a espécie de resposta a ser oferecida e analisar o seu nível de adequação em relação aos controles existentes, em termos de configuração e aplicação efetiva;

8- Mensurar o percentual de risco remanescente, após confrontar o risco identificado e avaliado (risco inerente) com a eficácia das atividades de controle já existentes, o que resultará na apuração do risco residual, o qual, eventualmente, demandará novas atividades de controle;

9- Estabelecer os protocolos para revisão dos processos de trabalho da organização, com a finalidade de obter segurança razoável quanto ao alcance dos objetivos estratégicos;

10- Manter um fluxo adequado de informações entre os jurisdicionados e o Tribunal de Contas; e

11- Fomentar, entre os jurisdicionados, as autoavaliações, que servirão como ponto de partida para observações independentes, no sentido de confirmarem o que foi autoavaliado, por meio de testes de desenho, implementação e efetividade operacional do controle interno, exatidão e validade das informações fornecidas.

O modelo seguido por este aplicativo voltado à gestão de riscos e aperfeiçoamento das atividades de controle é claramente inspirado no *Framework COSO ERM*, que constitui o padrão adotado por força da Resolução nº 018/2022 – TCE, de 14 de julho de 2022, para operacionalização do controle interno no âmbito das unidades jurisdicionadas, tendo como referência a estrutura de componentes integrados ao sistema de controle interno, organizada pelo *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*.

A concepção de estrutura de componentes integrados teve suas origens em 1985, nos Estados Unidos, através da iniciativa de entidades do setor privado preocupadas em desenvolver uma doutrina de aplicação comum a todos os pressupostos relacionados à visão do controle interno como instrumento de

gerenciamento de riscos e gestão corporativa, tendo sido amplamente adotada, em nível mundial, inclusive por entidades fiscalizadoras do setor público, como a *INTOSAI*, por introduzir uma forma de comparar a excelência na implementação (ambiente de controle), validação (avaliação de riscos, auditoria, divulgação de resultados e monitoramento) e definição dos papéis e responsabilidades dos gestores, neste cenário.

A estrutura do *COSO ERM (framework)* tem como base uma concepção tridimensional da relação entre a forma de organização da entidade e os oito componentes integrados ao seu arranjo de controle, ilustrada na figura de um cubo, tendo em conta quatro categorias de objetivos:

- Estratégica (cumprimento da missão e dos objetivos institucionais);
- Operacional (eficácia, economicidade, eficiência e efetividade das operações);
- Comunicação (transparência, busca e acesso às informações pertinentes, sistemas e fluxos de comunicação interno e externo); e
- Conformidade (observância às leis e regulamentos).

Definições relacionadas aos oito componentes integrados à estrutura de controle:

- Ambiente de controle (estrutura organizacional, normas de conduta, valores éticos, análise de contexto, planejamento estratégico, delegações de autoridade e competência, atribuição de responsabilidades, desenvolvimento de recursos humanos e tecnologia);
- Fixação de objetivos estratégicos claros e mensuráveis (expressos numericamente com base em um referencial), vinculados à definição da identidade institucional, identificação dos macroprocessos e regulamentação dos processos necessários ao cumprimento da missão atribuída à organização;
- Identificação de eventos com potencial para influenciar (positivamente ou negativamente) a consecução dos objetivos estratégicos;
- Avaliação de riscos (mensuração dos eventos potencialmente negativos, em termos de probabilidade e impacto);
- Definição das respostas mais adequadas para aceitar, mitigar, transferir/compartilhar ou evitar os riscos identificados;

- Atividades de controle (diretrizes e procedimentos internos aplicados com a finalidade de obter segurança razoável quanto ao alcance dos objetivos estratégicos);
- Informação e comunicação (transparência na divulgação dos resultados da gestão, busca por informações relevantes, através de meios eficazes, elaboração de relatórios íntegros, ampliação de canais para permitir um fluxo seguro de dados por todos os níveis da organização, além da troca de informações com o ambiente externo); e
- Atividades de monitoramento (manutenção de programas continuados para avaliação própria e/ou por entidade independente, sobre a eficácia dos procedimentos de controle empregados, para verificar o cumprimento de objetivos e metas e comunicar eventuais deficiências à estrutura de governança).

A terceira dimensão ou terceira face do cubo é composta pelo organograma institucional.

Em sintonia com esta abordagem, os componentes integrados ao sistema de controle interno são elementos essenciais para que os objetivos estratégicos sejam atingidos, enquanto os riscos constituem situações prováveis e potencialmente danosas a estes objetivos.

A feição ou organização das atividades ou divisões da entidade determinará como a doutrina será adaptada a cada realidade (*COSO*, 2013), a fim de que a estrutura de componentes integrados seja aplicada e contribua para a realização dos objetivos, independentemente da sua conformação (grande, médio ou pequeno porte, com ou sem fins lucrativos, de caráter privado ou governamental), podendo variar quanto ao aprofundamento das formalidades e complexidades, mantendo, entretanto, o foco na efetividade, sem perder de vista a preservação de níveis razoáveis de segurança.

Diagrama 1 – O cubo do *Framework COSO*

Fonte: Escola Nacional de Administração Pública (ENAP). Módulo 2, 2018, p. 6 (reprodução do *COSO ERM*, 2004).

Outro referencial importante para a utilização adequada do SIAI – GR, e que também foi recepcionado pela Resolução nº 018/2022 – TCE, de 14 de julho de 2022, é o sistema das três linhas de defesa (ENAP, 2018). Esse modelo ficou conhecido e foi amplamente difundido a partir da Declaração de Posicionamento emitida pelo *Institute of Internal Auditors (IIA)*, e propõe aprimorar a comunicação entre as etapas de identificação de riscos e aplicação dos controles, com ênfase no esclarecimento dos papéis e na divisão de responsabilidades essenciais (segregação de funções).

Assim como a estrutura de componentes integrados, o sistema das três linhas de defesa também é aplicável a qualquer organização, não importando o seu tamanho ou complexidade, a partir do seguinte desenho:

- Uma primeira linha de defesa, preenchida pelos chamados proprietários dos riscos, que são os gestores responsáveis por identificar, avaliar e apresentar respostas adequadas aos riscos, ou seja, os gerentes que implementam os procedimentos de resposta aos riscos e supervisionam a sua execução;

- Uma segunda linha de defesa, composta pela divisão responsável por monitorar o gerenciamento dos riscos e proporcionar suporte aos proprietários dos riscos, na tomada de decisões; e
- Uma terceira linha de defesa, formada pela auditoria interna, que avalia a eficácia das duas primeiras linhas de defesa, na gestão de riscos e aplicação de controles.

A imagem abaixo apresenta a esquematização deste modelo:

Fluxograma 1 – Esquema das três linhas de defesa

Fonte: Escola Nacional de Administração Pública (ENAP). Módulo 1, 2018, p.12 (adaptado de *Guidance on the 8th EU Company Law Directive*, da *ECIIA/FERMA*, artigo 41).

2 Controle interno e gestão de riscos: governança corporativa para um modelo de Estado fornecedor de serviços

A apropriação de todo este delineamento teórico é fundamental para obter o máximo aproveitamento sobre as funcionalidades disponíveis no SIAI – GR, que poderá converter-se em ferramenta de grande utilidade para a implementação de uma cultura de qualidade na prestação dos serviços, a partir de níveis de asseguração adequados, notadamente em relação às organizações menos complexas, isto porque as demandas estabelecidas por uma sociedade cada vez mais consciente da importância da participação popular no governo, potencializadas por instrumentos de comunicação de massa cada vez mais acessíveis, tornaram obsoletos os procedimentos burocráticos de caráter finalístico, que contribuíram para reduzir a eficiência esperada das organizações públicas.

A concepção de um Estado fornecedor de serviços exige um nível de governança corporativa capaz de conciliar uma identidade institucional clara, a conformidade dos procedimentos, a eficiência nos resultados e um fluxo adequado de informações, de forma que essas instâncias trabalhem em conjunto para permitir que a organização faça escolhas mais assertivas sobre o nível de risco que está disposta a assumir, auxiliando na aplicação de mecanismos de controle necessários para alcançar efetivamente os objetivos estratégicos.

Se os objetivos estratégicos forem mal estabelecidos pela organização, é improvável que qualquer programa ou aplicativo seja capaz de agregar valor aos seus processos de trabalho. Por isso é fundamental para o gestor, antes de definir qualquer plano de ação para a implementação dos controles propostos, cumprir uma sequência de tarefas fundamentais para que as atividades de controle forneçam segurança razoável quanto ao alcance dos objetivos estratégicos.

Em primeiro lugar, é necessário que a organização tenha uma noção sobre a sua identidade institucional (missão, visão e valores) claramente estabelecida, o que possibilitará a fixação de objetivos estratégicos relacionados aos macroprocessos pertinentes.

Por sua vez, a fixação de objetivos estratégicos, que é função de uma identidade institucional bem definida, viabilizará, com a projeção de resultados mensuráveis, avaliados a partir de expectativas realistas e metódicas, um diagnóstico sobre o ambiente de controle da organização, no intuito de identificar

riscos que comprometam a realização destes objetivos estratégicos ou oportunidades para o aperfeiçoamento da gestão.

Fluxograma 2 – Evolução da relação Estado x controles

Fonte: Elaboração própria (2025).

A identificação de eventos com potencial para influenciar negativamente os resultados pretendidos (riscos inerentes ou do negócio) abrange uma conceituação destes eventos por categorias, muitas vezes com seus efeitos deletérios se estendendo por mais de uma delas:

- Risco de conformidade, decorrente de falhas que impedem o cumprimento às leis, normas, regulamentos, princípios e planos de ação;
- Risco de integridade, decorrente da incompatibilidade do evento com valores, princípios e normas éticas estabelecidas pela própria instituição, notadamente quanto à caracterização de fraudes e à prática de atos de corrupção;
- Risco de registros, relacionado a falhas na segurança de registros e *backups*, gestão de documentos e bancos de dados, tratamento, validação e certificação de informações estratégicas, problemas de comunicação, imprecisão ou extravio de dados;
- Risco financeiro, relacionado a despesas indevidas que podem ocasionar desequilíbrio financeiro;
- Risco operacional, evento com potencial para comprometer a eficácia, economicidade, eficiência ou efetividade das operações;
- Risco reputacional, que está vinculado ao desgaste da imagem institucional ou perda da credibilidade junto ao controle externo, *stakeholders* ou ao controle social, por falhas de comunicação, atos ou negócios questionáveis; e
- Risco socioambiental, relacionado a repercussões negativas das atividades da organização sobre a sustentabilidade econômica e/ou ambiental.

Figura 1 – Modelo de Análise *SWOT* para a realização da análise de contexto da organização

AMBIENTE INTERNO		AMBIENTE EXTERNO
FORÇAS	+	OPORTUNIDADES
1.		1.
2.		2.
3.		3.
4.		4.
n.		*n.*
AMBIENTE INTERNO		AMBIENTE EXTERNO
FRAQUEZAS	-	AMEAÇAS
1.		1.
2.		2.
3.		3.
4.		4.
n.		*n.*

Fonte: Elaboração própria (2025).

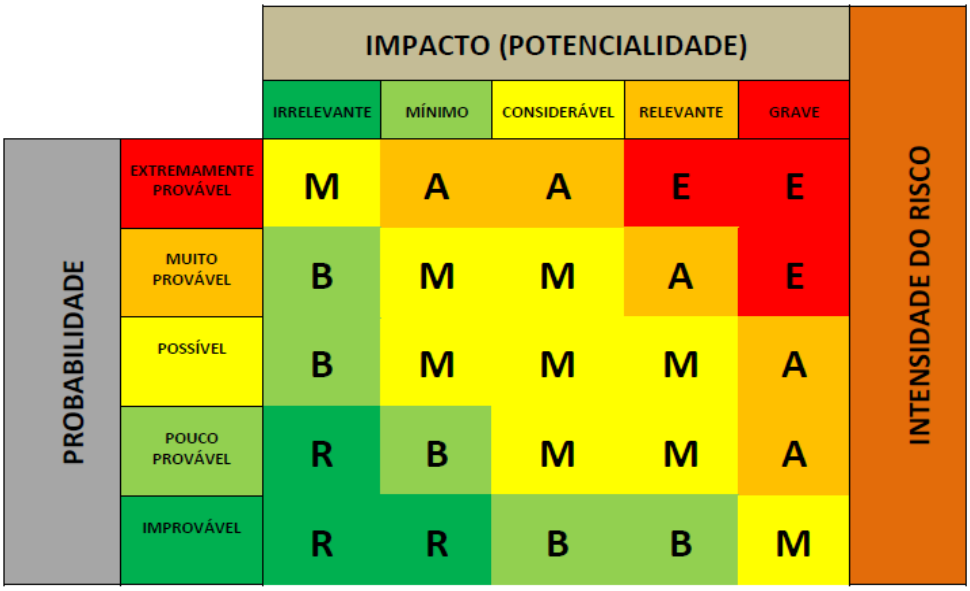
Figura 2 – Categorias de riscos

Fonte: Reprodução Pesquisa Google (google.com/search).

Antes de iniciar a próxima etapa para estabelecer um plano de controle, relacionada à avaliação dos riscos identificados, é necessário que esteja devidamente estabelecido o percentual de risco aceitável, que não demandará a eliminação dos processos de trabalho, a mitigação ou transferência do risco, com base em avaliação de custo-benefício, o que representará o nível de apetite a risco que a organização estará disposta a assumir.

No diagrama abaixo, esta margem de convivência e aceitação de atividades de controle já existentes ou não, por vezes empíricas ou anteriores à identificação do próprio evento potencialmente negativo, é representada pela faixa verde mais escura, com intensidade reduzida.

Diagrama 2 – Matriz de riscos



Fonte: Elaboração própria (2025).

LEGENDA (INTENSIDADE DO RISCO AVALIADO):

E	**ELEVADA**
A	**ALTA**
M	**MÉDIA**
B	**BAIXA**
R	**REDUZIDA**

Fonte: Elaboração própria (2025).

Considerando o nível de apetite a risco (A) como menor ou igual a 12% (0 < A ≤ 0,12), de acordo com o alcance da faixa em verde escuro, ao avaliarmos o risco inerente (RI), ao qual ainda não foi aplicada nenhuma das quatro espécies de resposta (aceitar, mitigar, transferir/compartilhar ou evitar), com intensidade limitada a este percentual, a alternativa correta, em termos de relação custo-benefício positiva, será aceitar o risco, o que implica em não providenciar qualquer procedimento ou atividade para mitigar (reduzir a probabilidade de ocorrência ou o impacto negativo do risco), transferir/compartilhar (dividir com outro responsável a

tarefa de mitigar ou contingenciar o risco, geralmente por obrigação de natureza contratual) ou evitar o risco (descontinuar os processos de trabalho relacionados ao evento).

Por outro lado, quando já existirem atividades de controle, ainda que empíricas ou insuficientes para mitigar, a níveis aceitáveis, ou evitar o risco, comportando elemento residual a ser tratado, ou risco residual (RR), a espécie de resposta a ser aplicada será: (*i*) mitigar o patamar de intensidade do risco, para níveis aceitáveis; (*ii*) transferir ou compartilhar com outrem a responsabilidade pela mitigação do risco; ou (*iii*) evitar o risco, dependendo do grau de intensidade do evento, em ordem crescente.

A matriz de riscos demonstra que o patamar de apetite a risco (aceitação) está situado entre o improvável e pouco provável, com potencialidade entre irrelevante e mínima (A ≤ P x I ≤ 0,12), e não deve ser confundido com o conceito de tolerância a risco, que não constitui uma categoria de resposta ao evento, mas o ajuste necessário das atividades de controle ou de outras providências adotadas para mitigar o risco que não foi aceito, sempre com vistas à consecução do objetivo estratégico.

O risco inerente (RI) é próprio da natureza da atividade ou dos processos de trabalho desenvolvidos pela organização.

O risco residual (RR) compõe a parcela dos riscos inerentes não mitigada ou evitada pelos mecanismos de controle. É um forte indicador sobre o nível de confiança dos controles internos aplicados (NC) e a dimensão do risco de controle (RC), que, por sua vez, representa a limitação do controle interno, em face dos recursos disponíveis para prevenir riscos inerentes à organização ou detectar e corrigir discrepâncias relativas aos critérios estabelecidos como padrões de qualidade, ou seja, a diferença entre o nível real e o nível ideal de controle.

RI → P x I, onde:

P = probabilidade de ocorrência do evento

I = impacto ou potencial dano sobre o objetivo estratégico

RC → 1 – NC, onde:

NC = nível de confiança dos controles internos

RR → RI x RC

RI ≤ 0,12 → margem de apetite a risco ou aceitação. Não requer mitigação, aplicação ou incremento de qualquer outra atividade pelo controle interno, ou mesmo a descontinuidade dos processos de trabalho.

RR ≤ 0,12 → margem de tolerância a risco ou situação em que as atividades de controle ou outras respostas a risco conseguem assegurar a consecução do objetivo estratégico.

Segundo o Tribunal de Contas da União (TCU, 2020), são princípios aplicáveis à gestão de riscos:

- Fomento à gestão empreendedora responsável, a fim de proporcionar maior possibilidade de sucesso às iniciativas inovadoras;
- Integralidade para a análise de contexto da organização, considerando riscos e também oportunidades;
- Universalidade em relação a qualquer iniciativa organizacional que tenha como ponto de partida um objetivo claramente definido;
- Caráter de continuidade como instrumento essencial para respaldar os processos decisórios;
- Abertura para admitir avaliações e revisões periódicas dos processos de trabalho;
- Compreensão sobre todo o contexto de cultura organizacional e fatores humanos relevantes; e
- Estreita relação com as políticas conduzidas pela alta administração.

De acordo com a Associação Brasileira de Normas Técnicas (ABNT, 2018), a incerteza a respeito da consecução dos objetivos estratégicos é um fenômeno que atinge todos os tipos de organizações, cujas causas podem ser atribuídas tanto a fatores externos como ao contexto interno (ambiente de controle, cultura organizacional, comportamento humano e fatores culturais).[2]

Finalmente, após cumprir esta sequência de atividades preparatórias necessárias para uma eficaz utilização e máximo aproveitamento sobre as

[2] O gerenciamento de riscos constitui parte essencial da governança e liderança corporativa. É um compromisso da alta administração com os resultados institucionais, que perpassa todos os níveis da organização, integra todas as atividades e processos de trabalho e interage com todas as instâncias de gestão (governança, planejamento, direção, execução, revisão dos processos de trabalho e manutenção de um fluxo de comunicação permanente e eficaz).

funcionalidades do SIAI – GR, o gestor estará habilitado para definir um plano de ação sobre as atividades de controle e cadastrar os processos de trabalho pertinentes, no ambiente de interação do aplicativo.

Então, em que consiste o ciclo completo do gerenciamento de riscos e das atividades de controle?

Este processo integral faz mover a engrenagem concebida pela governança da organização, no intuito de gerenciar riscos e obter segurança razoável quanto ao alcance dos objetivos estratégicos.

A governança com foco nos resultados marca a transição entre os modelos de Estado burocrático (segurança como fim) e gerencial (prestação de serviços de qualidade com segurança razoável).

A partir da internalização de um programa continuado de avaliação de riscos, em busca de fragilidades (fraquezas internas e ameaças externas) que ensejem a provável ocorrência de eventos com potencial para prejudicar os objetivos estratégicos, é possível alcançar os fins institucionais, agregando valor à organização, sem abrir mão de níveis razoáveis de segurança.

3 Implementando o plano de atividades de controle

O custo (moral, financeiro, operacional, humano, patrimonial, reputacional ou socioambiental) de um controle não pode ser maior do que o benefício proposto. Esta diretriz fundamental para a Administração Pública tem assento constitucional (artigo 70, *caput*, da Constituição Federativa) e é de observância obrigatória para a desburocratização e modernização do Estado, uma vez que a dimensão do dano a prevenir não pode ser inferior ao esforço necessário para a realização das ações preventivas.

Para o Departamento de *Compliance* e Riscos da Empresa Brasileira de Correios e Telégrafos (DECRI, 2023), a avaliação sobre o custo-benefício é essencial para otimizar o plano de atividades de controle a ser proposto, pois contribui para evitar o desperdício de recursos e a adoção de rotinas desproporcionais, ao se estabelecer uma política de gerenciamento de riscos e execução de atividades de controle.

Esta etapa permite o cadastro e acompanhamento das atividades de controle que serão realizadas de acordo com a estratégia escolhida para a abordagem e resposta aos riscos identificados e avaliados, inclusive sob a perspectiva do custo-benefício.

O plano de atividades de controle pode considerar, de acordo com a gravidade dos riscos, tanto a implementação de respostas a eventos ainda não tratados, o aprimoramento dos controles existentes ou a complementação destes instrumentos a partir da adoção de novas atividades de controle, através da delegação de autoridade, competência e responsabilidade pela execução das tarefas, e elaboração de um cronograma de trabalho (definição de prazos para a conclusão das tarefas e das metas ou etapas respectivas).

Além da graduação que deve ser estabelecida para os controles (desde a aplicação de controles ainda inexistentes, aprimoramento dos que já existem ou agregação de novas atividades), é necessário considerar também que mesmo as categorias de respostas inseridas nestes controles seguem um padrão de escalonamento que, como vimos anteriormente, vai da aceitação do risco ao encerramento do processo organizacional, de acordo com a seguinte disposição:

- **ACEITAR** riscos cuja relação custo-benefício (B – C) é negativa (o esforço para mitigar o evento é maior do que a sua intensidade avaliada);

- **MITIGAR** riscos com relação custo-benefício positiva, inclusive por intermédio da aplicação dos chamados controles compensatórios das fragilidades estruturais da organização, que devem ser implantados com o fim de reduzir a severidade dos eventos que apresentam potencial considerável de dano e elevada probabilidade de concretização;
- **TRANSFERIR/COMPARTILHAR**, com terceiros, riscos cujo custo de mitigação seja elevado; e
- **EVITAR**, após aprovação da instância de governança, riscos cujo custo de seguridade seja impraticável.

A elaboração de um plano de atividades de controle pressupõe o desenho ou configuração destes processos de trabalho, sua efetiva execução, a manutenção de um fluxo seguro, permanente e eficaz de dados por todos os níveis da organização, em todas as direções e por todos os ambientes (interno e externo), bem como a avaliação operacional destas atividades.

Atividades de controle estabelecidas antes de qualquer consideração a respeito da fixação dos objetivos estratégicos, da análise do ambiente de controle e da identificação de eventos com potencial para influenciar a consecução dos objetivos são, em geral, construídas a partir de uma lógica de empirismo, sem a aplicação de qualquer método para a gestão de riscos, e vinculam-se, não raramente, à execução de medidas de contingência, de caráter essencialmente reativo e que têm como causa eventos concretos, já realizados, que já experienciaram a frequência com que podem ser repetidos e o seu potencial de dano.

Medidas de contingência não são respostas a riscos, mas a eventos concretos. Não perfazem boas práticas de gestão, porque submetem a organização a uma permanente corrida contra o “prejuízo”.

A Assessoria Especial de Controles Internos do então Ministério do Planejamento, Desenvolvimento e Gestão (AECI, 2017) destaca que o acesso a informações confiáveis, íntegras e tempestivas é determinante para a consecução dos objetivos estratégicos. Consequentemente, a elaboração da informação e a comunicação aos interessados são essenciais para o estabelecimento do plano de atividades de controle.

O fluxo contínuo de dados deve gerar informações úteis, oportunas e adequadas, que perpassem todos os níveis da organização (da governança às atividades instrumentais), interagindo com o ambiente externo e os *stakeholders*.

Para encerrar, a execução do plano de atividades de controle demandará monitoramento, cujas conclusões serão objeto do relatório de implementação do plano de atividades de controle, e precisarão refletir a aplicação de um padrão mínimo de qualidade contextual e representação, suficiente para garantir a utilidade do trabalho: integralidade, adequação e objetividade das informações apresentadas.

Somente é possível avaliar ou monitorar a qualidade de controles efetivamente estabelecidos ou implementados. Os objetos destas avaliações serão a adequação do desenho empregado, a efetiva aplicação dos procedimentos e a eficiência operacional das atividades.

O procedimento para a avaliação dos controles estabelecidos no plano de ação envolve a aplicação de testes de desenho, implementação e eficiência operacional das atividades, exatidão e validade das informações geradas através do fluxo de comunicações da organização, baseados em indicadores adequados para estabelecer o nível de tolerância a risco e determinar os ajustes necessários.

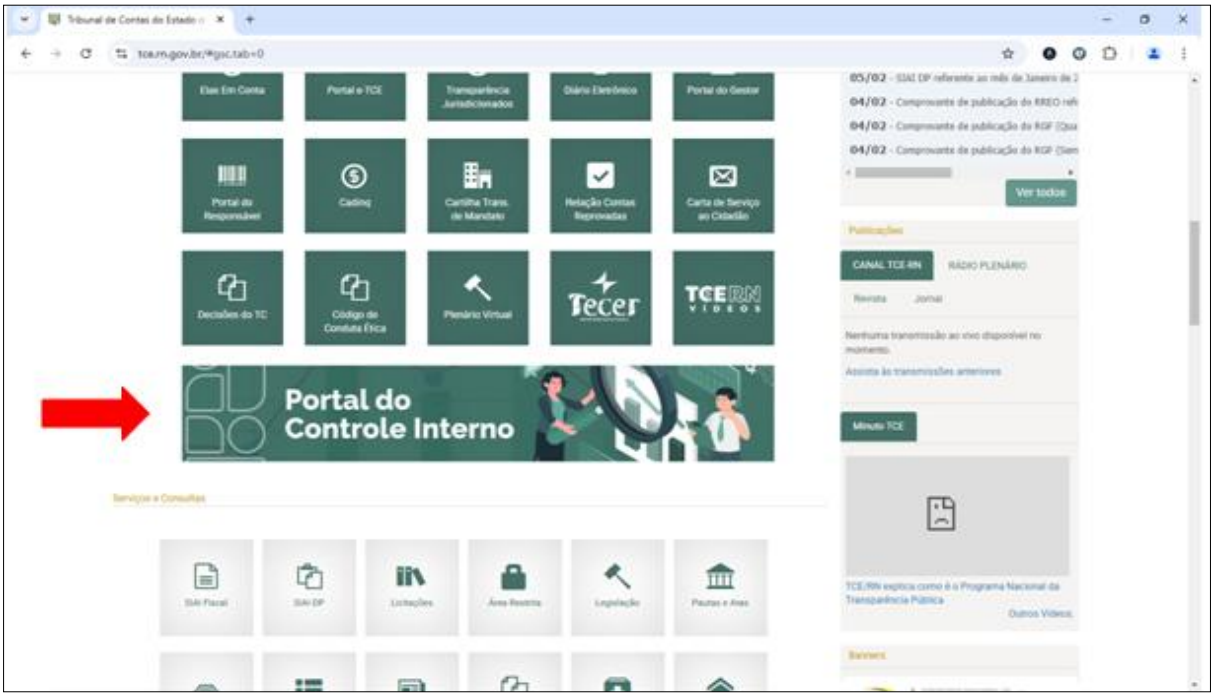
Fluxograma 3 – Ciclo do gerenciamento de riscos e controles

Fonte: Assessoria Especial de Controles Internos do Ministério do Planejamento, Desenvolvimento e Gestão (AECI), 2017, p. 23 (reprodução do *COSO ERM*, 2004).

4 Acesso ao SIAI – GR

Para iniciar a utilização sobre as funcionalidades do SIAI – GR, em primeiro lugar, o servidor devidamente habilitado como operador externo, com permissões para cadastrar ou validar a programação de gerenciamento de riscos e atividades de controle, deverá acessar, pelo respectivo *browser*, o Portal do Controle Interno gerido pelo Tribunal de Contas do Estado do Rio Grande do Norte, a partir do endereço https://pci.tce.rn.gov.br/#/ ou através do *banner* disponível no Portal do TCE (https://www.tce.rn.gov.br/#gsc.tab=0), de acordo com a interface a seguir:

Tela 1 – Portal do Controle Interno *(banner)*



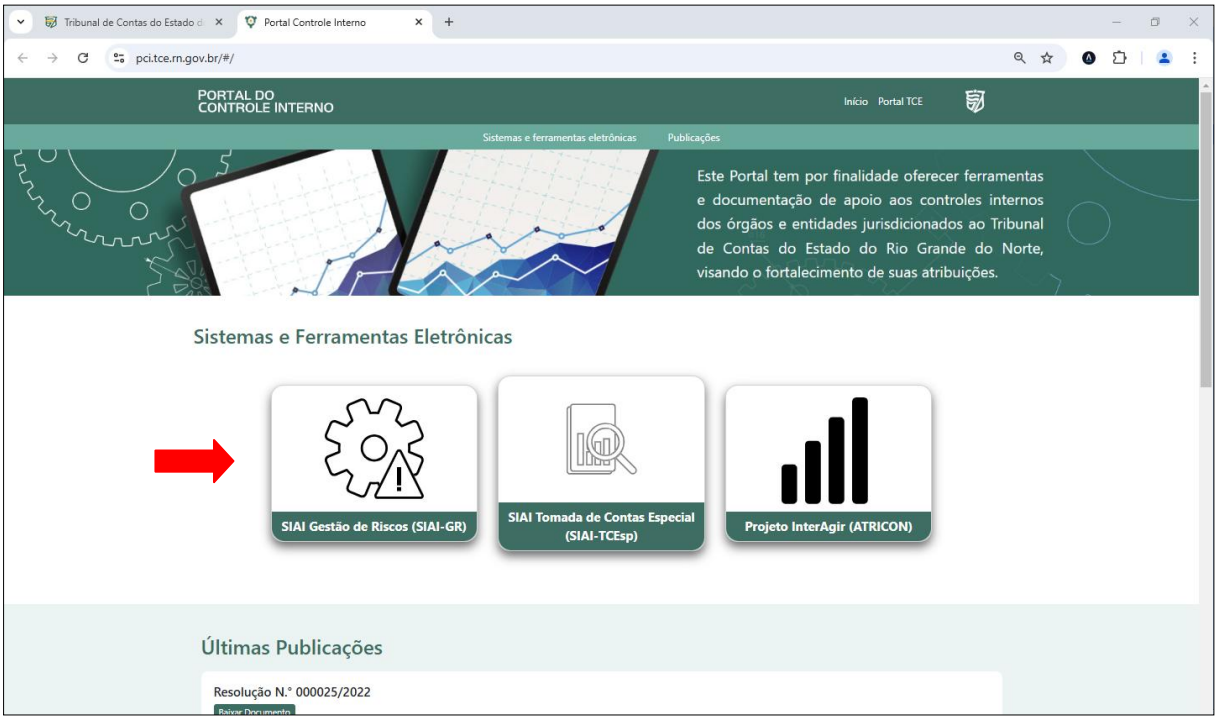
Fonte: Portal do TCE (2025).

Após acessar o Portal do Controle Interno, o usuário autorizado visualizará a tela inicial do *site* e deverá acionar o *botton* SIAI Gestão de Riscos (SIAI – GR).

A tela seguinte abre com os campos para a apresentação das credenciais fornecidas de acordo com a disciplina específica para o acesso e utilização das funcionalidades disponibilizadas pelo portal.

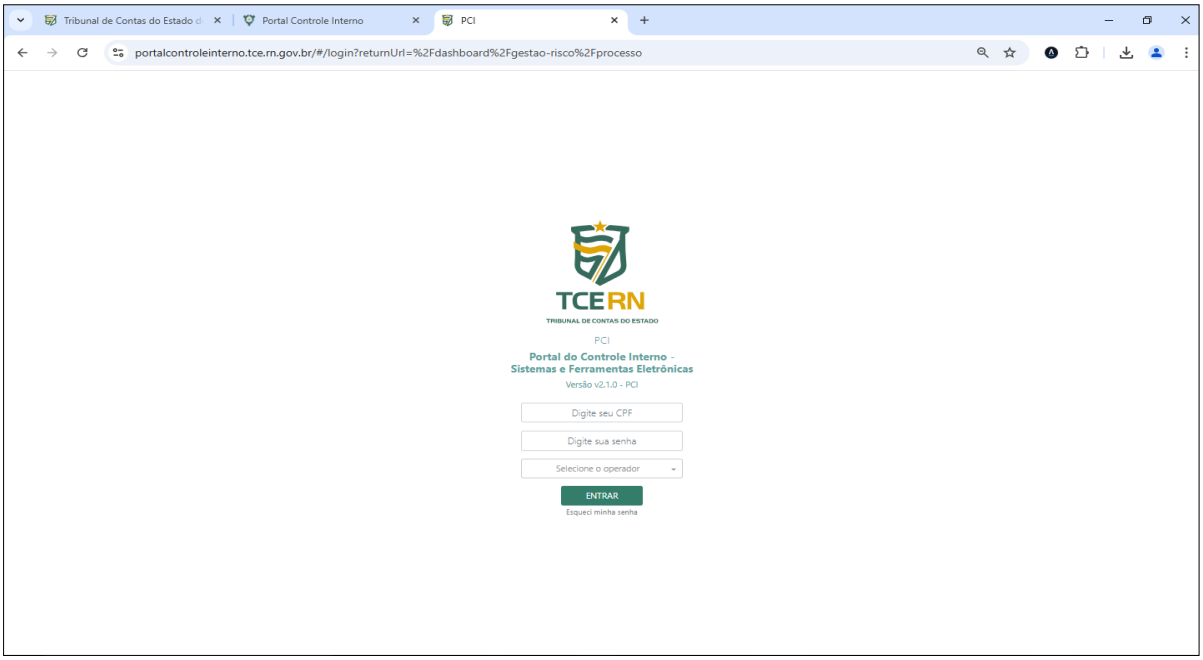
Após confirmar a identidade e senha para *login*, e indicar o perfil de operador (gestores e jurisdicionados), o usuário alcançará a tela inicial para a interface do sistema.

Tela 2 – Portal do Controle Interno *(home)*



Fonte: Portal do Controle Interno (2025).

Tela 3 – Apresentação das credenciais



Fonte: Portal do Controle Interno (2025).

Quanto ao perfil de operador externo, com permissão para cadastrar ou validar planos de atividades de controle, o usuário terá acesso, no menu Gestão de Riscos, à função Gerenciar Processo.

A tela inicial do SIAI – GR permite consultar cada plano de controle cadastrado pela entidade, unidade ou órgão jurisdicionado, relacionado a um processo voltado à consecução de um objetivo estratégico.

Os campos dos filtros que devem ser utilizados para refinar a pesquisa são:

- MACROPROCESSO

Constitui a área-chave para a consecução dos objetivos estratégicos de uma organização, pautados pela sua identidade institucional. Composto por agrupamentos de processos de trabalho informados por perspectivas de resultados finalísticos (interesse dos beneficiários do serviço ou da sociedade em geral), de apoio (instrumentos para a eficiência da organização) ou gestão (adequação à estratégia).

O campo com este filtro contém uma lista fechada de opções cadastradas pelo próprio operador externo.

- PROCESSO

É o conjunto de atividades que compõem e se voltam à consecução dos resultados do macroprocesso (finalísticos, de apoio ou gestão). Este campo deve ser informado, para consulta, de acordo com a nomenclatura dos processos já cadastrados pela organização.

- UNIDADES JURISDICIONADAS

Compreende uma lista fechada de opções cadastradas pelo gestor do sistema.

- DATA DE CADASTRO

Permite a busca pela data de cadastramento do plano de atividade de controle.

- DATA DE VALIDAÇÃO

Permite a busca pela data de validação do plano de atividades de controle, registrada após a revisão pelo supervisor da ação.

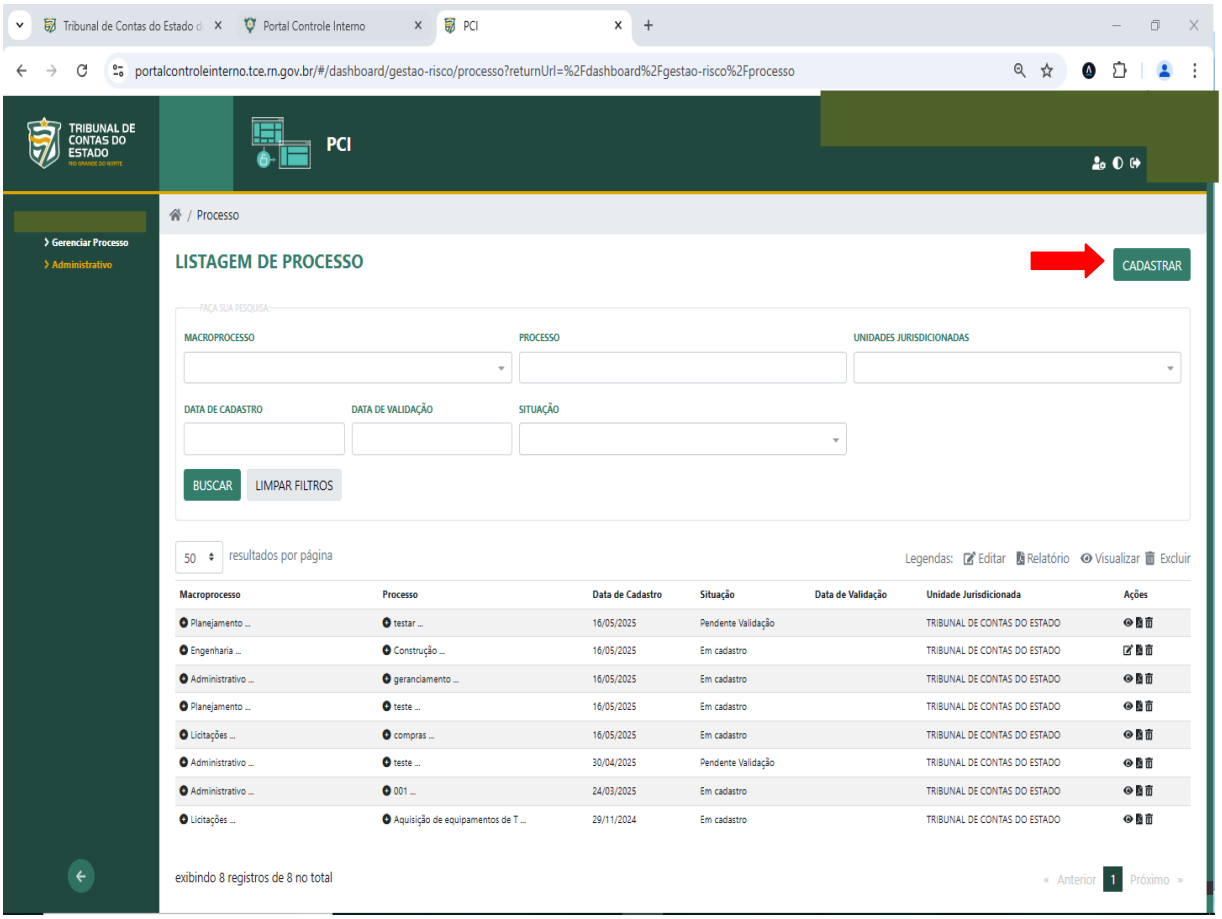
- SITUAÇÃO

Este campo permite especificar o objeto da pesquisa de acordo com uma lista fechada de opções a respeito da condição ou estágio do cadastro, relativo ao plano de controle buscado.

Para cadastrar um novo plano de atividades de controle, o operador deverá acionar o *botton* CADASTRAR, que aparece na cor verde, no canto superior direito da tela inicial, logo abaixo dos dados de identificação do usuário.

Será aberta uma nova tela (Gerenciar Processo), contemplando os seis *steppers* que representam o passo a passo para o cadastramento do plano de controle que deverá ser monitorado. O *stepper* indicado em verde claro corresponde à etapa cujos dados solicitados estão sendo inseridos nos campos respectivos, para a organização das informações. Em verde escuro com tique (✓), a etapa finalizada.

Tela 4 – SIAI – GR *(home)*



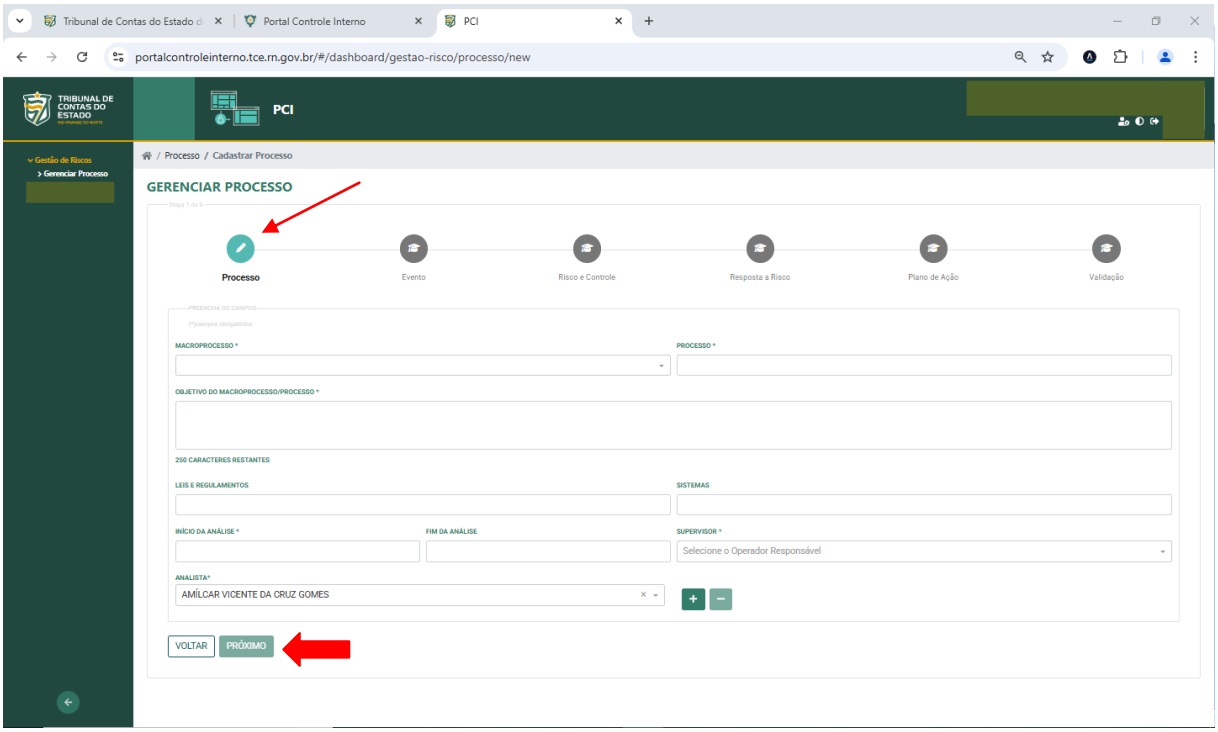
Fonte: Interface do SIAI – GR (2025).

4.1 Cadastrar dados do processo

O campo com descrição marcada por asterisco (*) deve ser adequadamente preenchido, para que o cadastramento do novo plano de atividades de controle avance para a etapa seguinte.

No campo OBJETIVO DO MACROPROCESSO/PROCESSO deve ser informada a finalidade do processo relacionado ao cadastramento do novo plano de atividades de controle e a sua vinculação a uma das três perspectivas de resultados (finalísticos, de apoio ou gestão).

Tela 5 – Cadastrar dados do processo



Fonte: Interface do SIAI – GR (2025).

No campo LEIS E REGULAMENTOS deve ser informada a legislação e os atos que esclarecem a aplicação das normas pertinentes ao processo que está sendo gerenciado.

O campo SISTEMAS deverá conter informações sobre sistemas ou meios informáticos já utilizados pelo órgão ou entidade, para gerenciar o processo respectivo.

Campos INÍCIO e FIM DA ANÁLISE: devem ser preenchidos com as datas de início do cadastramento do novo plano de atividades de controle e do fim da análise e revisão sobre o plano que está sendo gerenciado.

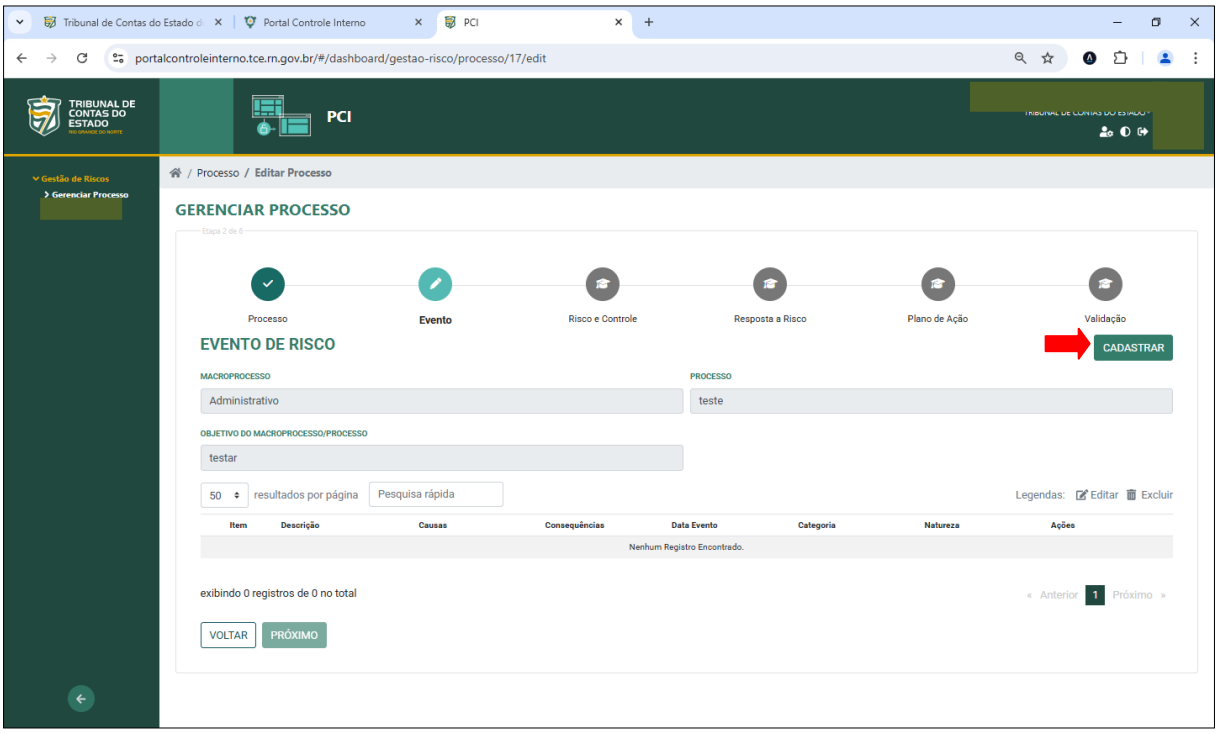
Os campos ANALISTA e SUPERVISOR apresentam listas fechadas de opções cadastradas pelo gestor do sistema, com os nomes dos servidores responsáveis pelo cadastramento e revisão/validação do plano de atividades de controle, respectivamente.

Os nomes destes servidores devem ser informados ao gestor do sistema (TCE) pelos respectivos órgãos jurisdicionados, de acordo com as instruções gerais e procedimentos pertinentes à operacionalização do Portal do Gestor, aplicáveis tanto ao modo de acesso quanto à sua utilização.

Acione o *botton* PRÓXIMO, localizado no canto inferior esquerdo da tela GERENCIAR PROCESSO, para a etapa seguinte.

4.2 Cadastrar evento de risco

Tela 6 – Cadastrar evento de risco



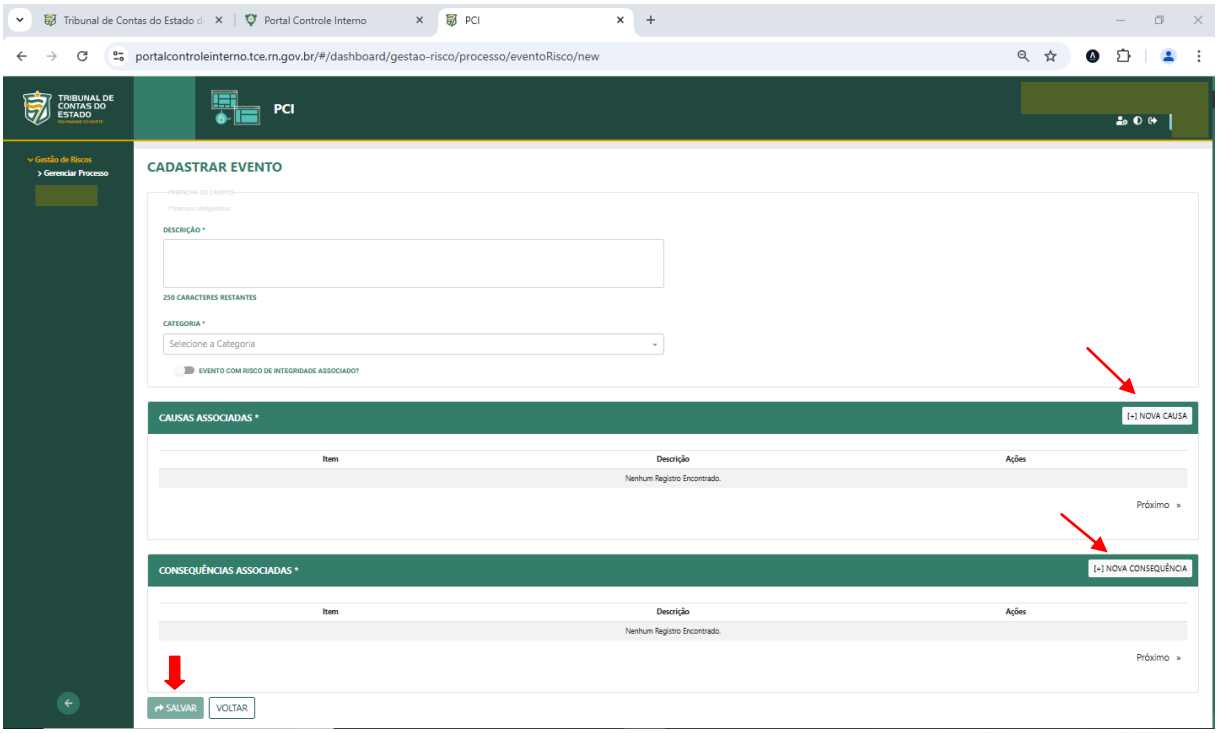
Fonte: Interface do SIAI – GR (2025).

Ao acionar o *botton* CADASTRAR, o operador do SIAI – GR acessará a tela CADASTRAR EVENTO. O campo DESCRIÇÃO, de preenchimento obrigatório, conterá uma exposição sucinta do evento potencialmente danoso em relação a algum dos objetivos estratégicos da organização, identificado de acordo com a sequência de tarefas fundamentais para que as atividades de controle forneçam segurança razoável quanto ao alcance dos objetivos estratégicos, descritas no item 2 deste manual, anteriores à implementação do plano de atividades de controle.

O campo CATEGORIA apresenta uma lista fechada de opções cadastradas pelo gestor do sistema. Está relacionado com a identificação do risco inerente (RI) à consecução do objetivo estratégico acautelado.

É importante observar, segundo (Decri, 2023) que um evento de risco pode estar vinculado a mais de uma categoria. Para evitar superestimação do impacto, deve ser escolhida apenas uma categoria de risco, com maior potencial de dano, de acordo com o planejamento e a análise de contexto previamente realizados pela organização.

Tela 7 – Cadastrar evento



Fonte: Interface do SIAI – GR (2025).

A exceção à regra da opção por uma única categoria de risco inerente (RI) ocorre quando o maior potencial de dano estiver vinculado a outra categoria e o evento contiver, também, risco de integridade associado. Nesta situação, além do preenchimento do campo CATEGORIA com a opção correspondente à maior perspectiva de impacto, é necessário também marcar a caixa de seleção *(checkbox)* com a pergunta: EVENTO COM RISCO DE INTEGRIDADE ASSOCIADO?

Lembramos que, se o risco de integridade já tiver sido identificado, avaliado e escolhido como aquela categoria de maior impacto, não precisará ser marcado na caixa de seleção.

O tratamento específico dispensado ao risco de integridade se deve à maior capacidade de intersecção desta com as demais categorias, potencial que não pode ser ignorado pelo proprietário do risco, para e elaboração de um plano de atividades de controle mais eficiente.

O campo NATUREZA é preenchido automaticamente pela operação do algoritmo, de acordo com a categoria de risco selecionada.

O *botton* ADICIONAR NOVA CAUSA permite editar a tabela CAUSAS ASSOCIADAS com as circunstâncias interiores ou exteriores (fatores de risco) que definem o indicador de probabilidade do evento.

O *botton* ADICIONAR NOVA CONSEQUÊNCIA permite editar a tabela CONSEQUÊNCIAS ASSOCIADAS com os potenciais impactos negativos do evento sobre a consecução dos objetivos estratégicos.

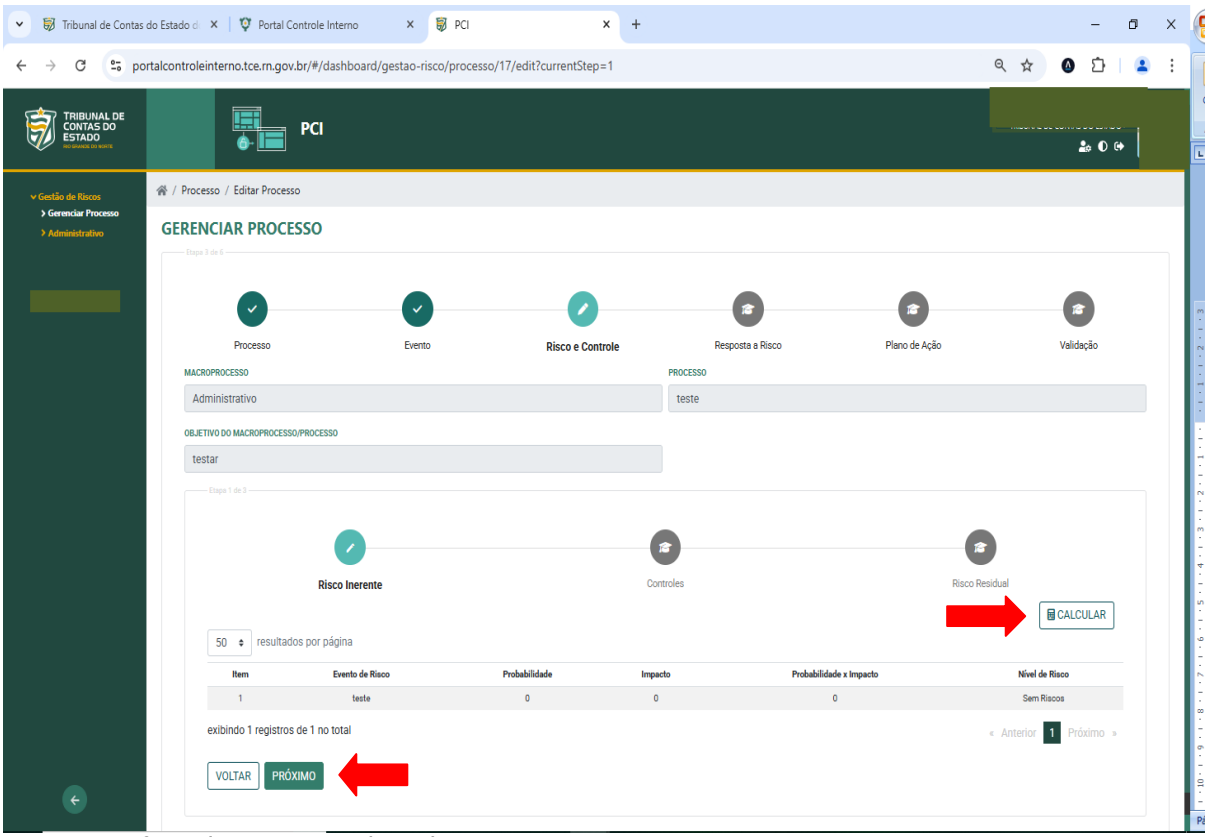
Para finalizar a etapa de edição do evento, o operador não pode esquecer de acionar o *botton* SALVAR, no canto inferior esquerdo da tela. Ao retornar à tela GERENCIAR PROCESSO, deverá ser acionado o *botton* PRÓXIMO, também localizado no canto inferior esquerdo.

4.3 Cálculo de riscos

Ao final da avaliação sobre a intensidade do risco inerente (RI) cadastrado, em face dos controles existentes, será determinado o patamar de risco residual (RR) que demandará o aperfeiçoamento dos controles existentes, a implementação de novas atividades de controle ou, simplesmente, a aceitação do risco em relação a uma eventual tolerância quanto à consecução do objetivo pretendido.

Mensurar o percentual de risco remanescente, após confrontar o risco identificado e avaliado (risco inerente) com a eficácia das ações de controle já existentes, constitui elemento imprescindível para uma revisão dos processos de trabalho e asseguração dos objetivos institucionais.

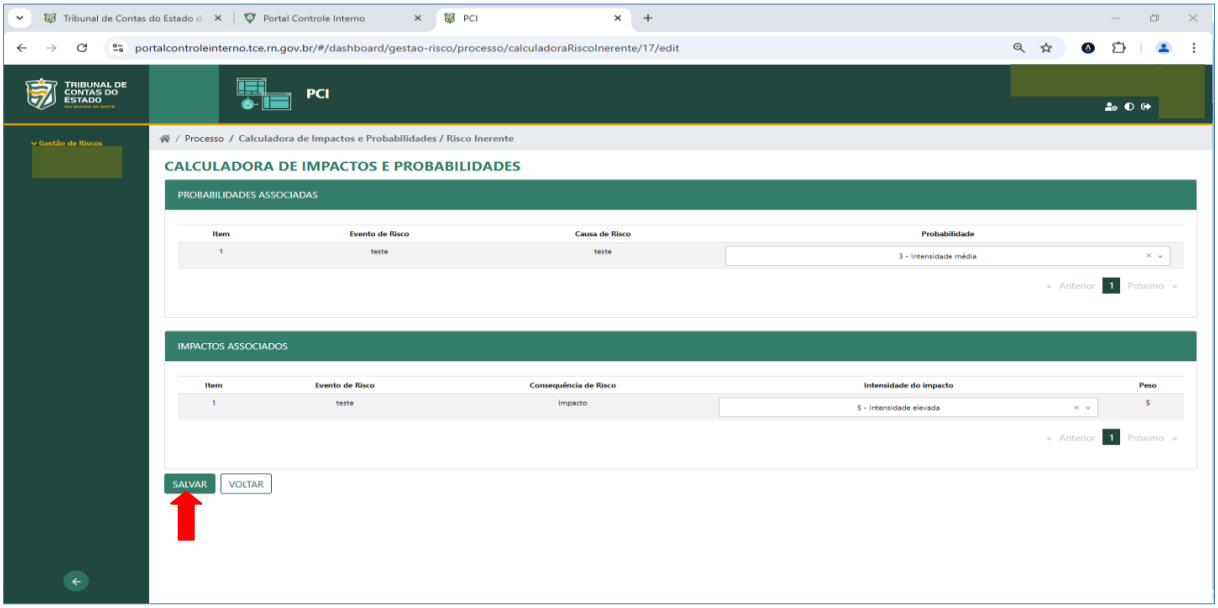
Tela 8 – Cálculo do risco inerente (RI)



Fonte: Interface do SIAI – GR (2025).

O primeiro passo para esta avaliação é indicar os níveis de intensidade associados à probabilidade e ao potencial de repercussão negativa (impacto) do evento de risco, sobre o objetivo estratégico acautelado, acionando o *botton* CALCULAR.

Tela 9 – Calculadora de impactos e probabilidades

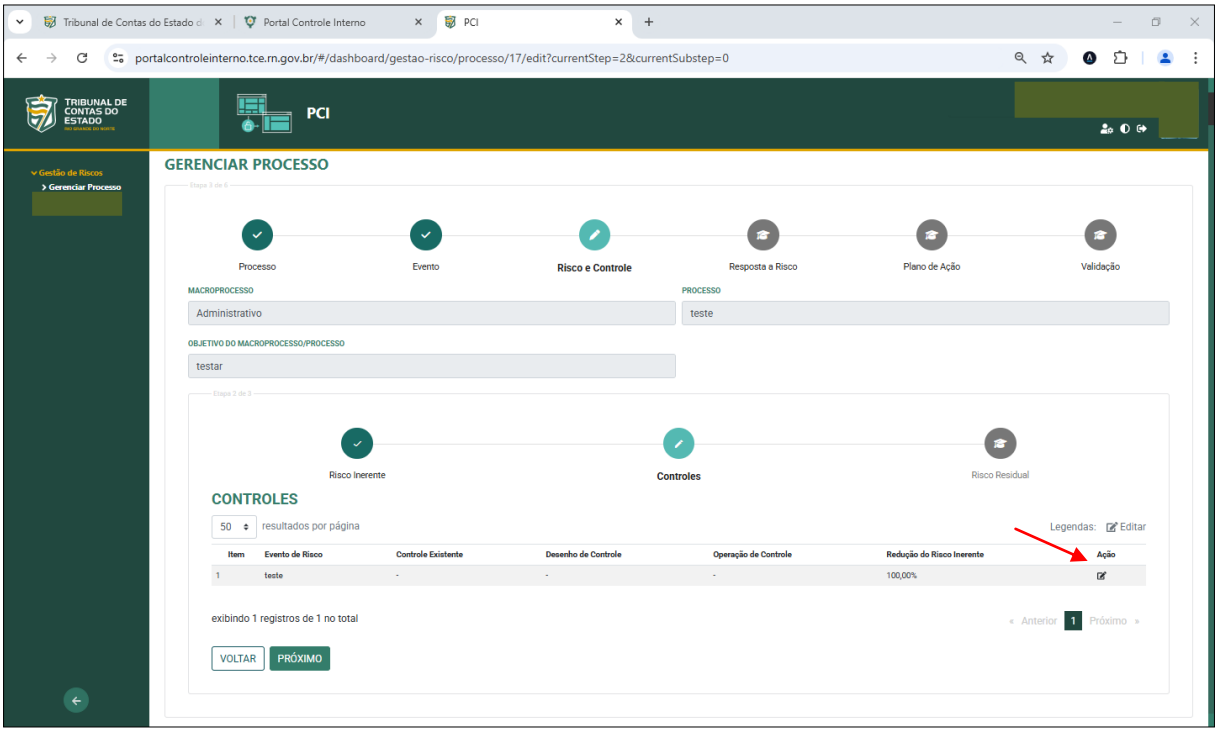


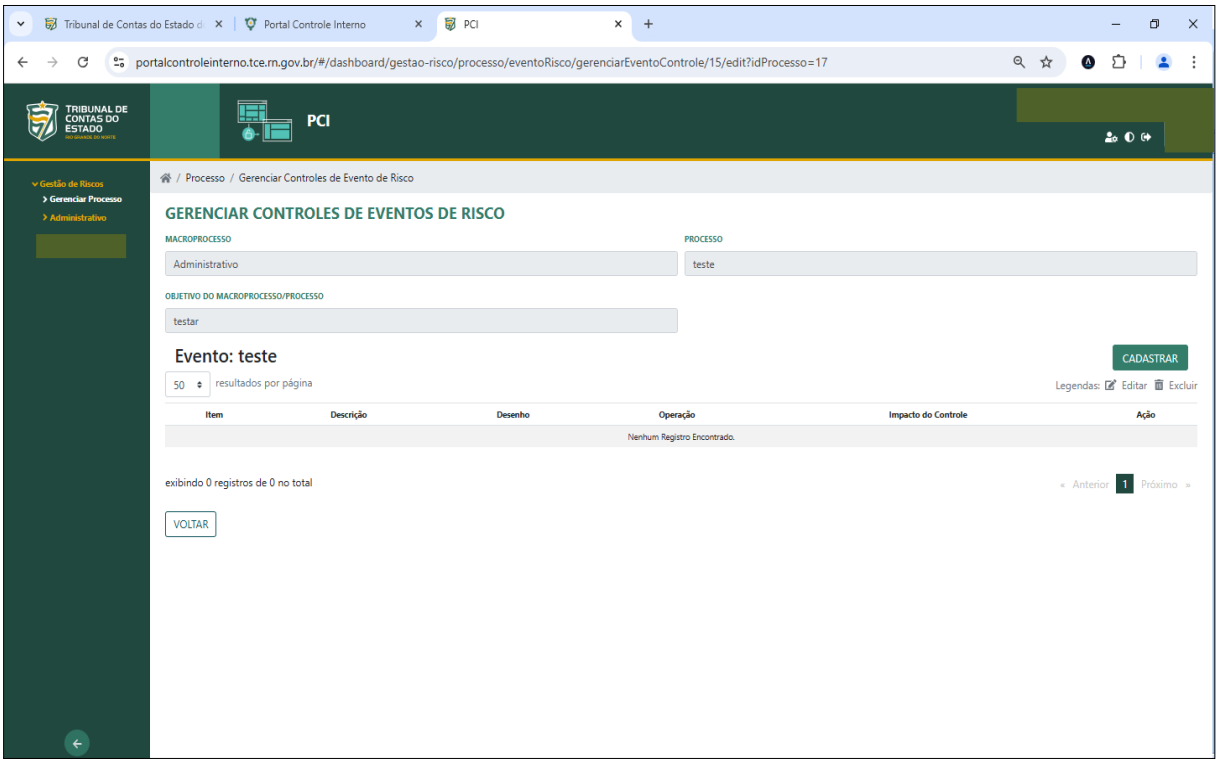
Fonte: Interface do SIAI – GR (2025).

Após salvar a operação, voltaremos para o *stepper* Risco e Controle, com a definição da intensidade do risco inerente (RI).

O *botton* PRÓXIMO conduzirá à etapa de avaliação dos controles existentes.

Tela 10 – Avaliação dos controles existentes





Fonte: Interface do SIAI – GR (2025).

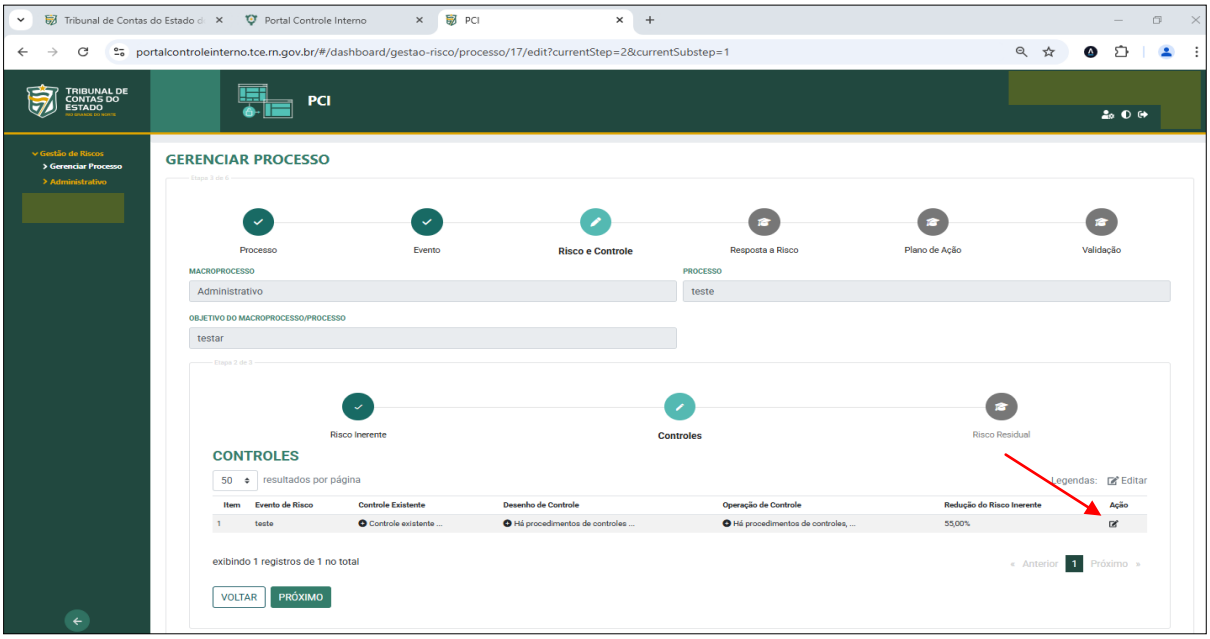
Acionando o *botton* Editar, à direita da Tela Gerenciar Processo, estará disponível a funcionalidade para cadastramento do controle existente, em relação ao risco inerente (RI) avaliado, com três campos de preenchimento obrigatório, onde o operador irá identificar, de forma sucinta, a atividade de controle respectiva (campo de livre descrição) e indicar, em campos com listas fechadas de opções cadastradas pelo gestor do sistema, o desenho do controle existente (nível de regulamentação da atividade) e a sua operação (nível de execução e documentação da atividade).

Se não houver regulamentação do controle correspondente ao evento de risco que está sendo cadastrado, os campos DESENHO CONTROLE e OPERAÇÃO deverão ser preenchidos com a opção *"Não há procedimento(s) de controle"*.

Após salvar a operação, estará determinado o impacto do controle sobre o risco inerente (RI), ou seja, o quanto (percentual) aquela atividade conseguiu mitigar ou transferir, em termos de dano potencial.

Na sequência, e "clicando" em VOLTAR, estaremos novamente na Tela Gerenciar Processo, com o percentual de intensidade restante, para o risco inerente (RI) avaliado, após considerar os controles existentes.

Tela 11 – Redução do risco inerente (RI)

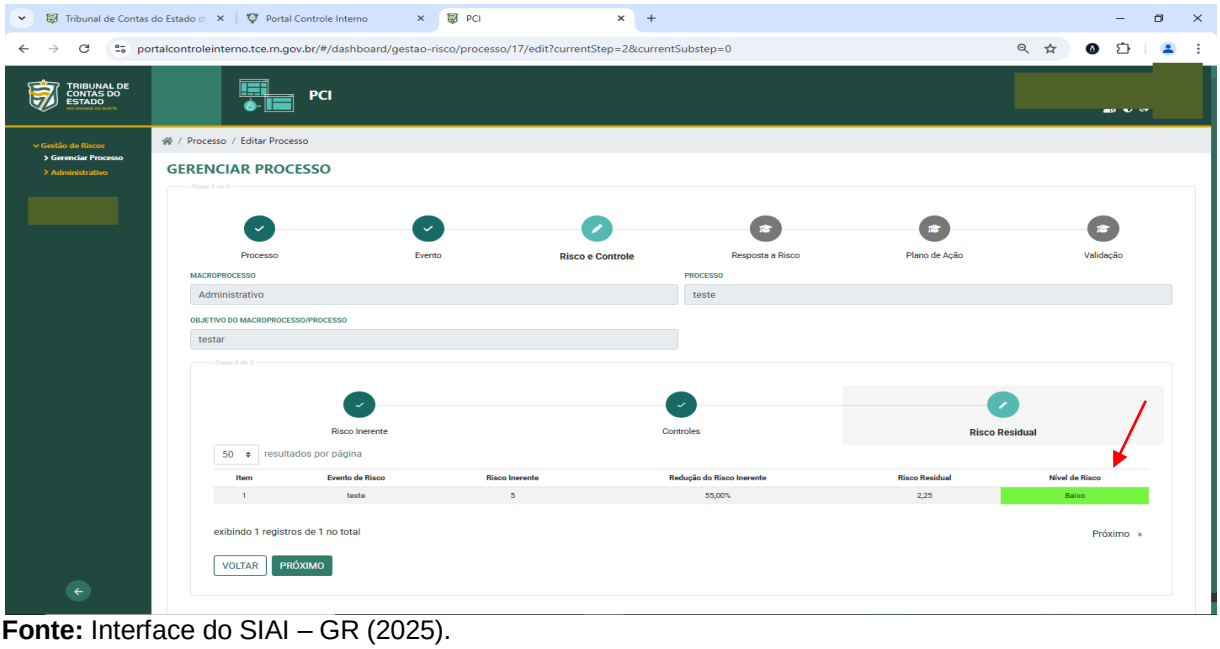


Fonte: Interface do SIAI – GR (2025).

A última etapa do cálculo de riscos é a definição do risco residual (RR) ou remanescente, após considerado o nível de confiança dos controles existentes.

O patamar atribuído ao risco residual (RR) constituirá o referencial para a definição das respostas adequadas aos eventos de risco, no cadastramento do plano de atividades de controle.

Tela 12 – Definição do risco residual (RR)



Fonte: Interface do SIAI – GR (2025).

Observamos que a valoração da intensidade do risco inerente (RI), do impacto dos controles existentes e do risco residual é realizada através de cálculo automatizado, pelo próprio algoritmo do SIAI – GR, a partir do cadastramento dos dados e preenchimento dos campos pelo operador.

Os níveis de risco residual (RR) padronizados são os seguintes, em comparação com a matriz de riscos apresentada no item 2, composta por 25 quadrantes:

- Os quadrantes 1 a 3, de intensidade reduzida, comportam riscos residuais de nível baixo, identificados no SIAI – GR pela coloração verde;
- Os quadrantes 4 a 8, de intensidade baixa até média, comportam riscos residuais de nível moderado, identificados no SIAI – GR pela coloração amarela;
- Os quadrantes 9 a 19, de intensidade média até alta, comportam riscos residuais de nível alto, identificados visualmente pela coloração laranja; e
- Os quadrantes a partir de 20, de intensidade elevada, comportam riscos residuais de nível muito alto, identificados pela coloração vermelha.

4.4 Definindo as respostas adequadas aos riscos

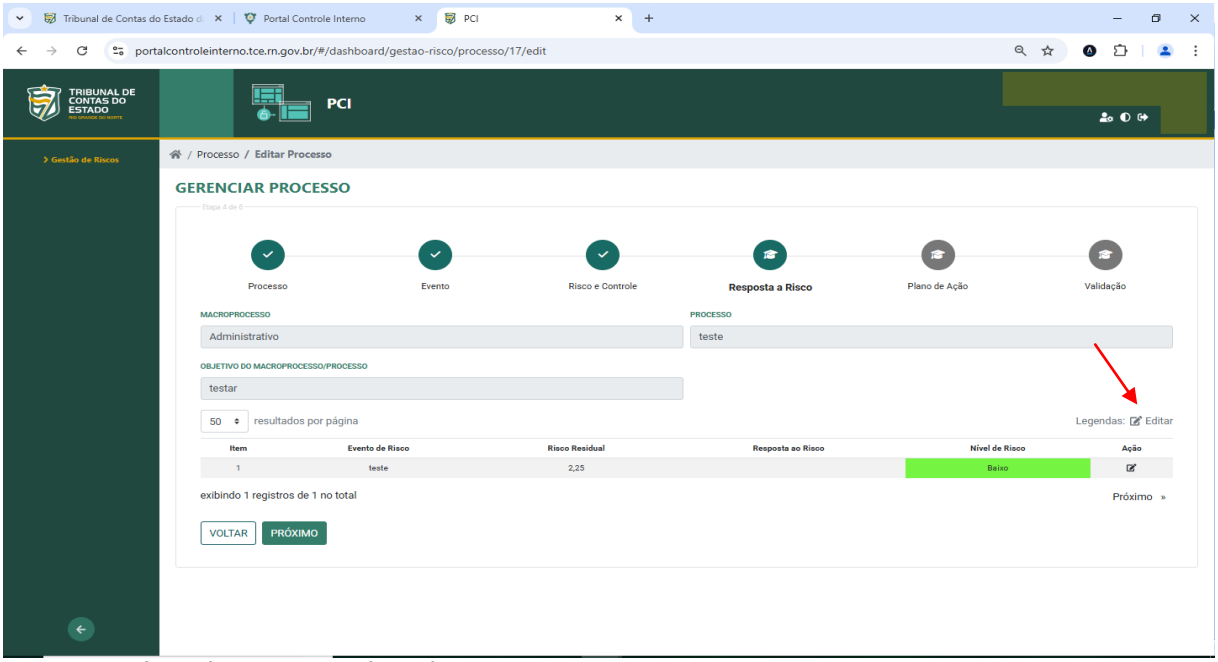
De acordo com o que observamos no item 3, a elaboração do plano de atividades de controle pode considerar, tendo em vista a gravidade dos riscos, tanto a implementação de respostas a eventos ainda não tratados, o aprimoramento dos controles existentes ou a complementação destes instrumentos a partir da adoção de novas atividades de controle, através da delegação de autoridade, competência e responsabilidade pela execução das tarefas, e elaboração de um cronograma de trabalho (definição de prazos para a conclusão das tarefas e das metas ou etapas respectivas).

Além da graduação que deve ser estabelecida para os controles, é necessário considerar também que mesmo as categorias de respostas inseridas nestes controles seguem um padrão de escalonamento que varia desde a aceitação do risco ao encerramento do processo organizacional.

A definição da resposta adequada ao risco avaliado é feita através de opção a partir de uma lista fechada, contendo as espécies já tratadas neste manual, e sugere uma progressão diretamente proporcional ao nível de risco apurado na etapa anterior, de forma que:

- Para um nível de risco residual considerado baixo, a resposta adequada é aceitar o risco;
- Para um nível de risco residual considerado moderado, a resposta adequada é mitigar o risco até uma situação de tolerância, o que poderá demandar desde a implementação de respostas a eventos ainda não tratados, o aprimoramento de controles existentes ou a complementação pelo cadastramento de mais de um processo de atividades de controle;
- Para um nível de risco residual considerado alto, o ideal é cadastrar tantos processos quantas sejam as atividades de controle necessárias para a mitigação e redução a padrões de tolerância; e
- Para um nível de risco residual considerado muito alto, além de levar em conta a elaboração de planos para mitigação, é importante cadastrar processos específicos para transferir riscos cujo custo de mitigação seja elevado ou descontinuar os processos de trabalho relacionados ao evento (evitar o risco), sempre após a aprovação pela instância de governança, quanto a riscos cujo custo de seguridade (ou transferência) seja impraticável.

Tela 13 – Resposta a risco



Fonte: Interface do SIAI – GR (2025).

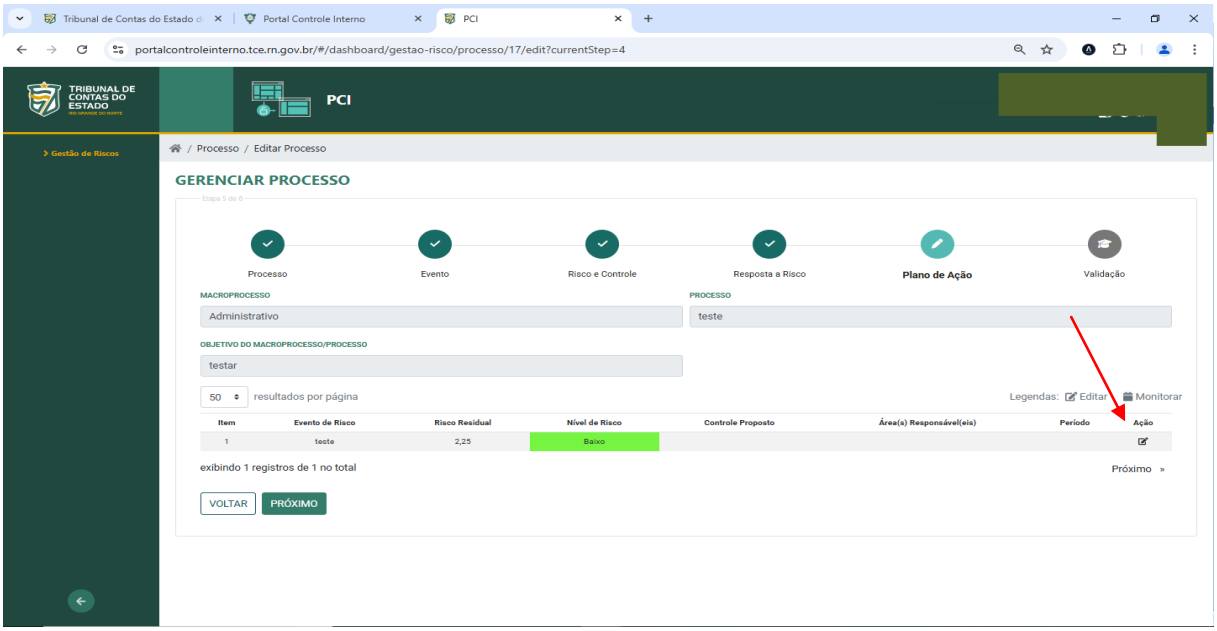
Acionando o *botton* Editar, à direita da Tela Gerenciar Processo, estará disponível a funcionalidade para cadastramento da resposta a risco.

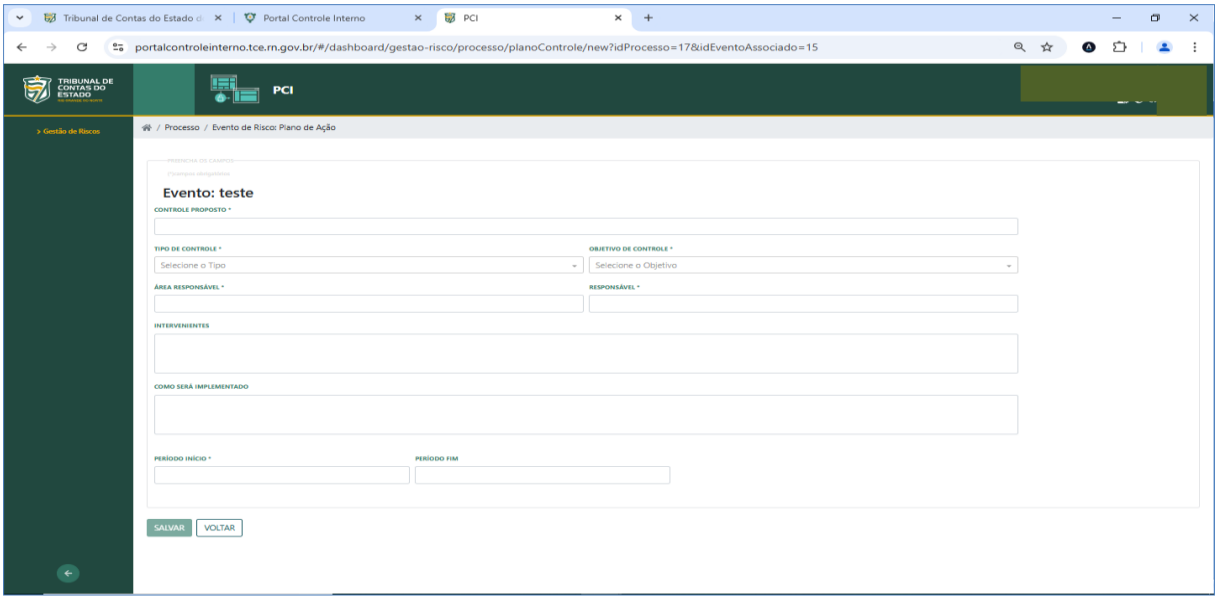
4.5 Plano de ação

A tela para cadastramento do plano de controle consiste numa ficha onde serão registrados os dados essenciais para a elaboração da programação referente às atividades de controle.

O campo CONTROLE PROPOSTO deve ser preenchido com a descrição da atividade que será adotada com base na espécie de resposta definida para o evento de risco.

Tela 14 – Plano de ação





Fonte: Interface do SIAI – GR (2025).

No campo TIPO DE CONTROLE será realizada a opção baseada na diferenciação entre resposta a risco e medida de contingência.

Também no item 3 vimos que respostas a eventos concretos não se coadunam com boas práticas de gestão, porque pressupõem a falta de análise de cenários que possam indicar, de forma preventiva, situações com potencial para influenciar negativamente os objetivos estratégicos da organização.

Assim, um planejamento de atividades de controle deverá sempre ser permeado por atividades de caráter preventivo, e a opção por medidas de contingência, de caráter corretivo, somente é considerada para remediar situações excepcionais e transitórias, que devem ser o quanto antes superadas por iniciativas mais apropriadas a uma gestão pública pautada na governança corporativa e coerentes com um modelo de Estado fornecedor de serviços.

O campo OBJETIVO DE CONTROLE indica se o planejamento é referente à implementação de respostas a eventos ainda não tratados ou de novas respostas, complementares a controles já existentes. Para estes situações, a opção adequada é adotar um controle novo.

Se o plano trata do aprimoramento de controles existentes, deve-se optar pela melhoria do controle existente.

No campo ÁREA RESPONSÁVEL será cadastrada a denominação da divisão ou setor administrativo incumbido da implementação das atividades de controle, de acordo com o organograma institucional e sob gestão do proprietário do risco.

O campo RESPONSÁVEL complementa a informação com a indicação do nome e do cargo ou função do proprietário do risco.

No campo INTERVENIENTES devem ser registrados os nomes, cargos ou funções de outros gerentes operacionais, responsáveis por outras áreas da organização, relevantes para a execução das atividades.

No campo COMO SERÁ IMPLEMENTADO constará um resumo do cronograma de trabalho, com a apresentação das metas ou etapas necessárias para o cumprimento do plano de ação, a definição de prazos para a conclusão de tarefas e a indicação das providências necessárias para a implementação das ações, assim como a delegação de autoridade, competência e responsabilidades.

Nos campos PERÍODO INÍCIO e PERÍODO FIM serão registrados os marcos temporais para a execução do plano de atividades de controle.

4.6 Monitoramento e validação

Após o preenchimento da ficha com os dados essenciais para a elaboração da programação referente às atividades de controle, e ainda no *stepper* Plano de Ação, surgirá o *botton* Monitorar, que dará acesso à tela de monitoramento dos controles planejados.

A opção CADASTRAR, à direita da tela, e em destaque, abrirá uma caixa de diálogo para a seleção de opções para registro de informações sobre o acompanhamento do plano de ação.

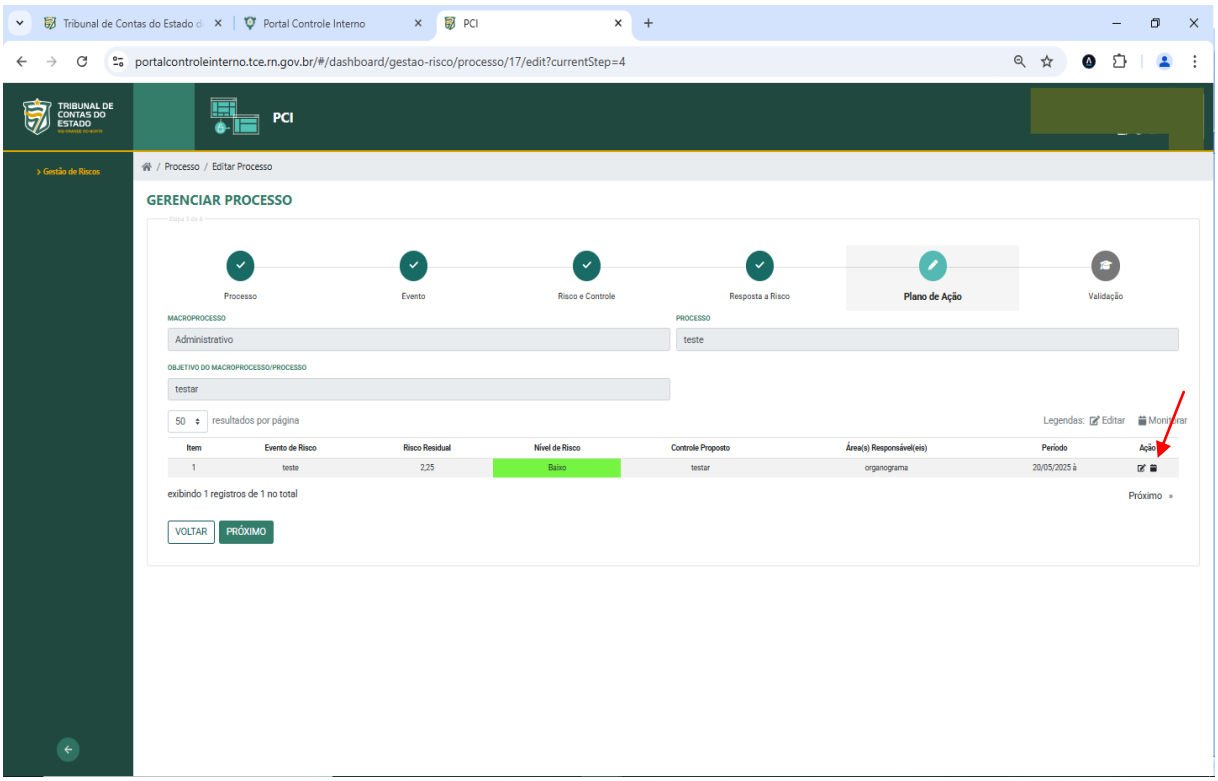
O monitoramento constitui parte essencial para a implementação de uma política de gerenciamento de riscos, através de ações continuadas de avaliação sobre a eficácia dos procedimentos de controle empregados, a fim de verificar o cumprimento de objetivos e metas e comunicar eventuais deficiências à estrutura de governança.

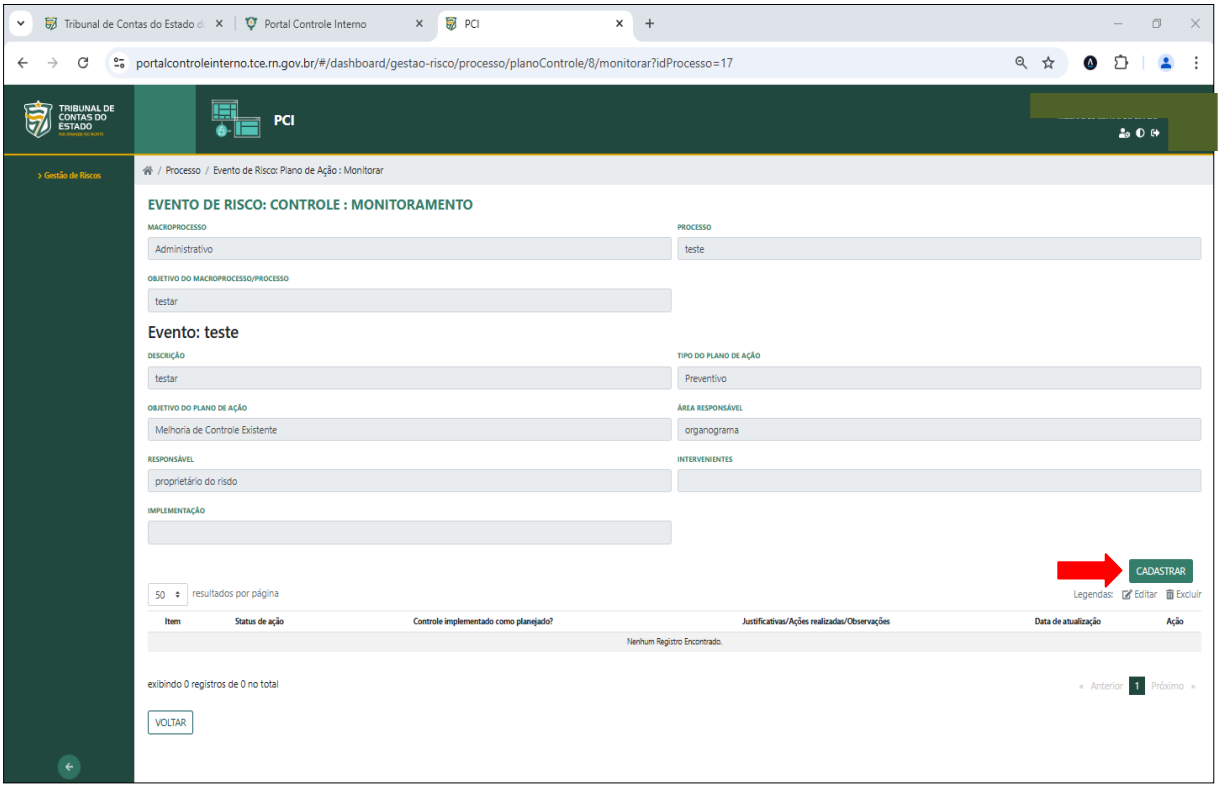
Não é despiciendo lembrar que os dados cadastrados no SIAI – GR não substituem os papéis de trabalho próprios das atividades de gerenciamento de riscos e implementação de controles. A proposta do aplicativo é auxiliar na organização das informações pertinentes, sobretudo quanto ao cálculo dos riscos tratados.

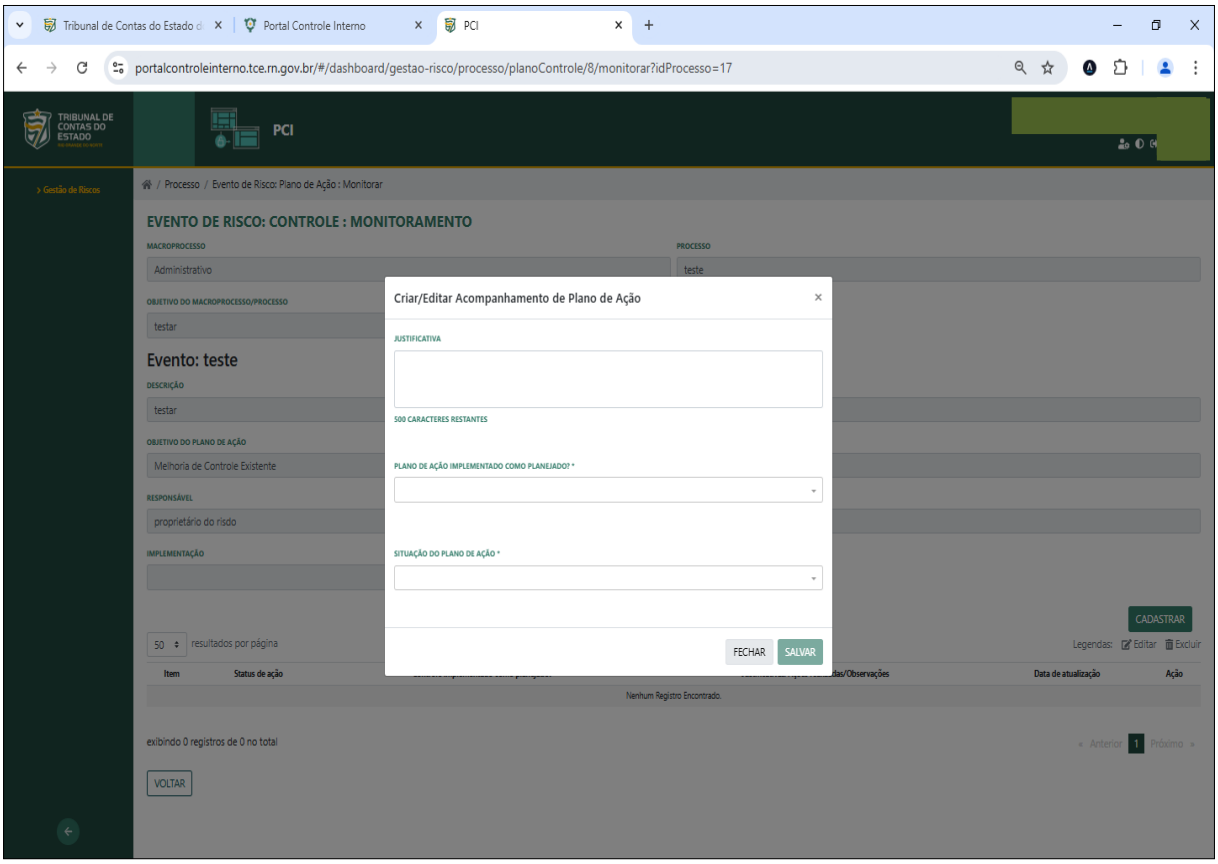
Tanto é assim que a referida caixa de diálogo apresenta campos para preenchimento com dados disponíveis sobre o plano de atividades de controle, de acordo com o estágio em que o mesmo se encontra, no momento do cadastramento, com a devida justificativa para a seleção das opções sobre a conformidade da implementação da programação e a sua situação na data do cadastramento.

O cumprimento da última etapa depende da validação, pelo supervisor, do processo de gestão de riscos cadastrado no SIAI – GR pelo analista, de acordo com os perfis de acesso disciplinados em regulamento sobre o Portal do Gestor, quanto ao modo de utilização das respectivas funcionalidades, considerando, inclusive, a distribuição de atribuições entre as diferentes linhas de defesa.

Tela 15 – Monitoramento do plano de ação

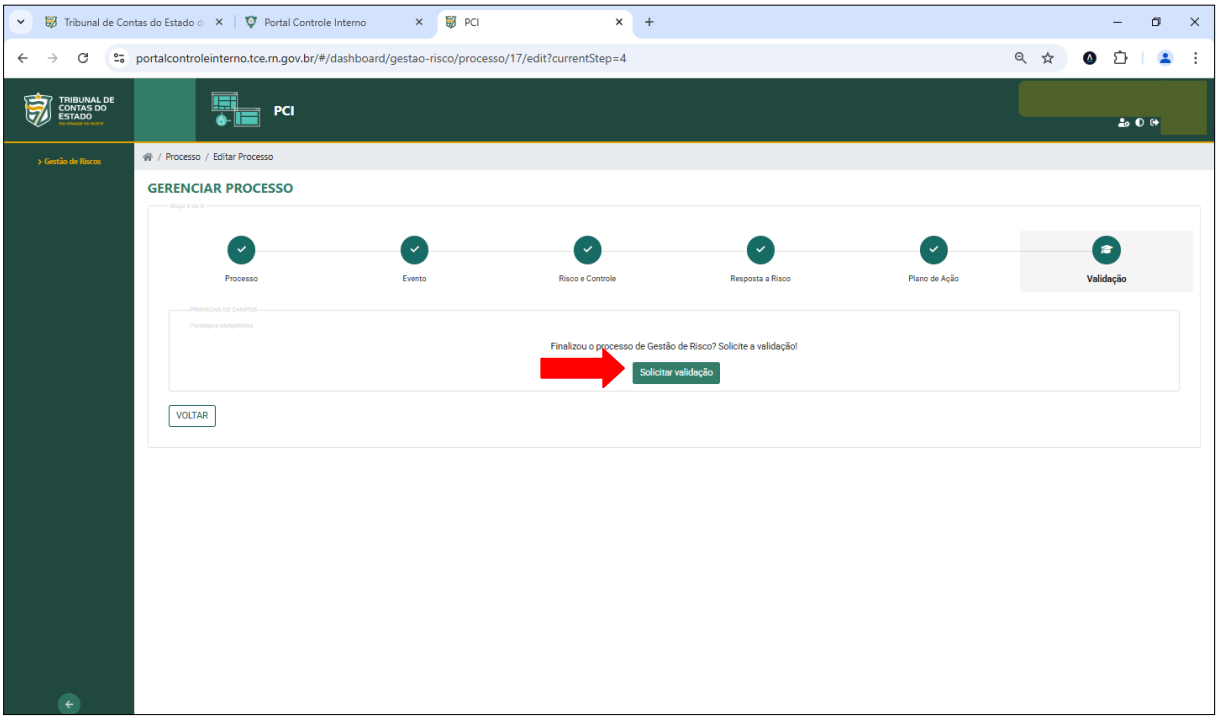


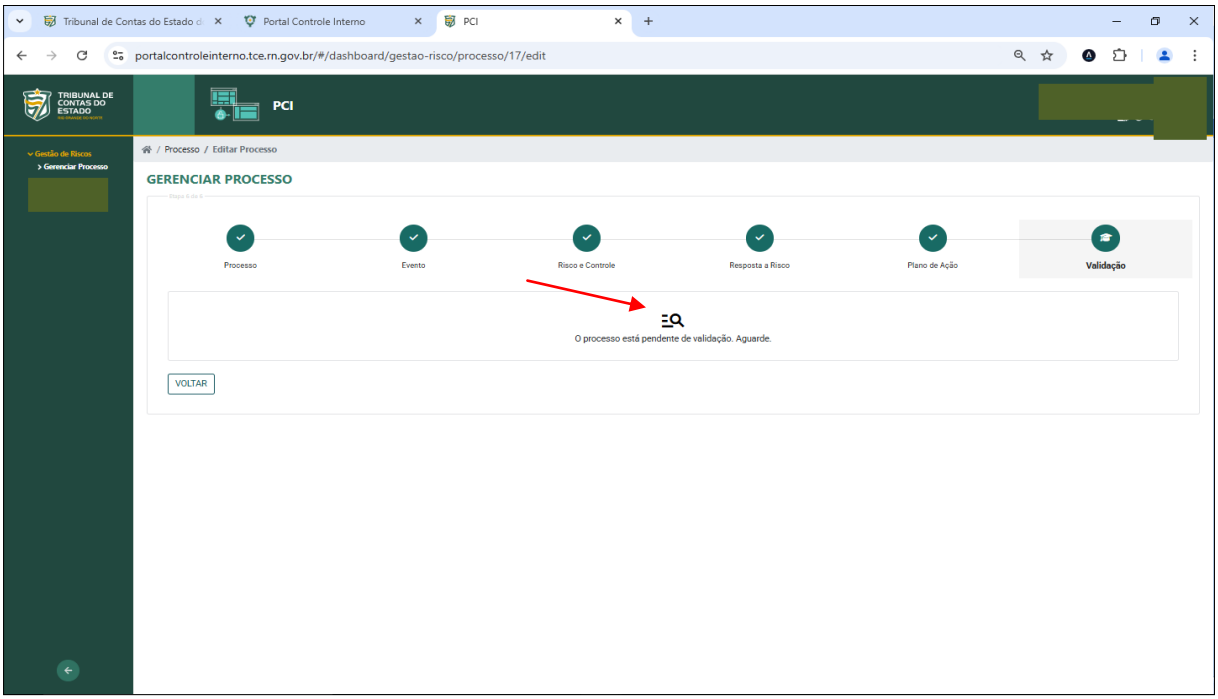




Fonte: Interface do SIAI – GR (2025).

Tela 16 – Validação do plano de ação



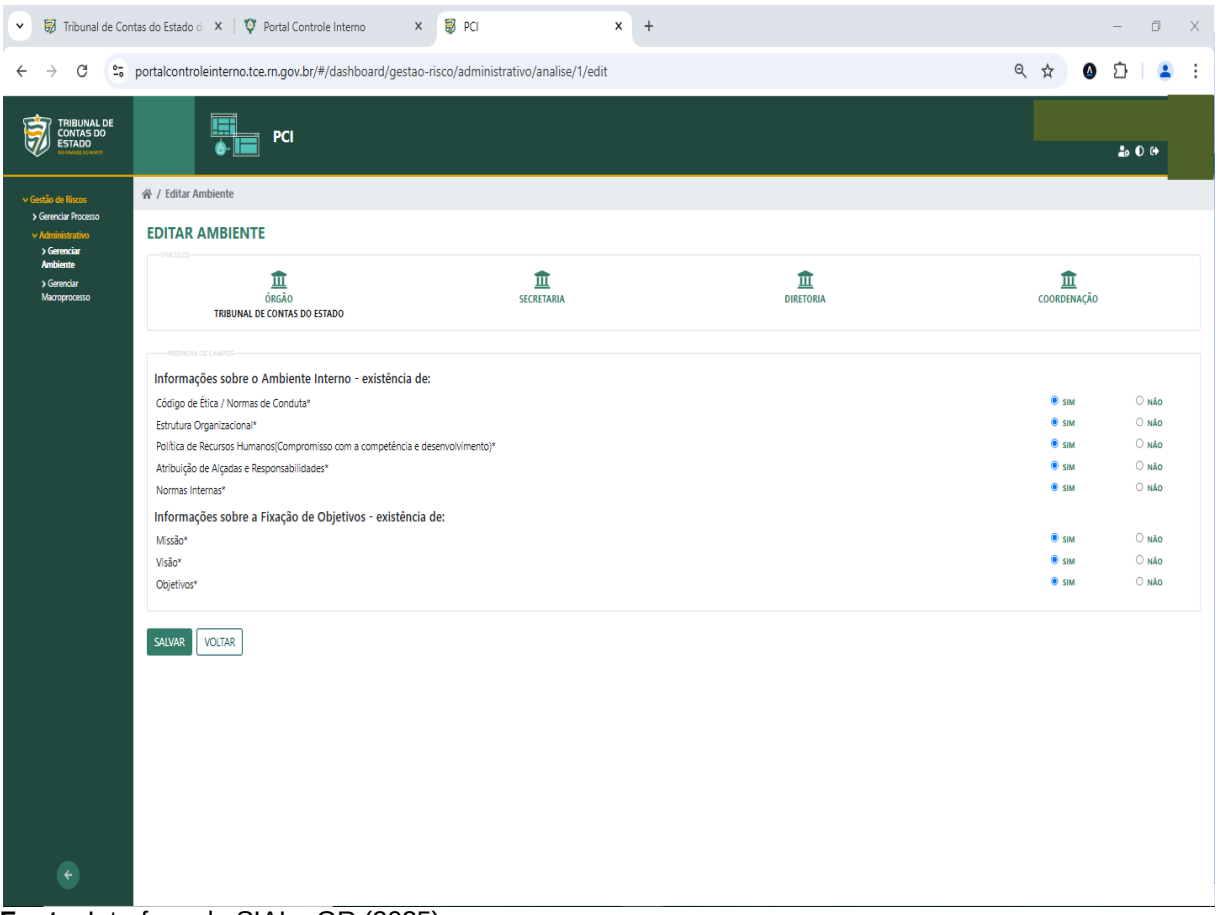


Fonte: Interface do SIAI – GR (2025).

4.7 Identidade institucional e ambiente de controle

No menu Administrativo, o usuário poderá acessar a função Gerenciar Ambiente, que permitirá visualizar uma tela para seleção de opções com respostas simples (sim ou não) sobre a definição da identidade institucional e configuração do respectivo ambiente de controle.

Tela 17 – Editar ambiente

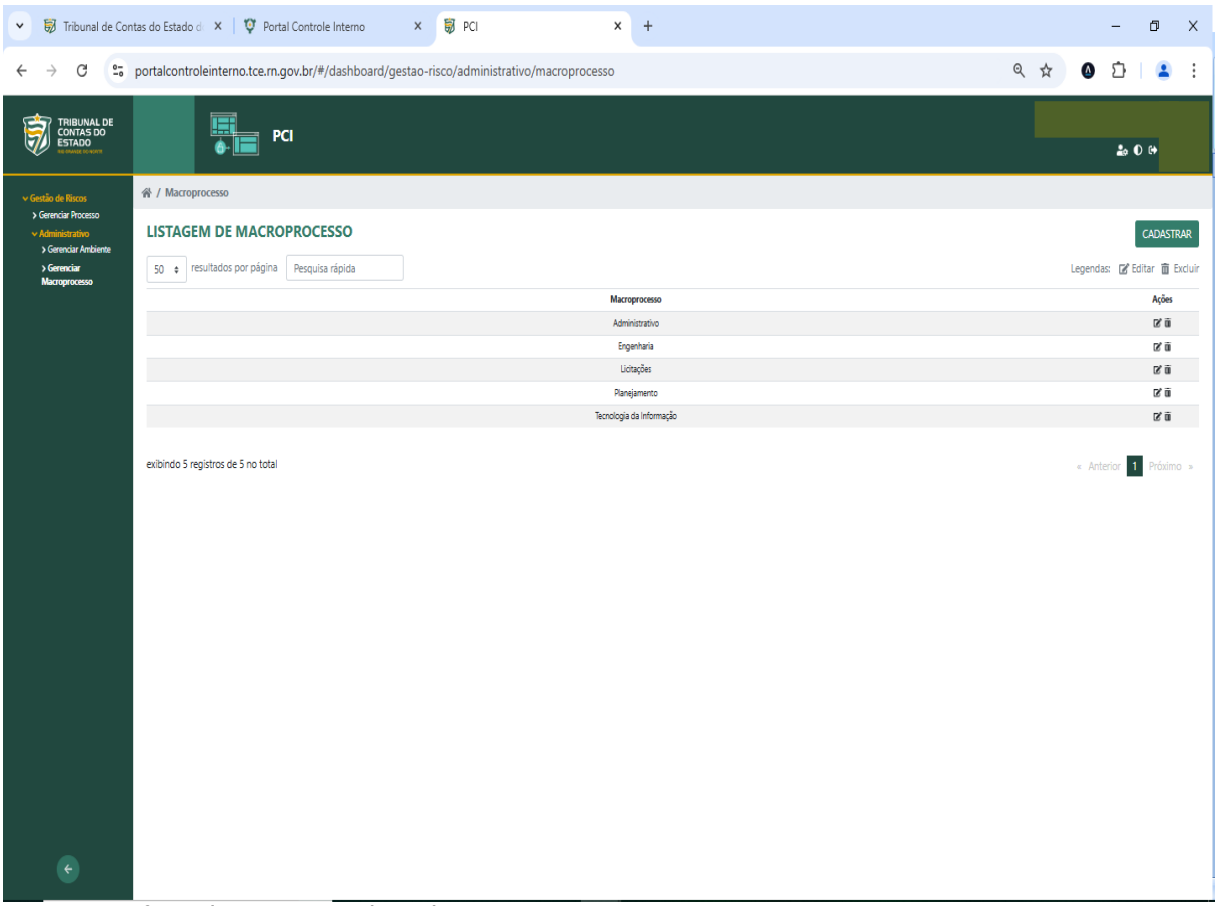


Fonte: Interface do SIAI – GR (2025).

4.8 Macroprocesso

Ainda no menu Administrativo, função Gerenciar Macroprocesso, a tela respectiva permite cadastrar os grupos de atividades estratégicas para a consecução dos objetivos institucionais ou editar macroprocessos anteriormente cadastrados.

Tela 18 – Lista de macroprocessos



Fonte: Interface do SIAI – GR (2025).

5 CONSIDERAÇÕES FINAIS

Como já foi consignado neste manual, a lógica para a realização das tarefas de cadastramento do processo de gestão de riscos é inspirada pelo *Framework COSO ERM*, cuja estrutura de componentes integrados requer a configuração de um ambiente de controle e o encadeamento de atividades propícios para fomentar um sistema de controle interno imbuído da proposta de alcançar níveis razoáveis de segurança quanto à consecução dos objetivos institucionais, a partir da internalização de uma programação continuada de avaliação de riscos, em busca de fragilidades (fraquezas internas e ameaças externas) que ensejem a provável ocorrência de eventos com potencial de prejudicar os objetivos institucionais.

Assim, para uma adequada utilização do SIAI – GR, de forma a extrair o máximo do potencial desta ferramenta de auxílio à gestão, não basta a adequação do controle interno às diretrizes estabelecidas pela Resolução nº 018/2022 – TCE.

É necessária também uma completa revisão dos processos de trabalho da organização, de forma a prepará-la para uma abordagem do controle a partir de uma política corporativa não mais sujeita a iniciativas individuais de contenção de problemas imprevistos.

O gerenciamento de riscos corporativos e a implementação de controles eficientes constitui um ciclo permanente de planejamento, execução, avaliação e, novamente, planejamento, que não pode prescindir das seguintes iniciativas:

- Definição da identidade institucional (missão, visão e valores);
- Fixação dos objetivos estratégicos para a preservação da identidade institucional;
- Mapeamento dos macroprocessos e processos institucionais necessários para a consecução dos objetivos estratégicos;
- Análise de contexto da organização, a fim de identificar capacidades e fragilidades internas, oportunidades de aperfeiçoamento e ameaças externas, situações as quais, uma vez combinadas, podem ensejar eventos potencialmente danosos à consecução dos objetivos institucionais;
- Definição das tarefas que deverão ser realizadas para alcançar os objetivos institucionais, bem como dos procedimentos e recursos financeiros e materiais que instrumentalizarão as tarefas;

- Estabelecimento das delegações de autoridade e competência e identificação dos responsáveis pela execução de cada tarefa (segregação de funções entre governança, alta administração, gerência operacional e execução);
- Determinação dos prazos para a conclusão das tarefas e das etapas respectivas (metas), para fins de controle;
- Identificação e avaliação de riscos inerentes, em termos de probabilidade (P) e impacto (I);
- Delimitação do nível de apetite a risco;
- Desenho do mapa estratégico da organização;
- Determinação do nível de confiança dos controles existentes;
- Definição do patamar de risco remanescente, após confrontar o risco identificado e avaliado (risco inerente) com a eficácia das ações de controle já existentes, o que resultará na apuração do risco residual, o qual, eventualmente, demandará novas atividades de controle;
- Implementação de respostas a eventos ainda não tratados, aprimoramento dos controles existentes ou a complementação destes instrumentos a partir da adoção de novas atividades de controle;
- Fixação de indicadores de desempenho que proporcionem maior objetividade aos procedimentos de avaliação sobre a eficácia das ações de controle empregadas;
- Monitoramento (avaliação) das atividades de controle e contínuo acompanhamento sobre a evolução dos riscos, a fim de adaptar o ambiente de controle e buscar os recursos mais adequados para preservar níveis razoáveis de segurança quanto à consecução dos objetivos estratégicos; e
- Deflagração de um novo ciclo de planejamento...

O fluxo das informações geradas no ambiente interno e coletadas do ambiente externo deve permear todos os níveis da organização e alcançar as partes interessadas, ou seja, aquelas que podem influenciar ou serem afetadas pelas atividades desempenhadas (*stakeholders*).

A comunicação institucional deve considerar o aperfeiçoamento dos relatórios financeiros, operacionais e de desempenho da gestão, bem como a elaboração de relatórios sobre o processo de gestão de riscos e monitoramento dos controles e outros instrumentos de comunicação que facilitem a tomada de decisões.

O ambiente de controle que ensejará a realização de toda esta gama de tarefas deverá estar configurado a partir da aplicação de políticas apropriadas de integridade, processamento e registro de dados, realização de investimentos, gerenciamento de recursos humanos e materiais, tecnologia e comunicação, além de contar com um arcabouço normativo que proporcione segurança jurídica para a execução das ações.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Gestão de riscos – diretrizes**. Rio de Janeiro: [s.n.], 2018.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Manual de gestão de integridade, riscos e controles internos da gestão**. Brasília: Assessoria Especial de Controle Interno, 2017.

BRASIL. Tribunal de Contas da União**. Manual de gestão de riscos do TCU / Tribunal de Contas da União**. Brasília: Secretaria de Planejamento, Governança e Gestão (Seplan), 2020.

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS. **Ágatha – Sistema de Gestão de Riscos**: manual do usuário. Departamento de Compliance e Riscos. [S.l. : s.n.], 2023.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Implementando a gestão de riscos no setor público – Módulo 1**: Introdução à gestão de riscos: estruturas de gerenciamento e bases normativas. Brasília: [s.n.], 2018.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. **Controle interno – estrutura integrada**: sumário executivo. [S.l. : s.n.], 2013.

INSTITUTO RUI BARBOSA. **Normas brasileiras de auditoria do setor público (NBASP)**: nível 1 – princípios basilares e pré-requisitos para o funcionamento dos tribunais de contas brasileiros. Belo Horizonte: [s.n.], 2015.

GLOSSÁRIO

***Accountability*:** requisito de transparência que inclui obrigações em três níveis: escrituração adequada, conformidade em relação às normas e desempenho satisfatório.

Aceitação do risco: espécie de resposta do controle interno que não demanda qualquer outra providência de mitigação, compartilhamento do risco ou descontinuidade do processo de trabalho, apresentando-se como suficiente para permitir a consecução do objetivo estratégico pretendido, dentro de uma margem de apetite a risco planejada.

Algoritmo: sequência de procedimentos definidos por instruções não ambíguas, utilizados para realizar cálculos ou solucionar problemas, a partir de uma base de dados.

Análise de contexto: meio para identificar eventos com potencial para influenciar a consecução dos objetivos estratégicos da organização, tomando como base as suas limitações e as circunstâncias exteriores contrárias ou favoráveis ao desenvolvimento institucional.

Análise *SWOT*: técnica aplicada para realizar análise de contexto sobre as capacidades de uma organização (ambiente interno) e sua relação com os fatores contrários e favoráveis à consecução dos objetivos institucionais (ambiente externo). *SWOT* constitui um acrônimo das palavras inglesas *Strengths* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) e *Threats* (ameaças), que compõem as quatro variáveis resultantes desta interação.

Apetite a risco: situação em que o patamar do risco inerente (RI) avaliado permite aceitar o risco como resposta suficiente para assegurar a consecução do objetivo estratégico pretendido.

Aplicativo: programação informática que tem por finalidade realizar tarefas específicas para o usuário.

***Backup*:** processo realizado para copiar dados em meio digital, com o objetivo de mitigar o risco de extravio de informações.

***Banner*:** meio de comunicação visual em ambiente digital, que objetiva chamar a atenção e facilitar o acesso a algum serviço ou funcionalidade disponível em rede de circulação de dados.

***Botton*:** elemento de interface gráfica para executar uma ação ou ativar uma opção.

***Browser*:** aplicação informática que permite o acesso a informações disponíveis em rede de circulação de dados.

Caixa de diálogo: interface gráfica para preenchimento de campos referentes a informações adicionais, necessárias para a conclusão da tarefa.

Campo: unidade informática para armazenamento de dados específicos, em formato de texto.

***Checkbox*:** elemento de interface gráfica que apresenta uma lista de opções para seleção.

***Compliance*:** capacidade para identificar, prevenir e tratar eventos danosos à conformidade em relação à legislação e às normas em geral, bem como à integridade em relação aos padrões éticos.

Contingenciar: apresentar resposta a evento danoso concreto, cuja intensidade não foi objeto de avaliação.

Credencial: meio de identificação e autenticação que permite o acesso a recursos ou sistemas informáticos.

Fator de risco: circunstância interna ou externa que define o indicador de probabilidade do evento potencialmente negativo.

Filtro: interface que permite a seleção de dados para a elaboração de informações adequadas ao contexto e objetivos da aplicação.

***Framework*:** estrutura, disposição ou organização que pressupõe a coerência entre os componentes de uma elaboração teórica.

Gerenciamento: revisão dos processos de trabalho da organização, com a finalidade de obter segurança razoável quanto ao alcance dos objetivos estratégicos.

Gestão: observância às diretrizes, planejamento operacional, execução, controle e divulgação de resultados.

Governança: liderança, planejamento estratégico, direção e monitoramento.

***Home*:** conteúdo inicial visualizado ao acessar um *site*.

Identidade institucional: forma de apresentação de uma organização, ou modo pelo qual a sua governança pretende que ela seja reconhecida, pela definição de sua missão (o que faz), visão (como faz) e valores (qual a sua essência).

Interface: interação entre os componentes físicos do dispositivo eletrônico e o algoritmo, parte lógica ou sequência de instruções programadas, que tem como resultado o intercâmbio de informações entre sistemas informáticos.

***Login*:** procedimento de acesso a um sistema ou recurso informático protegido, mediante o preenchimento de campos para a apresentação de dados alfanuméricos de identificação e senha.

Macroprocesso: sequência de processos ou atividades interdependentes, que abrange diferentes setores ou funções de uma organização, desencadeada para obter a consecução de um objetivo estratégico.

Menu: lista de opções ou comandos disponíveis para o usuário, em relação a um programa ou sistema informático.

Objetivo estratégico: propósito definido por uma organização, durante o planejamento das suas atividades, a fim de adequá-las à sua identidade institucional.

Perfil de usuário: nível de acesso às funcionalidades de um sistema informático.

Portal: categoria de *site* que reúne e organiza conteúdos de diferentes fontes, por área de interesse, e os apresenta ao usuário, como ponto de acesso a informações e serviços.

Processo: sequência de atividades interdependentes desencadeada para obter um resultado específico.

Proprietário do risco: corresponde, numa estrutura de gerenciamento de riscos e implementação de controles, ao gerente operacional que deve identificar, avaliar e apresentar respostas aos riscos, mantendo controles internos adequados à consecução dos objetivos estratégicos.

Risco de controle (RC): limitação do controle interno, em face dos recursos disponíveis para prevenir riscos inerentes à organização ou detectar e corrigir discrepâncias relativas aos critérios estabelecidos como padrões de qualidade. É a diferença entre o nível ideal e o real.

Risco inerente (RI): risco próprio da natureza da atividade ou dos processos de trabalho desenvolvidos pela organização.

Risco residual (RR): parcela dos riscos inerentes não tratada pelo controle interno.

***Site*:** conjunto de informações organizadas por um *browser*, interligadas e acessíveis através de protocolos de comunicação que permitem a transmissão de dados entre diferentes redes e dispositivos informáticos, que compartilham um mesmo localizador e são hospedadas por um computador que fornece dados ou aplicações em rede, compondo um meio para divulgação de produtos e serviços.

***Stakeholder*:** pessoa ou organização que pode influenciar, ser ou perceber-se influenciada, relativamente às decisões ou atividades de outra organização.

***Stepper*:** componente visual da interface de um programa informático, que auxilia na distinção das etapas ou sequências de um processo.

Tolerância a risco: situação em que o patamar do risco residual (RR) avaliado permite a consecução do objetivo estratégico pretendido.