

**IMPORTANTE:** sempre verifique no site do TJRJ se a versão impressa do documento está atualizada.

## 1 CAMPO DE APLICAÇÃO, OBJETIVO E VIGÊNCIA



Esta Rotina Administrativa (RAD) se aplica às unidades organizacionais (UOs) da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Com o objetivo de estabelecer critérios e procedimentos para a implementação, manutenção, monitoramento e revisão da gestão de riscos das unidades da (EMERJ), passando a vigorar a partir de 30/04/2024.

## 2 DEFINIÇÕES



Os termos técnicos deste documento constam no [Glossário do Sistema Integrado de Gestão do PJERJ](#).

## 3 RESPONSABILIDADE GERAIS



FUNÇÃO	RESPONSABILIDADE
Assessoria de Gestão Estratégica, da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ/ASGET)	<ul style="list-style-type: none"><li>• Fomentar práticas e estimular a cultura de gestão de riscos;</li><li>• construir e manter atualizada a metodologia de gestão de riscos na EMERJ;</li><li>• propor e manter atualizada a política de gestão de riscos;</li><li>• realizar o monitoramento e a análise crítica da estrutura de riscos dentro do escopo definido;</li><li>• acompanhar a implementação e a execução da gestão de riscos nas diversas áreas da EMERJ;</li><li>• estimular capacitações em gestão de riscos em parceria com a Escola de Administração Judiciária (ESAJ);</li><li>• fomentar o conhecimento em gestão de riscos e prestar consultoria interna nesta área;</li><li>• consolidar a situação dos riscos corporativos, a partir das informações coletadas nas auditorias de gestão da qualidade, comunicando os principais riscos à Administração Superior da EMERJ;</li></ul>

FUNÇÃO	RESPONSABILIDADE
	<ul style="list-style-type: none"> <li>• promover a melhoria contínua da gestão de riscos.</li> </ul>
Núcleo de Auditoria Interna do Tribunal de Justiça (PRES/NAI)	<ul style="list-style-type: none"> <li>• Auditar a gestão de riscos na EMERJ, conforme o detalhamento e o escopo de análise previstos no Plano Anual de Auditoria (PAA) aprovado pelo Presidente do TJ.</li> </ul>
Gestores de Risco	<ul style="list-style-type: none"> <li>• Identificar, analisar, avaliar, tratar e monitorar os riscos associados a ativos, processos de trabalho, projetos, ações e tomada de decisões, no âmbito de sua unidade;</li> <li>• assegurar a implementação das ações em resposta aos riscos e às oportunidades;</li> <li>• avaliar a eficácia e a eficiência dos controles atuais de tratamento de riscos;</li> <li>• definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos;</li> <li>• aperfeiçoar as decisões baseadas nos riscos;</li> <li>• incorporar, de forma gradativa, a gestão de riscos nas práticas e processos de gestão de sua unidade;</li> <li>• disseminar a cultura de gerenciamento de riscos na sua área, conscientizando os colaboradores sobre os riscos inerentes ao trabalho e suas responsabilidades no processo de gestão integrada de riscos;</li> <li>• comunicar sobre novos riscos inerentes ao processo.</li> </ul>
Corpo funcional da EMERJ	<ul style="list-style-type: none"> <li>• Compreender e utilizar o processo de gestão de riscos;</li> <li>• adotar postura proativa em relação à gestão de riscos na Instituição.</li> </ul>

#### 4 REFERÊNCIAS

- Instrução Normativa Conjunta MP/CGU nº 01/2016 - Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;
- Decreto nº 9.203/2017 - Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional;

- Resolução - TCU nº 287/2017 - Dispõe sobre a política de gestão de riscos do Tribunal de Contas da União e altera as Resoluções-TCU 266, de 30 de dezembro de 2014, que define a estrutura, as competências e a distribuição das funções de confiança das unidades da Secretaria do Tribunal de Contas da União; a 261, de 11 de junho de 2014, que dispõe sobre a Política de Segurança Institucional (PSI/TCU) e o Sistema de Gestão de Segurança Institucional do Tribunal de Contas da União(SGSIN/TCU) e a 247, de 7 de dezembro de 2011, que dispõe sobre a Política de Governança de Tecnologia da Informação do Tribunal de Contas da União;
- Associação Brasileira de Normas Técnicas - ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes;
- Associação Brasileira de Normas Técnicas – ABNT NBR ISO 31010 – Gestão de Riscos – Técnicas para o processo de avaliação de Riscos;
- Plano de Gestão de Riscos do Tribunal de Justiça do Estado do Rio de Janeiro.

## 5 DIRETRIZES GERAIS PARA A GESTÃO DE RISCOS DA EMERJ

### 5.1 A gestão de risco na EMERJ tem como objetivos:

- a) auxiliar a tomada de decisão com vistas a prover razoável segurança no atingimento dos objetivos da Instituição;
- b) atentar para a necessidade de se identificar e tratar riscos na EMERJ;
- c) facilitar a identificação de oportunidades e ameaças;
- d) prezar pelas conformidades legais e normativas dos processos organizacionais;
- e) melhorar a eficácia e eficiência operacional;
- f) melhorar a aprendizagem organizacional;
- g) aumentar a capacidade da organização de se adaptar a mudanças.

**5.2** A gestão de riscos está integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional da Instituição, sendo aplicável aos processos de trabalho, projetos, ações e tomada de decisões na EMERJ.

**5.3** Conforme a Política de Riscos da EMERJ, são os seguintes princípios que regem a gestão de riscos na Instituição:

- a) criação e proteção dos valores institucionais;

- b) integração de todos os processos organizacionais;
- c) participação na tomada de decisões;
- d) abordagem explícita da incerteza;
- e) sistematização, estruturação e pertinência;
- f) fundamentação nas melhores informações disponíveis;
- g) alinhamento ao contexto e ao perfil de riscos da Instituição;
- h) consideração dos fatores humanos e culturais;
- i) transparência e inclusão;
- j) dinamismo, interatividade e capacidade de reagir a mudanças; e
- k) facilitação da melhoria contínua da organização.

**5.4** Para realizar a gestão de riscos em qualquer UO da EMERJ, as seguintes etapas devem ser seguidas:

- a) análise do contexto organizacional e determinação dos processos de trabalho para avaliação e tratamento dos riscos;
- b) identificação dos eventos de risco;
- c) análise e avaliação dos riscos;
- d) tratamento dos riscos;
- e) monitoramento;
- f) comunicação.

**5.5** As unidades da EMERJ, ao elaborarem a gestão de riscos, devem considerar as seguintes categorias:

- a) estratégicos: os associados à tomada de decisão que possam afetar negativamente o alcance dos objetivos da organização;
- b) operacionais: os associados à ocorrência de perdas (produtividade, ativos e orçamento) resultantes de falhas, deficiências ou inadequação de processos internos, estrutura, pessoas, sistemas, tecnologia, assim como os provenientes de eventos externos (catástrofes naturais, greves, fraudes).

**5.5.1** Para a análise dos riscos estratégicos, são consideradas a análise do contexto organizacional e as partes interessadas.

**5.5.2** Para a análise dos riscos operacionais, são considerados os objetivos dos processos de trabalho da unidade e considerados como riscos, os efeitos da incerteza nos objetivos dos processos.

## **6 ANÁLISE DO CONTEXTO ORGANIZACIONAL**

**6.1** A análise do contexto organizacional tem a finalidade de colher informações para apoiar a identificação de eventos de risco estratégico, bem como contribuir para a escolha de ações mais adequadas para assegurar o atingimento da missão.

**6.1.1** É atualizada ou validada a cada semestre pela Administração Superior com a participação dos gestores da unidade que detêm o conhecimento estratégico da organização e têm condições de mapear os fatores externos e internos.

**6.2** A análise do contexto organizacional diz respeito à análise dos ambientes externos e internos da unidade e das partes interessadas, que influenciam o propósito, os objetivos e a sustentabilidade da organização.

**6.2.1** Para análise dos ambientes externos e internos e das partes interessadas, deve ser utilizado o FRM-EMERJ-045-01 – Análise do Contexto Organizacional.

**6.2.2** Para identificação dos ambientes externos – oportunidade e ameaça - e dos ambientes internos - força e fraqueza - é utilizada a ferramenta SWOT, que auxilia na análise dos cenários.

**6.2.2.1** A análise SWOT é realizada com foco na missão e visa a obtenção de informações para apoiar a identificação dos eventos de risco estratégico.

**6.2.3** Após a análise dos ambientes externos e internos da unidade, é realizada a análise de pertinência dos ambientes apresentados, somente as fraquezas e as ameaças, para que seja dada prioridade aos fatores mais importantes e relevantes para o propósito da unidade e para identificação dos riscos estratégicos.

**6.2.3.1** O tratamento das oportunidades será abordado em item próprio.

**6.2.4** A pertinência dos ambientes é determinada em relação à missão da unidade e ao seu usuário, com a utilização de escala qualitativa de pertinência, com intensidade baixa (1), média (2), alta (3) e muito alta (4).

**6.2.5** A pertinência total é definida com base no produto da pertinência à missão da organização x pertinência ao usuário, com amplitude de 4 níveis:

LEGENDA	PONTUAÇÃO
Baixa pertinência	1 a 3
Média pertinência	4 a 6
Alta pertinência	8 a 9
Altíssima pertinência	12 a 16

- 1 a 3 – Baixa pertinência – fator pouco relevante ao propósito da unidade;
- 4 a 6 – Média pertinência – fator relevante ao propósito da unidade;
- 8 a 9 – Alta pertinência – fator com alta relevância ao propósito da unidade;
- 12 a 16 – Altíssima pertinência – fator com altíssima relevância que compromete totalmente o propósito da unidade.

## 7 IDENTIFICAÇÃO DOS EVENTOS DE RISCO



**7.1** Eventos são situações em potencial, que ainda não ocorreram, que podem causar impacto na consecução dos objetivos da organização. Podem ser positivos ou negativos; os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

**7.2** Esta etapa tem por finalidade reconhecer e descrever os eventos de riscos que possam impedir que uma unidade alcance seus objetivos, convém que seja atualizada ou validada pelos gestores a cada semestre.

**7.3** A identificação dos eventos de risco deve levar em conta a análise dos ambientes externos e internos, fraquezas e ameaças, e os objetivos dos processos de trabalho.

**7.3.1** Para auxílio no desenvolvimento da identificação dos eventos de risco, é apresentada, a seguir, a seguinte estrutura:

- Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DA CONSEQUÊNCIA> impactando no <OBJETIVO DO PROCESSO>.

**7.3.2** Recomenda-se que, para a identificação dos riscos operacionais, sejam considerados todos os processos de trabalho da unidade e seus objetivos.

**7.4** Informações pertinentes, apropriadas e detalhadas são importantes para a identificação dos eventos de risco, portanto, deve-se buscar a participação dos colaboradores que conheçam bem os processos a serem analisados.

**7.5** Para identificação do evento de risco, é utilizado o FRM-EMERJ-045-02 – Análise de Riscos.

## **8 ANÁLISE E AVALIAÇÃO DOS EVENTOS DE RISCOS**

**8.1** Esta etapa tem por finalidade analisar e avaliar os eventos de risco identificados, buscando a compreensão de sua natureza e suas características, incluindo o nível de severidade do risco, a partir de critério de probabilidade e impacto.

**8.2** A análise de risco envolve a consideração detalhada da incerteza, fontes de risco, consequência, probabilidade, impacto e nível de severidade.

**8.3** A fonte de risco corresponde à origem dos riscos podendo envolver pessoas, processos de trabalho, sistema ou tecnologia, infraestrutura (física ou organizacional) e eventos externos (não diretamente gerenciáveis).

**8.4** A consequência refere-se ao resultado ou efeito negativo do acontecimento do evento de risco para o propósito da organização, e caso seja um risco operacional, para o processo de trabalho.

**8.5** Para a etapa de avaliação do risco, são considerados a probabilidade e o impacto do evento de risco.

**8.6** A probabilidade é a chance de o evento de risco ocorrer e é determinada com a utilização de escala quantitativa com amplitude de cinco níveis, a saber:

- 1 – Muito baixa probabilidade – Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência. Ocorre apenas em situações excepcionais;
- 2 – Baixa probabilidade – o evento pode correr, porém o histórico conhecido aponta para baixa frequência de ocorrência. Raramente ocorre;
- 3 – Média probabilidade – há indícios que o evento possa ocorrer em algum momento ou se repete com frequência razoável;
- 4 – Alta probabilidade – o evento provavelmente ocorrerá, pois, as circunstâncias indicam fortemente essa possibilidade. Sua frequência é elevada;
- 5 – Muito alta probabilidade – ocorrência praticamente certa do evento, pois as circunstâncias indicam claramente essa possibilidade.

**8.7** O impacto mede o potencial comprometimento dos objetivos e resultados da unidade e tem relação direta com as consequências da ocorrência do risco.

**8.8** O impacto é determinado com a utilização de escala quantitativa com amplitude de cinco níveis, a saber:

- 1 – Muito baixo impacto – Compromete minimamente o alcance dos objetivos e resultados. Mínimo impacto;
- 2 – Baixo impacto – Compromete em pequena medida o alcance dos objetivos e resultados. Pequeno impacto;
- 3 – Médio impacto – Razoável comprometimento no alcance dos objetivos e resultados. Moderado impacto;
- 4 – Alto impacto – Significativo comprometimento no alcance dos objetivos e resultados com difícil reversão. Significativo impacto;
- 5 – Muito alto impacto – Compromete totalmente o alcance dos objetivos e resultados. Irreversível impacto.

**8.9** A severidade, nível de risco, é determinada pela multiplicação da probabilidade e impacto, com amplitude de quatro níveis, a saber:

- 1 e 4 – Baixo risco;
- 5 a 10 – Médio risco;
- 12 a 16 – Alto risco;
- 20 a 25 – Altíssimo risco.

Abaixo, a matriz de risco que representa os possíveis resultados da combinação das escalas de probabilidade e impacto:

			PROBABILIDADE				
			1	2	3	4	5
			Muito Baixa	Baixa	Média	Alta	Muito Alta
IMPACTO	5	Muito Alto	5	10	15	20	25
	4	Alto	4	8	12	16	20
	3	Médio	3	6	9	12	15
	2	Baixo	2	4	6	8	10
	1	Muito Baixo	1	2	3	4	5

**8.10** Os riscos cujos níveis se encontram na faixa de médio, alto e altíssimo devem ser tratados e controlados pela unidade.

**8.10.1** Cabe ao gestor, diante das listas de riscos ordenados por seus níveis, decidir se aqueles que se encontram na faixa de baixo risco, merecem ações mitigadoras ou podem ser aceitos sem necessidade de ações de controle e/ou plano de contingência.

**8.10.2** Recomenda-se que, nos casos de um impacto alto ou muito alto, os riscos sejam mitigados com ações de controle e plano de contingência.

**8.11** Para análise e avaliação do evento de risco, é utilizado o FRM-EMERJ-045-02 - Análise de Riscos.

## 9 TRATAMENTO DOS RISCOS

**9.1** O propósito do tratamento de riscos é decidir qual é a resposta ao risco, determinar e implementar opções para abordar riscos, com ações de controle e de contingência.

**9.2** Selecionar as opções mais apropriadas de tratamento de riscos envolve balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação.

**9.3** Conhecido o nível do risco, verifica-se qual estratégia a ser adotada para responder ao evento de risco.

- 9.4** A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecidos em confronto com a avaliação que se fez do risco.
- 9.5** Para resposta ao risco, temos as seguintes opções:
- Evitar o risco – Tem como objetivo eliminar a causa raiz do risco, implementando ações para levar a probabilidade do risco a zero. Pode tratar de suspensão ou eliminação de atividades que dão origem ao risco;
  - Compartilhar o risco – Redução da probabilidade ou do impacto pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas mais comuns compreendem a aquisição de produtos de seguro ou terceirização de uma atividade;
  - Aceitar o risco – Nos casos em que o risco se encontre no nível baixo;
  - Mitigar o risco – Adoção de procedimentos de controle para minimizar o impacto ou reduzir a probabilidade de ocorrência.
- 9.6** As ações de controle são medidas preventivas, definidas de acordo com a resposta ao risco escolhida pelo gestor e são implementadas para manterem ou modificarem o risco, com objetivo de reduzir os níveis de probabilidade e impacto.
- 9.6.1** As ações de controle devem ser imediatas e/ou tempestivas e pertinentes ao risco identificado. Ações que dependam de variáveis relacionadas a outras unidades do PJERJ e que demandem tempo para sua implementação devem ser evitadas no intuito de não terem eficácia para mitigar o risco.
- 9.6.2** Deve-se avaliar a necessidade de melhorar ou manter as ações de controle já existentes para tratar o evento de risco identificado, sob a ótica de custo/benefício com o objetivo de otimizá-las.
- 9.6.3** As ações de controle devem ser detalhadas e completas de modo que demonstrem eficácia para o tratamento do evento do risco e, caso necessário, novos controles devem ser propostos como, por exemplo, controles automatizados em substituição aos manuais ou alterações em rotinas administrativas para melhor monitoramento dos processos organizacionais.
- 9.6.4** Caso haja necessidade de se estruturar os novos controles para tratarem o evento de risco, um plano de ação é recomendado.

**9.7** Plano de contingência é o planejamento emergencial e alternativo para atuação durante a ocorrência do risco determinado. Visa prover a unidade de procedimentos e responsabilidades com objetivos de orientar as ações durante o evento indesejado.

**9.7.1** A unidade deve determinar as ações a serem tomadas, em que momento tomar, como realizar os procedimentos necessários, quais responsáveis e outras informações necessárias para que a implementação do plano de contingência seja eficaz e minimize os impactos da ocorrência do evento indesejável.

**9.7.2** Deve-se fornecer treinamento inicial sobre o plano de contingência e manter todos os envolvidos atualizados sobre as mudanças.

**9.8** Para tratamento dos riscos, é utilizado o FRM-EMERJ-045-02 - Análise de riscos.

## 10 COMUNICAÇÃO



**10.1** Comunicação do risco diz respeito ao fornecimento de informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco, sob pena de sua ocorrência plena.

**10.1.1** A comunicação busca promover a conscientização e o entendimento do risco.

**10.2** A comunicação visa:

- reunir diferentes áreas de especialização para cada etapa do processo de gestão de riscos;
- assegurar que pontos de vista diferentes sejam considerados apropriadamente ao se definirem critérios de risco e ao se avaliarem os riscos;
- fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisão;
- construir um senso de inclusão e propriedade entre os afetados pelo risco.

**10.3** A direção da UO como também o gestor de risco pode acionar o ASGET para orientações técnicas relativas à gestão de riscos.

## 11 MONITORAMENTO



**11.1** Monitoramento compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos.

**11.2** O monitoramento deve atuar em dimensões:

- no funcionamento do processo de gestão de risco da EMERJ e análise crítica da estrutura de risco;
- na implementação e nos resultados do tratamento dos riscos;
- na evolução do nível dos riscos que não merecem tratamento por parte do gestor.

**11.3** A avaliação do funcionamento do processo de gestão de risco na EMERJ está a cargo do NAI.

**11.4** O monitoramento das ações de tratamento de riscos está a cargo do gestor de risco e compreende a verificação contínua ou periódica da eficácia da implementação e dos resultados das ações de controle.

**11.5** Para o monitoramento do tratamento de riscos, a direção da unidade responsável pelo processo avaliado e o gestor de risco devem:

- a) garantir que os controles sejam eficazes e eficientes;
- b) analisar as ocorrências dos riscos;
- c) detectar mudanças que possam requerer revisão dos controles;
- d) identificar riscos emergentes.



## **12 TRATAMENTO DAS OPORTUNIDADES**

**12.1** As oportunidades são encontradas no momento da análise de contexto realizada pela organização, conforme apresentado no capítulo 6 – Análise do Contexto Organizacional.

**12.2** Para tratamento das oportunidades, temos as seguintes opções:

- Explorar a oportunidade – Tem como objetivo garantir que a oportunidade seja concretizada. Todos os recursos disponíveis são colocados para aproveitá-la.
- Melhorar a oportunidade – Tem como objetivo facilitar as possibilidades que a oportunidade aconteça. Identificar e maximizar os principais impulsionadores desse risco positivo pode aumentar sua probabilidade de ocorrência e ou seu impacto.
- Compartilhar a oportunidade – Tem como objetivo unir-se a terceiros com qualificação para capturar a oportunidade em benefício da parceria.
- Aceitar a oportunidade – Quando não é possível adotar nenhuma das opções anteriores e, dessa forma, decide-se não tomar ações para abordá-la. Entretanto, a oportunidade que,

momentaneamente, foi aceita, pode, futuramente, ser explorada, melhorada ou compartilhada. Por isso, a importância de um eficaz monitoramento no contexto organizacional da unidade.

**12.2.1** Quando aplicável, é elaborado um plano de ação para a execução das ações necessárias ao tratamento proposto pela unidade.

**12.3** Para unidade certificada pela ISO 9001, deve ser considerada, em sua análise crítica, a eficácia das ações tomadas para abordar as oportunidades.



### 13 GESTÃO DA INFORMAÇÃO DOCUMENTADA

**13.1** As informações deste processo de trabalho são geridas pela UO e mantidas em seu arquivo corrente, de acordo com a tabela de gestão da informação documentada apresentada a seguir:

IDENTIFICAÇÃO	CÓDIGO CCD*	RESPON-SÁVEL	ACESSO	ARMAZE-NAMENTO	RECUPE-RAÇÃO	PROTEÇÃO	RETENÇÃO (ARQUIVO CORRENTE - PRAZO DE GUARDA NA UO**)	DISPOSIÇÃO
Análise do Contexto Organizacional - FRM-EMERJ-045-01	0-1c	ASGET	Irrestrito	Pasta	RAD	Condições Apropriadas	2 anos	Eliminação na UO
Análise de Risco - FRM-EMERJ-045-02	0-1c	ASGET	Irrestrito	Pasta	RAD	Condições Apropriadas	2 anos	Eliminação na UO

Legenda:

\*CCD = Código de Classificação de Documentos.

\*\*UO = Unidade Organizacional.

\*\*\* SGADM/DEGEA = Departamento de Gestão de Acervos Arquivísticos, da Secretaria-Geral de Administração.

Notas:

- a) Eliminação na UO – procedimento – Organizar os Arquivos Correntes das Unidades Organizacionais.
- b) SGADM/DEGEA – procedimentos – Arquivar e Desarquivar Documentos no DEGEA; Avaliar, Selecionar e Destinar os Documentos do Arquivo Intermediário e Gerir Arquivo Permanente.
- c) Os dados lançados no Sistema Corporativo são realizados por pessoas autorizadas e recuperados na UO. O armazenamento, a proteção e o descarte desses dados cabem à Secretaria-Geral de Tecnologia da Informação -SGTEC, conforme RAD-SGTEC-021 – Elaborar e Manter Rotinas de Armazenamento de Segurança dos Bancos de Dados e Servidores de Aplicação.



**Base Normativa:** Ato Executivo nº 2.950/2003



**Proposto por:** Representante da Administração Superior (RAS)



**Aprovado por:** Secretária da Secretaria-Geral (SECGE)

14 ANEXO DIAGRAMA DO PROCESSO DE GESTÃO DE RISCOS

ANEXO 1 – DIAGRAMA PROCESSO DE GESTÃO DE RISCOS

