**Tribunal de Justiça do Estado do Tocantins**

**MANUAL DE METODOLOGIA DE GESTÃO DE RISCOS**

**CONTROLE DE VERSÃO**

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA** | **VERSÃO** | **ANOTAÇÕES** | **RESPONSÁVEL** |
| 18/05/2021 | v.1 | AprovaçãoATA SEI 19.0.000024429-8 - Evento 3722344 | Comitê Gestão de Riscos - CGRIS |
|  |  |  |  |

TRIBUNAL DE JUSTIÇA DO TOCANTINS

Desembargador JOÃO RIGO GUIMARÃES

**Presidente**

Desembargador PEDRO NELSON DE MIRANDA COUTINHO

**Vice Presidente**

Desembargadora ETELVINA MARIA SAMPAIO FELIPE

**Corregedora**

Desembargadora ÂNGELA MARIA RIBEIRO PRUDENTE

**Vice Corregedora**

JONAS DEMOSTENE RAMOS

**Diretor Geral**

|  |  |
| --- | --- |
| **DIRETORES**Ronilson Pereira da SilvaDiretor Administrativo Gizelson Monteiro de Moura Diretor Financeiro José Sebastião Pinheiro de Souza Diretor do Centro De Comunicação Social Ernandes Rodrigues da Silva Diretor de Tecnologia da Informação Wallson Brito da Silva Diretor Judiciário Antônio José Ferreira de Rezende Diretor de Gestão de Pessoas Rogério José Canalli Diretor de Infraestrutura e Obras Ana Beatriz de Oliveira Pretto Diretora Executiva da ESMAT  | **COMITÊ DE GESTÃO DE RISCOS**Océlio Nobre da Silva - CoordenadorJonas Demostene RamosKênia Cristina de OliveiraJoão Ornato Benigno BritoJeane Silva Justino FilhoVinicius Fernandes BarbozaElizabeth Maria Lima Barbosa PugliesiJosé Atílio BeberDanillo Lustosa Wanderley**EQUIPE DE APOIO**Ana Carina Mendes SoutoAgnes Souza da RosaGizelson Monteiro de MouraJúlio César Pereira de OliveiraPaulo Vitor Gutierrez de OliveiraRoger Freitas Nascimento |

# APRESENTAÇÃO

Calcular risco é uma atividade antiga executada pela humanidade. No entanto, em sua maioria, foi executada de forma empírica e não sistematizada.

A tecnologia moderna, com desenvolvimento acelerado, fez com que o mundo empresarial e os órgãos públicos passassem a utilizar meios de análise e controle dos riscos inerentes as suas atividades, de forma ordenada e documentada.

Adotar a análise de riscos é uma quebra de paradigma que, como em qualquer mudança, precisa ser trabalhada para que as resistências sejam minimizadas e a sua implantação seja otimizada. Anota-se que os órgãos de controle vêm sistematicamente cobrando sua implantação.

Os processos de trabalho e o uso de alguns ativos envolvem algum tipo de risco. Logo, a consciência de sua existência e a capacidade de administrá-los, associadas à disposição de correr riscos e de tomar decisões, é indispensável. O Tribunal tem que gerenciar as ameaças de modo a mantê-las em níveis aceitáveis e aproveitar as oportunidades.

O desafio é determinar o nível de incerteza que o Tribunal está preparado a aceitar, na medida em que se empenha em ampliar e aperfeiçoar os serviços aos jurisdicionados.

Por fim, a presente metodologia, na forma de manual, busca facilitar a compreensão e tornar essa atividade acessível e descomplicada e está obedecendo a Política de Gestão de Riscos aprovada pelo Poder Judiciário.

**Desembargador João Rigo Guimarães**

PRESIDENTE

Sumário

[1. APRESENTAÇÃO 4](#_Toc80359118)

[2. INTRODUÇÃO 7](#_Toc80359119)

[3. GESTÃO DE RISCOS 7](#_Toc80359120)

[4. OBJETIVOS 7](#_Toc80359121)

[5. ESTRUTURA E RESPONSABILIDADES DA GESTÃO DE RISCOS 8](#_Toc80359122)

[5.1. Tribunal Pleno 9](#_Toc80359123)

[5.2. Presidente 9](#_Toc80359124)

[5.3. Líderes do Planejamento Estratégico 9](#_Toc80359125)

[5.4. Diretor Geral 9](#_Toc80359126)

[5.5. Diretoria de Controle Interno 9](#_Toc80359127)

[5.6. Coordenadoria de Gestão Estratégica, Estatística e Projetos 9](#_Toc80359128)

[5.7. Comitê de Gestão de Riscos 10](#_Toc80359129)

[5.8. Gestor de Riscos 10](#_Toc80359130)

[5.9. Matriz RACI para as atividades do processo de gestão de riscos 10](#_Toc80359131)

[6. PROCESSO DE GESTÃO DE RISCOS 11](#_Toc80359132)

[6.1. Processo de Gestão de Riscos no Poder Judiciário do Tocantins - PJTO 12](#_Toc80359133)

[6.1.1 Definição do contexto 14](#_Toc80359134)

[6.1.2 Estabelecimento do contexto interno e externo 14](#_Toc80359135)

[6.1.3 Contexto Geral 14](#_Toc80359136)

[6.1.4 Contexto Específico 15](#_Toc80359137)

[6.2. Mapear processos e ativos 16](#_Toc80359138)

[6.3. Identificação de riscos 16](#_Toc80359139)

[6.4. Análise de riscos 18](#_Toc80359140)

[6.5. Avaliação de Riscos 19](#_Toc80359141)

[6.5.1 Matriz “Apetite a Risco” 20](#_Toc80359142)

[6.6. Tratamento de Riscos 20](#_Toc80359143)

[6.7. Plano de Tratamento de Riscos 22](#_Toc80359144)

[6.8. Comunicação e Consulta 23](#_Toc80359145)

[6.9. Monitoramento e Análise Crítica 24](#_Toc80359146)

[7. CONSIDERAÇÕES FINAIS 25](#_Toc80359147)

[8. TERMOS E DEFINIÇÕES 25](#_Toc80359148)

[9. REFERÊNCIAS 26](#_Toc80359149)

[10. ANEXOS 28](#_Toc80359150)

[10.1. ANEXO I Modelo de Relatório de Contextualização 28](#_Toc80359151)

[10.2. ANEXO II Modelo de Matriz de Identificação de Riscos 29](#_Toc80359152)

[10.3. ANEXO III Modelo de Matriz de Análise e Avaliação de Riscos 30](#_Toc80359153)

[10.4. ANEXO IV Modelo de Relatório de Avaliação de Riscos 31](#_Toc80359154)

[10.5. ANEXO V Modelo de Matriz de Priorização dos Riscos 33](#_Toc80359155)

[10.6. ANEXO VI Modelo de Plano de Tratamento de Riscos 34](#_Toc80359156)

[10.7. ANEXO VII Modelo de Formulário de Comunicação e Consulta 35](#_Toc80359157)

[10.8. ANEXO VIII Modelo de Relatório de Monitoramento e Análise Crítica 36](#_Toc80359158)

[10.9. ANEXO IX Mapa de Risco 37](#_Toc80359159)

[10.10. ANEXO X Fluxo do Processo de Trabalho da Gestão de Riscos do PJTO 38](#_Toc80359160)

[10.11. ANEXO XI - Atividades do Processo de Gestão de Riscos 39](#_Toc80359161)

Lista de Figuras

[**Figura 1** – Organograma estrutura Gestão de Riscos 8](#_Toc80359203)

[**Figura 2** - Matriz RACI 11](#_Toc80359204)

[**Figura 3** - Processo de Gestão de Risco 12](#_Toc80359205)

[**Figura 4** - Processo de gestão de riscos em forma de mapa mental 13](#_Toc80359206)

[**Figura 5** - Resumo comparativo de normas 13](#_Toc80359207)

[**Figura 6** - Contexto Interno e Externo 15](#_Toc80359208)

[**Figura 7** - Modelo Matriz SWOT 16](#_Toc80359209)

[**Figura 8** - Elementos do risco 17](#_Toc80359210)

[**Figura 9** - Passos para identificação de riscos 17](#_Toc80359211)

[**Figura 10** - Exemplo de identificação de riscos e levantamento de controle 17](#_Toc80359212)

[**Figura 11** - Escala de probabilidade de ocorrência de uma ameaça 18](#_Toc80359213)

[**Figura 12** - Escala de Impacto da ocorrência 18](#_Toc80359214)

[**Figura 13** - Escala de Impacto nas dimensões do objetivo 18](#_Toc80359215)

[**Figura 14** - Matriz de impacto x probabilidade 19](#_Toc80359216)

[**Figura 15** - Escala de classificação de risco 19](#_Toc80359217)

[**Figura 16** - Exemplo de Matriz de Análise e Avaliação de Riscos 19](#_Toc80359218)

[**Figura 17** - Critérios para priorização e tratamento de riscos 20](#_Toc80359219)

[**Figura 18** - Matriz de Apetite a Risco 20](#_Toc80359220)

[**Figura 19** - Estratégia de resposta aos riscos 21](#_Toc80359221)

[**Figura 20** - Exemplo de matriz de priorização de riscos 21](#_Toc80359222)

[**Figura 21** - Exemplo de Plano de Tratamento de Riscos 23](#_Toc80359223)

[**Figura 22** - Exemplo de Comunicação e Consulta 24](#_Toc80359224)

[**Figura 23** - Avaliação dos controles 24](#_Toc80359225)

[**Figura 24** - Apuração do risco residual 25](#_Toc80359226)

# INTRODUÇÃO

A gestão de riscos ainda não está consolidada no setor público. Diversas são as dificuldades para sua implantação. A dificiência de mão de obra especializada e a dificuldade em passar a relevância desses conceitos aos gestores fazem com que a gestão de riscos não tenha o avanço desejado.

O objetivo principal da gestão de riscos é diminuir o grau de incertezas na condução dos projetos, atividades, processos de trabalho e ativos e assim aumentar o grau de eficiência e eficácia das ações realizadas. Contribuindo com essa premissa foi aprovada a Emenda Constitucional nº 19, de 1998, que acrescentou o conceito da eficiência no rol dos princípios que regem toda a administração pública federal (CF, art. 37, *caput*).

Em 2017 foi editado o Decreto Federal nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, que trata, entre outros temas, em seu artigo 17 que *“A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional”*

Em 2018 o TCU dá um grande passo e publica o Manual de Gestão de Riscos, que tem por objetivo orientar os gestores do TCU na gestão dos riscos organizacionais do Tribunal. Mas o alcance dessa publicação é bem maior, pois pode servir de norte para as demais Instituições Públicas. É um documento de fácil compreensão e, pela simplicidade, busca facilitar o uso da gestão de riscos.

O Tribunal de Justiça do Tocantins, seguindo essa premissa, aprovou a Resolução nº 18 de 09 de julho de 2021, que incorpora em suas atividades a gestão de riscos.

O manual de metodologia ora apresentado busca ser simples e de fácil compreensão, propiciando que os operadores possam cumprir suas tarefas incorporando em seus processos de trabalho a gestão de riscos.

# GESTÃO DE RISCOS

A gestão de riscos é um processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos. Consiste em identificar, avaliar e administrar eventos diante de incertezas críticas. As incertezas emanam da incapacidade de determinar com precisão a probabilidade da ocorrência de determinado evento e os impactos a ele associados. Os riscos podem ser positivos ou negativos e são capazes de afetar os objetivos, programas, projetos, atividades ou processos de trabalho, nos níveis estratégico, tático e operacional.

É tarefa da Administração planejar e executar ações para modificar o risco, bem como monitorar e comunicar, com vistas ao efetivo alcance dos objetivos da instituição.

Trata-se, portanto, de um processo de trabalho de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, aplicável em qualquer área da organização e que contempla as atividades de identificar riscos, analisar, avaliar, decidir sobre estratégias de resposta a riscos e, para tal, conta com o apoio dos magistrados, servidores e colaboradores, de modo a manter os riscos compatíveis com a tolerância desejada e assim auxiliar no cumprimento dos objetivos institucionais.

# OBJETIVOS

O principal objetivo da Gestão de Risco no Poder Judiciário do Tocantins - PJTO é auxiliar a tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão, no alcance dos objetivos institucionais e apoiar a governança coorporativa, bem como aprimorar os controles internos.

Com isso, vários outros objetivos também são alcançados (TRE-TO, adaptado):

1. **Potencializar o orçamento** – o conhecimento dos riscos permite ao Tribunal conduzir uma avaliação eficaz das necessidades, como um todo, e aprimorar a alocação orçamentária;
2. **Oportunizar oportunidades** – oportunidade é também chamado de risco positivo, pois constitui a possibilidade de um evento afetar positivamente os objetivos. O Tribunal deve posicionar-se para identificar e aproveitar as oportunidades de forma proativa;
3. **Ajustar a tolerância a risco com a estratégia adotada** – tolerância ao risco é o grau de risco que a administração quer aceitar. Os gestores avaliam o perfil de risco e desenvolvem mecanismos para gerenciar esses riscos;
4. **Reduzir prejuízos operacionais** – é a capacidade para identificar riscos em potencial e estabelecer respostas aos mesmos, reduzindo surpresas e custos ou prejuízos associados;
5. **Reforçar as decisões para rebater os riscos** – identificando os riscos possibilita-se ao gestor selecionar alternativas de respostas, quais sejam: como evitar, reduzir, compartilhar e aceitar os riscos;

Risco é a possibilidade de que um evento afete negativamente o alcance dos objetivos. Não considerar explicitamente os riscos na tomada de decisões pode acarretar o não alcance dos objetivos ou resultados que poderiam ser atingidos.

Oportunidade é a possibilidade de que um evento afete positivamente o alcance de objetivos.

Neste contexto, o objetivo da gestão de riscos é aumentar a probabilidade e o impacto dos riscos positivos (oportunidades) e reduzir a probabilidade e o impacto dos riscos negativos (ameaças).

# ESTRUTURA E RESPONSABILIDADES DA GESTÃO DE RISCOS

De acordo com a Política de Gestão de Riscos do Tribunal de Justiça do Tocantins as instâncias responsáveis pelo Sistema de Gestão de Riscos são:

I - o Tribunal Pleno;

II - o Presidente;

III - os Líderes do Planejamento Estratégico;

IV - o Diretor Geral;

V - a Diretoria do Controle Interno;

VI - a Coordenadoria de Gestão Estratégica, Estatística e Projetos;

VII - a Comitê de Gestão Riscos;

VIII - os Gestores de Riscos;

**Figura 1** – Organograma estrutura Gestão de Riscos



Obedecendo essa estrutura hierárquica, descreve-se as competências e responsabilidades definidas na Política de Gestão de Riscos.

## Tribunal Pleno

I – Aprovar a Política de Gestão de Riscos;

II – Aprovar o grau de apetite e tolerância a riscos.

## Presidente

I - submeter ao Pleno as revisões da Política de Gestão de Riscos;

II - submeter ao Pleno o grau de apetite e tolerância a riscos;

III - designar os membros do Comitê de Gestão de Riscos;

IV - decidir sobre prioridades de atuação;

V - patrocinar a cultura de gestão de riscos.

## Líderes do Planejamento Estratégico

I - avaliar, monitorar e revisar os riscos estratégicos em conformidade com a governança da estratégia.

## Diretor Geral

I - aprovar os processos de trabalho que devem ter seus riscos gerenciados e tratados no âmbito tático e operacional, tendo em vista a dimensão dos prejuízos que possam causar;

II – monitorar os riscos táticos e operacionais;

## Diretoria de Controle Interno

I - avaliar a política de gestão de riscos;

II - avaliar se o processo e os planos de gestão de riscos estão de acordo com esta política;

III - avaliar a eficácia dos controles internos da gestão, implementados para mitigar os riscos, bem como outras respostas aos riscos avaliados;

IV - acompanhar de forma sistemática a gestão de riscos para garantir sua eficácia e o cumprimento de seus objetivos;

V - reportar à Presidência os resultados das avaliações de riscos, assim como o estágio de realização das ações para seu tratamento.

## Coordenadoria de Gestão Estratégica, Estatística e Projetos

I - elaborar, em conjunto com o Comitê de Gestão de Riscos, a metodologia de gestão de riscos, bem como propor as atualizações necessárias;

II - monitorar, em conjunto com Comitê de Gestão de Riscos o processo de gestão de riscos estratégicos;

III - estimular, em conjunto com o Comitê de Gestão de Riscos, a adoção da cultura de gestão de riscos em todo o Poder Judiciário do Estado do Tocantins;

IV - coordenar o processo de gestão de riscos no nível estratégico;

V - prestar apoio técnico aos gestores para que utilizem a metodologia de gestão de riscos de forma eficaz;

VI - dar suporte e auxiliar no mapeamento dos processos de trabalho que terão os riscos monitorados.

## Comitê de Gestão de Riscos

I - propor a revisão da Política de Gestão de Riscos ao Presidente;

II - propor o adequado grau de apetite e tolerância a riscos ao Presidente;

III - monitorar a execução da Política de Gestão de Riscos;

IV - dar suporte metodológico à implantação e operacionalização do gerenciamento de riscos;

V - propor ações de sensibilização e capacitação sobre gestão de riscos;

VI - fomentar práticas de gestão de riscos;

VII - elaborar e analisar periodicamente o mapa de riscos;

VIII - sugerir ao Presidente prioridades de atuação.

## Gestor de Riscos

I - gerir os riscos sob sua responsabilidade relativos a processos, projetos e iniciativas, de acordo com o contexto organizacional da gestão de riscos;

II - gerenciar os riscos inerentes aos processos de trabalho sob sua responsabilidade, de forma a mantê-los em nível de exposição aceitável;

III - elencar os riscos e sugerir ao Comitê quais deverão ser priorizados para tratamento;

IV - elaborar o mapa de riscos e submeter ao Comitê de Gestão de Riscos;

V - elaborar e implementar planos de ação para tratamento dos riscos inerentes, definindo as ações a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos;

VI - comunicar ao Comitê novos riscos que impactem seus processos;

VII - executar as medidas de controle relacionadas ao risco identificado nos seus processos;

VIII - reportar ao Comitê situações que, eventualmente, extrapolem à sua competência e capacidade para gerenciamento.

Gestor de risco é a pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco, em seus respectivos âmbitos e escopos de atuação.

Os gestores de riscos têm a atribuição de executar as atividades do processo de gestão de riscos dos objetos de gestão e ativos sob sua responsabilidade.

Os gestores de risco podem ser:

1. responsáveis por um processo, ativo, atividade ou ação de plano institucional;
2. gestores de projetos;
3. gestores operacionais;
4. dirigentes de unidade, de coordenação e chefes de gabinete.

Os dirigentes de unidades e/ou coordenadores são gestores de risco de objetos de gestão que tenham natureza transversal.

## Matriz RACI para as atividades do processo de gestão de riscos

RACI é uma sigla que corresponde aos seguintes atores: Responsável, Aprovador, Consultado e Informado.

A matriz RACI é uma ferramenta por meio da qual o gestor toma consciência de suas atribuições no processo, ativo, projeto e/ou atividade. É uma matriz de distribuição de responsabilidades.

**Figura 2** - Matriz RACI

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ITEM** | **ATIVIDADE** | **PLENO** | **PRESI** | **LÍDERES P.E.** | **DIRETOR GERAL** | **COGES** | **COMITÊ GESTOR DE RISCOS** | **GESTOR DE RISCOS** |
| 1.1 | Estabelecer política de riscos | A | R |  | I | C | C | I |
| 1.2 | Elaborar e manter e revisar o processo de gestão de riscos | - | - | **-** | A | R | R | I |
| 1.3 | Decidir sobre o grau de tolerância ao risco | A | R |  | I | - | C | I |
| 1.4 | Estrutura de gestão de riscos | A | R | **-** | I | - | C | I |
| 1.5 | Plano de Gestão de Riscos do TJTO | - | - | **-** | A | I | R | R |
| 1.6 | Realizar análises críticas periódicas do processo deGestão de Riscos | - | - |  | - | - | R | I |
| 1.7 | Disseminar e dar suporte metodológico à implantação e operacionalização do gerenciamento de riscos | - | - | **-** | - | A | A | I |
| 1.8 | Gerir os Riscos (identificar, analisar e avaliar) | - | - | - | - | - | C | R |
| 1.9 | Tratamento de Riscos | - | - | - | - | - | A | R |
| 1.10 | Monitoramento de Riscos | - | - | R | R | I | I | I |

**R- Responsável A – Aprovador C – Consultado I – Informado**

# PROCESSO DE GESTÃO DE RISCOS

Processo é um conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar um produto, resultado ou serviço predefinido.

A gestão de riscos deve ser parte integrante nos processos de gestão existentes na organização e que o gerenciamento de riscos seja incluído como um dos processos que dão suporte à definição de estratégias, à execução de planos, ao controle dos atos e ao processo de melhoria contínua. Deve ser adaptado aos processos de negócio da organização e incorporado na cultura e nas práticas organizacionais, assim é importante que se adote o costume em reconhecer a existência de riscos e a necessidade de administrá-los, seja reduzindo a probabilidade de ocorrência dos mesmos ou reduzindo o impacto das consequências causadas pela ocorrência dos riscos identificados

Para realizar a gestão de riscos, as seguintes etapas devem ser seguidas: Estabelecimento do contexto, identificação dos riscos, análise dos riscos, avaliação dos riscos e tratamento dos riscos.

Em todas essas etapas deverá haver comunicação e consulta com partes interessadas, monitoramento e análise crítica visando a melhoria contínua.

Dada a natureza multidisciplinar da gestão de riscos, o processo deve ser conduzido, preferencialmente, de forma coletiva, em oficinas de trabalho, por pessoas que conhecem aquele ativo, processo, projeto, atividade.

**Figura 3** - Processo de Gestão de Risco



## Processo de Gestão de Riscos no Poder Judiciário do Tocantins - PJTO

A metodologia de Gestão de Riscos PJTO adota o ciclo composto pelas etapas apresentadas na Política de Gestão de Riscos do PJTO. São elas: definição do contexto, identificação, análise, avaliação, tratamento de riscos, monitoramento e comunicação.

**Figura 4** - Processo de gestão de riscos em forma de mapa mental



A metodologia proposta para a Gestão de Riscos utiliza como base as seguintes Normas: ABNT NBR ISO/IEC 31000, ABNT NBR ISO/IEC 31010 e ABNT NBR ISO/IEC GUIA 73.

**Figura 5** - Resumo comparativo de normas

|  |  |  |  |
| --- | --- | --- | --- |
| Norma | Título | Objetivo | Observação |
| 31000 | Gestão de riscos – Princípios e diretrizes | Fornece diretriz para gerenciar riscos enfrentados pelas organizações. A sua aplicação pode ser personalizada para qualquer organização e seu contexto. | Pode ser aplicada a qualquer atividade, incluindo a tomada de decisão em todos os níveis. |
| 31010 | Gestão de riscos – Técnicas para o processo de avaliação de riscos | Descreve as diversas técnicas e ferramentas de análise de riscos. | Deve ser trabalhada em apoio à Norma 31000. |
| Guia 73 | Gestão de riscos - Vocabulário | Apresenta as definições de termos genéricos relativos à gestão de riscos. | Destina-se à utilização de terminologia uniforme de gestão de riscos em processos e estruturas para gerenciar riscos. |

Fonte: BEZERRA, 2013, adaptado

Foram considerados três critérios para a escolha da metodologia:

1. Simplicidade no modelo de gestão;
2. Compatibilidade com a prática de Gestão do Poder Judiciário do Tocantins (PJTO);
3. Flexibilidade. As etapas do ciclo de Gestão de Riscos podem ser adaptadas às diversas áreas do PJTO.

Os riscos inerentes às atividades podem ser identificados e avaliados partindo de estruturas como processos de negócio, ativos, ambientes específicos e pessoas.

Nos processos de negócio, a identificação e avaliação de riscos podem partir da análise de um processo específico das áreas que compõem o Poder Judiciário do Tocantins, levando em consideração todos os procedimentos, atividades e tarefas que contribuem para a execução do processo.

Os riscos podem ser identificados e avaliados também em relação a determinado ativo de informação e/ou um ambiente, sobretudo quando eles são considerados como essenciais ao funcionamento do PJTO. Por exemplo, pode-se levantar riscos em relação a um ambiente específico como o *data center*.

Como um ativo importante, pode-se destacar pessoas que detêm informações ou desempenham atividades relevantes para o negócio. Podem ser servidores, colaboradores terceirizados, estagiários etc.

### Definição do contexto

Consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

Recebida uma solicitação para que se proceda a gestão de risco de um determinado escopo, a primeira atividade a ser executada é a comunicação das áreas e pessoas envolvidas, a data de início dos trabalhos, os prazos, custos, pessoas envolvidas e resultados esperados.

Nesta fase ocorre a definição e detalhamento do escopo ou contexto de aplicação da gestão de riscos a fim de delimitar o âmbito de atuação. O escopo pode ser uma estrutura funcional, um processo, sistema, recurso ou determinado ativo. Também devem ser definidos os prazos (cronograma), partes interessadas, pessoas envolvidas e resultados esperados. Estas informações devem ser comunicadas às áreas e pessoas envolvidas já no início dos trabalhos.

Conforme Manual de Gestão de Riscos do TCU, o estabelecimento do contexto deve seguir os seguintes passos:

- Identificar quais objetivos ou resultados devem ser alcançados;

- Identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;

- Identificar as pessoas envolvidas nesses processos e especialistas na área;

- Mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, *stakeholders* etc.).

### Estabelecimento do contexto interno e externo

O passo inicial para se estabelecer o contexto é analisar o ambiente interno e o ambiente externo em que está inserida a organização quanto as variáveis que possam afetar seu funcionamento e ocasionar riscos as suas atividades.

### Contexto Geral

É a análise que se faz de todo o contexto que envolve a organização. Busca-se identificar os fatores capazes de afetar a organização e consequentemente auxiliam no reconhecimento de possíveis situações que possam interferir e possibilitar a definição de quais riscos deverão serem geridos.

Para essa identificação, a tabela seguinte apresenta alguns fatores internos e externos em que a organização está inserida e podem servir de norte nesta análise.

**Figura 6** - Contexto Interno e Externo

|  |  |
| --- | --- |
| **INTERNO** | **EXTERNO** |
| **Valores**- Código de ética- Planejamento Estratégico | **Políticos**- Políticas Públicas- Guerras e Conflitos- Subsídios |
| **Cultura interna**- Cultura organizacional- Costumes | **Econômicos**- Macro economia- Impostos- Câmbio- Juros- Sazonalidades- Indicadores econômicos |
| **Competência**- Gestão das competências- Segregação de funções | **Sociais**- Imagem da Instituição- Demografia- Impactos ambientais e sociais |
| **Conhecimento Organizacional**- Liderança- Clima organizacional- Carga horária- Carga de trabalho- Condições de trabalho | **Tecnológicos**- Inovações disponíveis do mercado- Acesso a tecnologia- Disponibilidade de prestares de serviço |
| **Desempenho**- Elementos que influenciam o alcance dos objetivos estratégicos- Programas de gestão  | **Ambiental**- Exigências legais- Sustentabilidade |
| **Recursos Financeiros**- Disponibilidade orçamentária e financeira- Histórico de contingenciamentos | **Legislação**- Leis que afetam o Poder Judiciário- Normas aplicadas ao Poder judiciário- Leis e Normas de Licitações |
| **Infraestrutura**- Condições físicas dos ambientes de trabalho- Condições físicas dos ambientes de atendimento |  |
| **Tecnologia**- Condições do parque tecnológico- Sistemas disponíveis- Alinhamento da TI com o planejamento estratégico institucional e planejamento estratégico de TI |  |

A análise do contexto geral não se restringe a esses fatores. Muitas outras possibilidades poderão ser levantadas. O apresentado permite nortear os gestores de riscos nos levantamentos que serão feitos ao longo da definição dos riscos possíveis.

### Contexto Específico

Aqui pretende-se analisar o ambiente interno e o ambiente externo em que está inserido o processo de gestão, ativo ou outra atividade que esteja sendo avaliada quanto aos riscos existentes.

Para analisar diretamente os fatores internos e externos que impactam na execução de determinado processo ou atividade, faz-se necessário relacionar alguns fatores. Uma ferramenta que permite relacionar esses fatores é a Matriz SWOT. Nessa matriz os fatores podem ser classificados como Pontos Fortes e Pontos Fracos do processo, estando relacionados à organização (fatores internos), Oportunidades e Ameaças relacionadas ao ambiente de atuação (fatores externos).

Num processo de **aquisição** pode-se imaginar a seguinte distribuição no quadro SWOT.

**Figura 7** - Modelo Matriz SWOT

|  |  |  |
| --- | --- | --- |
| **Fatores Internos****(Organização)** | **PONTOS FORTES** | **PONTOS FRACOS** |
| - Boa qualificação da equipe de licitações e Contratos.- Existência do Plano Anual de contratações.- Existência de Planejamento e Gestão Estratégica definindo as ações a longo prazo. | - Falta de servidores.- Dificuldade na obtenção de cotações dos preços dos produtos e serviços. |
| **Fatores Externos****(Ambiente)** | **OPORTUNIDADES** | **AMEAÇAS** |
| - Resolução CNJ 347/2020 que orienta as ações para planejamento das contratações. | - Orçamento com contingenciamento.- Conjuntura político-econômica do Brasil como resultado da pandemia.- Variação imprevisível do preço dos produtos e serviço. |

Fonte: Exercício elaborado pelo Autor

Conhecendo os fatores internos e externos que possam afetar de forma positiva ou negativa o processo de trabalho ou atividade evidenciamos em que eles podem influenciar na sua execução. Isso facilita a identificação de possíveis **fontes de risco** e poderão servir de base para a etapa de identificação dos riscos.

Dessa forma cada Gestor de Riscos passa a conhecer o contexto específico do processo ou atividade que está sob sua responsabilidade e deverá ser atualizado periodicamente.

O produto a ser gerado nessa etapa será o **Relatório de Contextualização, conforme Anexo I**.

## Mapear processos e ativos

Esta etapa corresponde ao conjunto de ações necessárias para levantamento, detalhamento e estruturação dos processos e ativos (tecnologias, ambientes e pessoas) que podem impactar os objetivos, missão ou atividades finalísticas do PJTO.

Para que a execução do ciclo de gestão de riscos seja realizada de acordo com os objetivos estratégicos, é necessário que os principais processos sejam mapeados e os ativos sob o escopo sejam inventariados. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas. Como resultado, o produto a ser gerado será uma lista de processos e ativos com riscos a serem gerenciados, e fará parte do relatório de contextualização.

## Identificação de riscos

Etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas e o objetivo é produzir uma lista abrangente de riscos, incluindo fontes e eventos que possam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto.

A Norma ABNT NBR ISO/IEC 31010 fornece orientações sobre a seleção e a aplicação de técnicas sistemáticas para o processo de avaliação de riscos. Uma das técnicas abordadas pela Norma é a de ***Brainstorming*,** que consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado (TCU, 2018).

Os riscos necessariamente possuem uma ou mais causas conhecidas e podem gerar uma ou mais consequências. As causas podem se originar de ações ou omissões de indivíduos (agentes causadores), de fontes de risco inerente (exemplo, líquido inflamável tem risco de entrar em combustão por natureza; um equipamento elétrico pode parar de funcionar por falta de energia elétrica) ou da combinação de ambos (um agente utilizar uma fonte de risco para causar um dano).

A materialização da ocorrência do risco é denominada evento de risco. Ocorrendo o risco, ele irá trazer consequências diretas ou indiretas aos objetivos organizacionais ou ao processo analisado, que podem representar perdas ou danos, ou mesmo ganhos quando se trata de riscos positivos (TRT8, 2015).

**Figura 8** - Elementos do risco

Fonte: TRT8, 2015, adaptado

Visando racionalizar a etapa, foram definidos 5 (cinco) passos básicos para identificação de riscos em qualquer processo, ambiente, projeto ou sistema, conforme citado em TRT8 (2015).

**Figura 9** - Passos para identificação de riscos

|  |
| --- |
| 1º Passo: Identificar as principais funções ou objetivos do processo, ambiente, projeto ou sistema. |
| 2º Passo: Levantar possíveis eventos que podem impedir ou dificultar a execução ou o atingimento dos objetivos do processo, ambiente, projeto ou sistema. |
| 3º Passo: Levantar as possíveis causas que levam a ocorrência do evento. |
| 4º Passo: Levantar as possíveis consequências da ocorrência do evento (levando em consideração os objetivos organizacionais e conformidade normativa). |
| 5º Passo: Identificar os responsáveis e levantar os controles que atualmente já sejam aplicados na mitigação das causas dos riscos. |

Fonte: TRT8, 2015, adaptado

O produto a ser gerado nessa etapa será a **matriz de identificação de riscos, conforme Anexo II.**

**Figura 10** - Exemplo de identificação de riscos e levantamento de controle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ativo | Evento de Risco | Causas | Consequências | Controles Implementados |
| Data Center | Incêndio no Data Center | 1. Curto circuito no Data Center;2. Curto circuito nas dependências do prédio. | 1. Destruição parcial ou total do Data Center. | 1. Nenhum. |
| Estações de Trabalho | Ataques por *software* de código malicioso às estações de trabalho | 1. Não possuir antivírus instalado;2. Antivírus está desatualizado;3. Acesso indevido a *site* com códigos maliciosos;4. Mau uso de dispositivos de armazenamento externo. | 1. Mau funcionamento das estações de trabalho;2. Roubo de dados;3. Proliferação de programas de código malicioso para outras estações de trabalho. | 1. Solução corporativa de antivírus. |

Fonte: TRT8, 2015, adaptado

## Análise de riscos

Com os riscos identificados, com as respectivas causas e consequências relacionadas, e com o levantamento prévio de controles internos, começa a etapa de análise dos riscos com base nos critérios pré-definidos de probabilidade de ocorrência e impacto, e assim definir o NRI (nível de risco inerente) ou seja, o nível das consequências para o processo ou atividade.

Segundo a ABNT (2018), a análise de riscos é o processo de compreendê-los e determinar seu nível, de modo a subsidiar a avaliação e o tratamento destes. Envolve a apreciação das causas e fontes de risco, suas consequências e a probabilidade de que estas possam ocorrer.

A multiplicação entre os valores de probabilidade e impacto definem o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

**NÍVEL DO RISCO INERENTE (NRI) = Impacto x Probabilidade**

Para estabelecer um entendimento comum das classificações de probabilidade e impacto, as tabelas a seguir apresentam as escalas de valores para cada um desses fatores.

**Figura 11** - Escala de probabilidade de ocorrência de uma ameaça

|  |  |  |
| --- | --- | --- |
| PROBABILIDADE | DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES | VALOR |
| Muito baixa | **Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade. | **1** |
| Baixa | **Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. | **2** |
| Média | **Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. | **3** |
| Alta | **Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. | **4** |
| Muito alta | **Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade. | **5** |

Fonte: TCU, 2018, adaptado

**Figura 12** - Escala de Impacto da ocorrência

|  |  |  |
| --- | --- | --- |
| IMPACTO | CONSEQUÊNCIA, CASO O EVENTO OCORRA | VALOR |
| Muito baixa | **Mínima,** quase não afeta o processo ou ativo. | **1** |
| Baixa | **Pequena,** afeta pouco o processo ou ativo. | **2** |
| Média | **Moderada,** afeta moderadamente o processo ou ativo, porém recuperável. | **3** |
| Alta | **Significativa,** afeta gravemente o processo ou ativo. De difícil reversão. | **4** |
| Muito alta | **Catastrófica,** afeta o processo ou ativo de forma irreversível. | **5** |

Fonte: TCU, 2018, adaptado

**Figura 13** - Escala de Impacto nas dimensões do objetivo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NÍVEL | CUSTO | PRAZO | ESCOPO | QUALIDADE |
| 1 | aumentar em até 5% | atrasar em até 5% | Insignificante | Irrisória |
| 2 | aumentar entre 5% e 10% | atrasar entre 5% e 10% | Pouco | Pouco |
| 3 | aumentar entre 10% e 15% | atrasar entre 10% e 15% | Significativa | Relevante |
| 4 | aumentar entre 15% e 20% | atrasar entre 15% e 20% | Muito Significativa | Muito relevante  |
| 5 | aumentar mais de 20% | atrasar mais de 20% | Ampla | Grave |

Fonte: TRE-TO, adaptado

Os níveis de risco obedecerão ao resultado do produto das variáveis, podendo gerar valores que vão de 1 a 25.

**Figura 14** - Matriz de impacto x probabilidade

|  |  |
| --- | --- |
| **Muito Alto****Alto****Médio****Baixo** | **Probabilidade** |
| **Muito baixo** | **Baixa** | **Média** | **Alta** | **Muito alta** |
| **Impacto** | **Muito baixo** | **1** | **2** | **3** | **4** | **5** |
| **Baixo** | **2** | **4** | **6** | **8** | **10** |
| **Médio** | **3** | **6** | **9** | **12** | **15** |
| **Alto** | **4** | **8** | **12** | **16** | **20** |
| **Muito alto** | **5** | **10** | **15** | **20** | **25** |

Fonte: TRE-TO, adaptado

**Figura 15** - Escala de classificação de risco

|  |  |
| --- | --- |
| NÍVEL DO RISCO | NRI  |
| Muito baixo e baixo | De 1 a 2 |
| Médio | De 3 a 7 |
| Alto | De 8 a 14 |
| Muito alto | De 15 a 25 |

Fonte: TRT8, 2015, adaptado

O documento base para essa etapa é a **Matriz de Análise e Avaliação de Riscos, conforme Anexo III.**

**Figura 16** - Exemplo de Matriz de Análise e Avaliação de Riscos

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ativo | Evento de Risco | Causas | Consequências | P | I | NRI  | NRI |
| Data Center | Incêndio no Data Center | 1. Curto circuito no Data Center;2. Curto circuito nas dependências do prédio. | 1. Destruição parcial ou total do Data Center. | 2 | 5 | 10 | **ALTO** |
| Estações de Trabalho | Ataques por *software* de código malicioso às estações de trabalho | 1. Não possuir antivírus instalado;2. Antivírus está desatualizado;3. Acesso indevido a *site* com códigos maliciosos;4. Mau uso de dispositivos de armazenamento externo. | 1. Mau funcionamento das estações de trabalho;2. Roubo de dados;3. Proliferação de programas de código malicioso para outras estações de trabalho. | 4 | 3 | 12 | **ALTO** |

Fonte: TRT8, 2015, adaptado

## Avaliação de Riscos

O propósito da avaliação de riscos é apoiar decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Caso já existam controles implementados, se eles devem ser modificados, mantidos ou eliminados**.**

As decisões estratégicas devem considerar o contexto mais amplo do risco, incluindo o exame de quão tolerável são os riscos a serem assumidos. Para isso, com as informações sobre os processos de negócio da organização e os ativos que os suportam, deve-se:

* Priorizar os riscos – As ações e os ativos que possuírem os maiores níveis de risco (NRI) serão priorizados em termos de recursos e proteções;
* Ter maior conhecimento sobre os riscos e avaliar as melhores soluções de proteção, considerando seu custo-benefício.

Para o processo de avaliação foi estabelecido critérios para priorização e tratamento associados aos níveis de risco. A documentação desta etapa será o **Relatório de Avaliação de Riscos (Anexo IV)**, que consiste em uma lista dos riscos que requerem tratamento, com suas respectivas **classificações e prioridades**.

**Figura 17** - Critérios para priorização e tratamento de riscos

|  |  |
| --- | --- |
| NÍVEL DE RISCO | CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS |
| Muito Baixo | São riscos aceitáveis e devem ser informados aos gestores dos processos ou ativos. |
| Baixo | São riscos que podem ser aceitáveis, não havendo necessidade de tratamento imediato, devendo apenas ser reconhecidos e monitorados quanto às ocorrências e possíveis consequências. |
| Médio | São riscos toleráveis, e os responsáveis devem ser orientados a adotar estratégias para mitigar ou compartilhar, porém devem passar por análise de custo-benefício quanto à necessidade de aplicação de controles. |
| Alto | São riscos rejeitáveis, e os responsáveis devem ser orientados para pelo menos reduzi-los e controlá-los. |
| Muito Alto | São riscos inaceitáveis, e os responsáveis devem ser orientados para que os evitem ou reduzam imediatamente. |

Fonte: TRT8, 2015, adaptado

### Matriz “Apetite a Risco”

O apetite a risco é um nível de exposição a riscos e, portanto, possíveis perdas que o Tribunal vê como aceitável, dados os objetivos e recursos empregados.

Tolerância ao risco é o grau de variação do apetite ao risco que o Tribunal está disposto a tolerar. Em sentido mais abrangente é a quantidade de risco que o Tribunal se dispõe a aceitar na busca por agregar valor aos serviços prestados para a sociedade. O apetite a risco está diretamente associado à estratégia da instituição e deve ser considerado no momento de definir as estratégias, pois estas expõem o TJTO a diferentes riscos.

O apetite a riscos do TJTO está definido na Tabela – Matriz de Apetite a Risco. Não cabe aos gestores de riscos fazer adequações neste critério de riscos. Conforme previsto na Política de Riscos, é um parâmetro proposto pela Presidência e aprovado pelo Tribunal Pleno.

**Figura 18** - Matriz de Apetite a Risco

|  |  |  |
| --- | --- | --- |
| NÍVEL DE RISCO | PONTUAÇÃO | APETITE A RISCO |
| Muito baixo e baixo | **De 1 a 2** | Oportunidade |
| Médio | **De 3 a 7** | Tolerável  |
| Alto | **De 8 a 14** | Rejeitável |
| Muito alto | De 15 a 25 | Inaceitável |

Fonte: TRE-TO, adaptado

## Tratamento de Riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão novos controles ou modificação dos existentes. Opções de tratamento de riscos incluem evitar, mitigar, compartilhar e aceitar o risco, devendo-se observar que elas não são mutuamente exclusivas (TCU, 2018).

Como risco aceitável, o Poder Judiciário do Tocantins considera os riscos que foram classificados como **Muito Baixo** e **Baixo.** Portanto, deverão ser tratados os riscos classificados como **Médio, Alto e Muito Alto,** cabendo ao Gestor da área analisar os casos especiais, nos quais a aceitação do risco é justificável. Podem ser entendidos como casos especiais, dentre outros, as atividades temporárias ou de curto prazo, a implantação de controles cujo custo supera o valor da consequência causada pela ocorrência do evento.

Segundo a ABNT NBR ISO/IEC 31000, a finalidade dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado.

O plano de tratamento deve ser validado pelo Comitê Gestor de Riscos, que definirá ou ajustará as atividades de acordo com as restrições que porventura existam, como orçamento disponível ou priorização de atividades externas à gestão de riscos. Com isso, será atualizado o plano com as devidas justificativas para a não implantação dos controles sugeridos.

Paralelamente, o gestor de riscos deverá comunicar ao Comitê de Gestão de Riscos do Poder Judiciário quais foram os processos identificados que impactam na Gestão Estratégica e este deverá analisar as medidas de tratamento adotadas e caso necessário, propor adequações. Cabe ainda ao Comitê de Gestão de Riscos comunicar a Presidência do Tribunal de Justiça sobre os riscos que impactam no alcance dos objetivos estratégicos e os planos de ação adotados para o tratamento.

Executar o Plano de Tratamento significa a implantação dos controles selecionados para cada ativo, de acordo com suas particularidades e características.

Dar uma resposta ao risco encontrado envolve decidir se ele vai ser tratado ou não, promovendo a priorização de tratamento dos riscos. Cabe ressaltar que a priorização de tratamentos é atribuída na Política de Riscos do PJTO quando da definição do apetite ao risco, cabendo aos gestores de riscos a identificação, avaliação e tratamento. A estratégia de resposta ao risco adotada no PJTO é composta pelas opções evitar, mitigar, compartilhar e aceitar, conforme descrito na Tabela - Estratégia de resposta aos riscos.

**Figura 19** - Estratégia de resposta aos riscos

|  |  |
| --- | --- |
| RESPOSTA AO RISCO | DESCRIÇÃO |
| Evitar | Inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de um processo de trabalho. |
| Mitigar | São adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos. Tipicamente, esse procedimento abrange qualquer uma das centenas de decisões do negócio no dia a dia. |
| Compartilhar | Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras. |
| Aceitar | Quando o nível de risco for baixo ou muito baixo, o risco residual não justifica a implementação de novos controles para mitigá-lo, em uma análise da relação de custo e benefício. Portanto, nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos, podendo ser aceitos pelo gestor. |

Fonte: TRT8, 2015, adaptado

Para definir a priorização do risco deverá ser utilizada a **Matriz de Priorização dos Riscos (anexo V).**

**Figura 20** - Exemplo de matriz de priorização de riscos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ativo | Evento de Risco | Causas | Consequências | NRI | Resposta ao Risco |
| Data Center | Incêndio no Data Center | 1. Curto circuito no Data Center;2. Curto circuito nas dependências do prédio. | 1. Destruição parcial ou total do Data Center. | **ALTO** | **Mitigar** |
| Estações de Trabalho | Ataques por *software* de código malicioso às estações de trabalho | 1. Não possuir antivírus instalado;2. Antivírus está desatualizado;3. Acesso indevido a *site* com códigos maliciosos;4. Mau uso de dispositivos de armazenamento externo. | 1. Mau funcionamento das estações de trabalho;2. Roubo de dados;3. Proliferação de programas de código malicioso para outras estações de trabalho. | **ALTO** | **Mitigar** |

Fonte: TRT8, 2015, adaptado

## Plano de Tratamento de Riscos

Após a avaliação, a definição da estratégia de resposta e a priorização de tratamento dos riscos, faz-se necessário o detalhamento do tratamento dos riscos. Essa etapa será responsável pela seleção e implementação de uma ou mais ações de tratamento para modificar os níveis de riscos.

Antes de elaborar o plano de tratamento de riscos, primeiro é necessário decidir quais controles precisam ser implementados, correlacionando as opções de mitigação e controles com cada risco priorizado. Os controles internos precisam ser reavaliados quanto à eficácia e suficiência, e com base nessa avaliação os gestores de riscos irão definir os controles internos que devem ser aperfeiçoados ou adicionados no tratamento (TRT8, 2015).

As perguntas que devem ser respondidas na reanálise dos controles internos são basicamente:

* Os controles existentes são capazes de tratar adequadamente o risco, de modo que ele seja controlado a um nível que seja tolerável?
* Na prática, os controles estão operando na forma pretendida e pode ser demonstrado que são eficazes quando requerido?

Conceitualmente, os controles internos podem ser classificados:

a) Pelo impacto na mitigação dos riscos

* Primário: proveem garantia razoável de que os objetivos serão atingidos, por meio da redução do risco de um resultado indesejado a um nível aceitável.
* Secundário: não são totalmente confiáveis do ponto de vista de efetividade, sendo frequentemente associado a controles corretivos ou compensatórios.

b) Por sua natureza de identificação

* Preventivo: projetado com a finalidade de evitar a ocorrência de erros, desperdícios ou irregularidades; atua sobre a probabilidade da ocorrência.
* Detectivo: projetado para detectar erros, desperdícios ou irregularidades, no momento em que eles ocorrem, permitindo a adoção de medidas tempestivas de correção; atua sobre a probabilidade e a severidade da ocorrência do risco.
* Corretivo: projetado para detectar erros, desperdícios ou irregularidades depois que já tenham acontecidos, permitindo a adoção posterior de ações corretivas; atua sobre a severidade da ocorrência do risco.

c) Pelo modo de processamento pode ser automatizado, quando processado por sistema informatizado e, não automatizado, quando processado manualmente.

d) Pela periodicidade ou frequência: anual, trimestral, mensal, diário e eventual.

Reanalisados os controles e definidos quais serão utilizados no tratamento dos riscos priorizados, é necessário elaborar o **Plano de Tratamento dos Riscos (Anexo VI).** Para elaborar o plano, o mais simples é visualizá-lo como um plano de ação onde são especificados: quais controles deverão ser aperfeiçoados, desenvolvidos e implementados, quem será o responsável por eles, e quais são os prazos e recursos requeridos.

**Figura 21** - Exemplo de Plano de Tratamento de Riscos

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Evento de Risco | Controles | Descrição | Monitoramento | Responsável | Prazo | Nível de Risco Pretendido |
| Incêndio no Data Center | Sistema de detecção e combate a incêndio. | O sistema de detecção e combate a incêndio tem como função perceber, captar, sinalizar e evitar a propagação de chamas no data center. | Acompanhar etapas de elaboração e execução do projeto.Registro de ocorrência do evento com periodicidade mensal | Chefe da DASR | 120 dias | Atual**Alto**Pretendido**Baixo** |
| Ataques por *software* de código malicioso às estações de trabalho | Solução corporativa de antivírus. | A solução detecta, impede e atua na remoção de programas de software maliciosos, como vírus e *worms*. | Monitoramento das estações via servidor de administração do antivírus.Registro de ocorrência do evento com periodicidade semanal. | Chefe da DMSU | 30 dias | Atual**Alto**Pretendido**Baixo** |
| Campanhas de conscientização de segurança. | O treinamento dos usuários para que eles sejam conscientes da segurança os fornecerá as habilidades necessárias para identificar comportamentos suspeitos, como *e-mails* de *phishing*, por exemplo. | Relatório de capacitação de pessoal.Registro de ocorrência do evento com periodicidade mensal | Chefe da DMSU | 90 dias |

Fonte: TRT8, 2015, adaptado

## Comunicação e Consulta

A comunicação e consulta é a etapa responsável pela manutenção de um fluxo regular e constante de informações com as partes interessadas, ocorrendo de forma concomitante durante todas as fases do processo de gestão de riscos. O gerenciamento das comunicações inclui os processos necessários para assegurar que as informações sejam geradas, coletadas, distribuídas, armazenadas, recuperadas e organizadas de maneira oportuna e apropriada (TRT8, 2015).

Durante a execução do processo de avaliação e tratamento de riscos, todas as etapas e atividades deverão ser devidamente comunicadas, seja às partes interessadas bem como às partes envolvidas. Tipos de informação que pode ser gerada no processo: relatórios, quadros, tabelas, inventários, matrizes de análise e avaliação, planos, planilhas de registro, ofícios e outros comunicados internos e externos, boletins de informação (notícias), convites em agenda eletrônica, formulários físicos e eletrônicos etc.

A comunicação poderá ser realizada por meio de ferramentas de apoio como correio eletrônico e comunicação instantânea, divulgação de informações no portal do Tribunal, por informações e despachos em processos administrativos, ferramenta de gerenciamento de projetos, reuniões etc.

O **Anexo VII deste manual contém um modelo de Formulário para Comunicação e Consulta.**

**Figura 22** - Exemplo de Comunicação e Consulta

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Partes | Comunicador | Propósito | Conteúdo | Meio de Comunicação | Data | Frequência |
| Gestores de Risco | Comitê Gestor de Riscos | Promover a análise dos riscos identificados | Convocar os gestores de riscos para a etapa de análise dos riscos identificados, visando apurar o nível de risco | Sistema SEI | 15/10/19 | Única |

Fonte: TRT8, 2015, adaptado

## Monitoramento e Análise Crítica

O processo de gestão de riscos deverá ser constantemente controlado e avaliado. Depois de planejada e executada a avaliação e tratamento dos riscos, durante sua execução deverá haver controle e ao final de cada ciclo de gestão de riscos deverá haver uma avaliação sobre o que deu certo e o que deu errado, visando adoção de medidas que corrijam os desvios em um próximo ciclo de gestão de riscos.

Devem ser analisados os artefatos do projeto (relatórios) em todas as fases do processo de gestão de riscos, de forma a mantê-los alinhados às diretrizes gerais estabelecidas. Os riscos devem ser monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

1. Nos critérios de avaliação e aceitação dos riscos;
2. No ambiente;
3. Nos processos de trabalho do PJTO;
4. Nos ativos do PJTO;
5. Nas ações do PJTO;
6. Nos fatores do risco (ameaça, vulnerabilidade, probabilidade e severidade).

**Figura 23** - Avaliação dos controles

|  |  |
| --- | --- |
| **Avaliação dos controles** | **Risco de Controle** |
| Controles inexistentes. | Muito Alto1,0 |
| Controle fraco, tendem a ser aplicados caso a caso e a responsabilidade é individual, dependendo das pessoas envolvidas. | Alto0,8 |
| Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas. | Médio0,6 |
| Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente. | Baixo0,4 |
| Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco | Muito Baixo0,2 |

,

**Figura 24** - Apuração do risco residual

|  |
| --- |
| **Apuração do Risco Residual** |
| **Risco Inerente** | **Risco de Controle** | **Risco Residual** |
| É o Nível de Risco (Risco Inerente = impacto x probabilidade) obtido quando de identificação e avaliação dos riscos | É o coeficiente (redutor) definido utilizando-se a tabela de avaliação dos controles | Resultado do Risco Inerente x Risco de controle |
| **Observação:***<< A atividade de Monitoramento e Análise Crítica pode gerar recomendações de melhorias para o tratamento do risco. >>* |

Conforme a evolução dos processos internos de gestão de riscos podem ser necessárias atualizações nas diretrizes e normas aplicáveis, isso implica em possíveis revisões da Política e no Manual de Gestão de Riscos. Revisar diretrizes e normas também é parte da análise crítica do processo de gestão de riscos, e visa garantir que as regras aplicáveis ao gerenciamento de riscos estejam sempre atuais e condizentes com a realidade organizacional.

O documento base para essa etapa é o **Relatório de Monitoramento e Análise Crítica, conforme Anexo VIII.**

# CONSIDERAÇÕES FINAIS

Os anexos I a IX apresentam os documentos básicos que deverão ser utilizados no processo de gestão de riscos no âmbito do Poder Judiciário do Tocantins. O Comitê Gestor de Riscos é o responsável por atualizar este Manual bem como os documentos padronizados, além de elaborar outros modelos básicos que sejam necessários.

#

# TERMOS E DEFINIÇÕES

**Análise crítica –** Estudo e avaliação realizado para determinar a adequação, suficiência e eficácia de um determinado setor, projeto, produto, serviço, processo ou informação com relação a requisitos pré-estabelecidos, tendo como objetivo a identificação de problemas, visando atingir os objetivos estabelecidos;

**Apetite a riscos –** É o nível de exposição a riscos e o grau de tolerância a possíveis perdas que o órgão vê como aceitável, dados os objetivos e recursos empregados;

**Ativos:** É um termo básico utilizado para expressar bens, equipamentos, valores e direitos. Podem ser tangíveis e intangíveis. Na gestão de riscos é a possibilidade da ocorrência de eventos que provoquem danos ou perdas e possam causar prejuízo ao normal funcionamento do órgão;

**Fonte de risco –** Conforme a ISO, fonte de risco é o elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;

**Identificação de riscos -** Processo de busca, reconhecimento e descrição de riscos;

**NRI –** Nível de risco inerente;

**Nível de risco -** Magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades;

**PJTO -** Poder Judiciário do Tocantins;

**Plano de gestão de riscos –** É a definição de como serão conduzidas as atividades de gestão de riscos. Especifica a abordagem, os componentes de gestão (incluem procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades) e os recursos a serem aplicados para gerenciar riscos (a um determinado produto, processo e projeto);

**Política de gestão de riscos -** Declaração das intenções e diretrizes gerais de uma organização relacionadas ao processo de gestão de riscos;

**Processo de avaliação de riscos -** Processo global de identificação de riscos, análise de riscos e avaliação de riscos;

**Processo de gestão de riscos -** Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos;

**Risco -** Efeito da incerteza nos objetivos, expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada;

**Risco residual -** Risco remanescente após o tratamento do risco;

**TCU** – Tribunal de Contas da União

**TRT8 –** Tribunal Regional do Trabalho da 8ª Região.

**Vulnerabilidade –** Incapacidade ou fragilidade de resistir aos efeitos de uma situação adversa. Ausência, inadequação ou deficiência, a qual pode vir a contribuir com a concretização de um evento indesejado.

# REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005:2011: **Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação.** Rio de Janeiro, 2011. 87 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31000:2018: **Gestão de Riscos - Diretrizes.** Rio de Janeiro, 2018a. 17 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31010:2012: **Gestão de Riscos - Técnicas para o processo de avaliação de riscos.** Rio de Janeiro, 2012. 96 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. GUIA 73:2009: **Gestão de Riscos - Vocabulário.** Rio de Janeiro, 2009. 12 p.

TCU. Tribunal de Contas da União. **Referencial básico de gestão de riscos** / Tribunal de Contas da União. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018. 154 p. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>. Acesso em: 5 out. 2018.

TRT8. Tribunal Regional do Trabalho da 8ª Região. **Manual de Gestão de Riscos**. Coleção Manuais de Gestão. Volume III. Manual Vermelho: Gestão de Riscos. Belém, 2015. 69 p. Disponível em: <https://www.trt8.jus.br/governanca/gestao-de-riscos>. Acesso em: 23 ago. 2019.

CNJ. Conselho Nacional de Justiça. Segurança da Informação - **Diretrizes para a gestão de segurança da informação no âmbito do Poder Judiciário.** Brasília, 2012**.** Disponível em: <http://www.cnj.jus.br/images/dti/Comite\_Gestao\_TIC/Diretrizes\_Gestao\_SI\_PJ.pdf>. Acesso em: 13 out. 2018.

CNJ. Conselho Nacional de Justiça. **Resolução n. 211, de 15 de dez. de 2015.** Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário. Brasília, 2015. Disponível em: <http://www.cnj.jus.br///images/atos\_normativos/resolucao/resolucao\_211\_15122015\_18122015173345.pdf>. Acesso em: 13 out. 2018.

TJTO. Tribunal de Justiça do Tocantins. **Resolução n. 18, de 09 de julho de 2021.** Dispõe sobre a Política de Gestão de Riscos do Poder Judiciário do Estado do Tocantins. Palmas, 2021. Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/2458>. Acesso em 19 ago. 2021.

TJTO. Tribunal de Justiça do Tocantins. **Portaria n. 3433, de 26 de jun. de 2017**. Dispõe sobre a Política de Segurança da Informação (PSI). Palmas, 2017. Disponível em: <http://www.tjto.jus.br/tic/index.php/governanca-de-tic/documentos-normativos/send/98-normativas/1147-politica-de-seguranca-da-informacao>. Acesso em: 15 nov. 2018.

TJTO. Tribunal de Justiça do Tocantins. **Portaria n. 1660, de 12 de agosto de 2019**. Promove atualizações em seu conteúdo e inclui normas de gestão de risco de segurança da informação e de gestão dos processos de backup, alterando a Portaria nº 3.433, de 26 de junho de 2017. Palmas, 2019. Disponível em: < http://wwa.tjto.jus.br/elegis/Home/Imprimir/1970>. Acesso em: 8 out. 2019.

TJTO. Tribunal de Justiça do Tocantins. **Resolução n. 10, de 19 de maio de 2016**. Dispõe sobre o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC). Palmas, 2016. Disponível em: < http://wwa.tjto.jus.br/elegis/Home/Imprimir/1100>. Acesso em: 4 out. 2019.

TCU. Tribunal de Contas da União. **Manual de gestão de riscos do TCU** / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2018. 46 p.: il. Obtido no <https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/> em 29.03.2021

Brasil. Governo Federal. **Decreto Federal 9.203 de 22.01.2017**, obtido junto ao link www.planalto.gov.br /ccivil\_03/\_Ato2015-2018/2017/Decreto/D9203.htm em 26.03.2017.

TRE-TO. Tribunal Regional Eleitoral do Tocantins. **Metodologia de Gestão de Riscos** obtido junto ao link [www.justicaeleitoral.jus.br/arquivos/tre-to-metodologia-de-gestao-de-riscos/rybena\_pdf?file=https://www.justicaeleitoral.jus.br/arquivos/tre-to-metodologia-de-gestao-de-riscos/at\_download/file em 29.03.2021](http://www.justicaeleitoral.jus.br/arquivos/tre-to-metodologia-de-gestao-de-riscos/rybena_pdf?file=https://www.justicaeleitoral.jus.br/arquivos/tre-to-metodologia-de-gestao-de-riscos/at_download/file%20em%2029.03.2021)

ANP. Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. **Metodologia de Gestão de Riscos ANP**, obtido junto ao link [www.anp.gov.br/arquivos/gestao-riscos/metodologia-gestao-riscos-anp.pdf](http://www.anp.gov.br/arquivos/gestao-riscos/metodologia-gestao-riscos-anp.pdf) em 04.04.2021.

BEZERRA, Edson Kowask. **Gestão de Riscos de TI: NBR 27005.** Rio de Janeiro: RNP/ESR, 2013. 138 p.

# ANEXOS

## ANEXO IModelo de Relatório de Contextualização

|  |  |
| --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* |
| **GESTÃO DE RISCOS** |
| **RELATÓRIO DE CONTEXTUALIZAÇÃO** | **DATA:** |
| **Área:** *<< Informar da divisão responsável pela avaliação dos riscos. >>* |
| **Gestor de Risco:** |

1. **Definição do escopo da avaliação de riscos**

*<< Descrever o escopo da avaliação de riscos (quais processos, subprocessos, atividades, tarefas, projetos, sistemas, ambientes, ativos terão os riscos avaliados e tratados). >>*

1. **Relevância do(s) processo(s)/ativo(s) na estratégia institucional**

*<< Identificar de que forma o processo/ativo que está sendo analisado quanto aos riscos contribui para o alcance dos objetivos organizacionais definidos no plano estratégico institucional. >>*

1. **Descrição do(s) processo(s)/ativo(s)**

*<< Descrever o processo que está sendo avaliado quanto aos riscos, além de levantar todos os ativos envolvidos. Se necessário avaliar as interações do processo com os demais processos da organização. Solicitar apoio do escritório de projetos para mapear fluxo do processo >>*

|  |  |  |
| --- | --- | --- |
| **Processo/Ativo** | **Descrição** | **Responsável** |
| *<< Listar processo/ativo >>* | *<< Descrever processo/ativo >>* | *<< Área responsável pelo processo/ativo.* |

1. **Partes interessadas e envolvidas no(s) processo(s)/ativo(s)**

*<< Identificar que são as partes interessadas, tanto interna quanto externamente, e as partes envolvidas no processo/ativo, no intuito de equilibrar os interesses das partes na execução da atividade e no processo de gerenciamento de riscos. >>*

|  |
| --- |
| **Partes Interessadas** |
| **Internas** | **Externas** |
| *<< Listar as partes interessadas internas >>* | *<< Listar as partes interessadas externas >>* |
| **Partes Envolvidas**  |
| *<< Listar as partes envolvidas internamente >>* |

## ANEXO IIModelo de Matriz de Identificação de Riscos

|  |  |  |
| --- | --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* | **Data:** |
| **Gestor de Risco:** | **Área:** |
|  |
|  |
| **Matriz de Identificação de Riscos** |
| **ID** | **Processo/Ativo** | **Evento de Risco** | **Causa** | **Consequência** | **Controles Implementados** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## ANEXO IIIModelo de Matriz de Análise e Avaliação de Riscos

|  |  |  |
| --- | --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* | **Data:** |
| **Gestor de Risco:** | **Área:** |
|  |
|  |
| **Matriz de Análise e Avaliação de Riscos** |
| **ID** | **Processo/Ativo** | **Evento de Risco** | **Causa** | **Consequência** | **P** | **I** | **NRI**  | **Nível de Risco** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## ANEXO IVModelo de Relatório de Avaliação de Riscos

|  |  |
| --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* |
| **GESTÃO DE RISCOS** |
| **RELATÓRIO DE AVALIAÇÃO DE RISCOS** | **Data:** |
| **Área:** *<< Informar da divisão responsável pela avaliação dos riscos. >>* |
| **Gestor de Risco:** |

1. **Resumo da Avaliação de Riscos**

*<< Nesta Seção deverão ser resumidas as informações da etapa de identificação dos riscos, análise e avaliação dos riscos, levando em consideração os objetivos do levantamento, as bases de conhecimento utilizadas e o resultado da identificação (quantidade de riscos, de causas e de consequências). >>*

*Exemplo: O levantamento de riscos do processo/ativo XYZ teve como objetivo mapear as principais fontes de riscos, eventos, causas e consequências que podem vir a comprometer o alcance dos objetivos organizacionais. O mapa de riscos foi baseado nos serviços XYZ, em que são relevantes a identificação e o monitoramento dos riscos. Para tanto, foram levantadas informações em documentos gerados no processo, bem como o conhecimento e experiência de pessoas-chave no processo. Com isso, ao todo foram identificados 20 (vinte) eventos de riscos, 35 (trinta e cinco) causas e 30 (trinta) consequências.*

*<< Deverá constar como anexo a esse documento a Matriz de Identificação de Riscos. >>*

1. **Metodologia Adotada**

*<< Neste campo deverá ser explicada a metodologia adotada para a identificação, análise e avaliação dos riscos. É importante pontuar quais as técnicas utilizadas para a identificação dos riscos, bem como a abrangência do estudo inicial. A forma de cálculo dos parâmetros da análise de riscos e do nível de risco referente à avaliação deve ser citada, porém sem detalhamentos, haja vista se encontrar no Manual de Gestão de Riscos. >>*

*Exemplo: Na etapa de identificação dos riscos foram utilizadas as técnicas de brainstorming e de análise de fluxograma para mapear as fontes de risco e chegar aos possíveis eventos, bem como suas causas e consequências. Para tanto, a equipe do projeto se reuniu com pessoas-chave no processo analisado, tendo previamente desenhado junto com a COGES o fluxograma básico do processo. Com os riscos identificados, foram aplicados os critérios definidos no Manual de Gestão de Riscos do TJTO para classificar a relevância do processo, a probabilidade de ocorrência dos eventos e a severidade do impacto das consequências para os objetivos organizacionais. Com os parâmetros aplicados, foi realizado o cálculo do nível de risco, conforme a metodologia adotada (produto entre os parâmetros e aplicação na faixa de nível de risco).*

*<< Deverá constar como anexo a esse documento a Matriz de identificação e a Matriz de Avaliação de Riscos. >>*

1. **Conclusões**

**3.1. Riscos identificados por processo/ativo**

*<< Neste campo, deve ser apresentada uma lista dos riscos identificados por processo/ativo com sua classificação e se eles possuem ou não algum controle implementado. >>*

|  |  |  |
| --- | --- | --- |
| **PROCESSO/ATIVO** | **RISCO IDENTIFICADO** | **CONTROLE** |
|  |  |  |

*<< Comentário sobre as informações prestadas. >>*

**3.2. Quantidade de riscos por nível**

*<< Nesse campo, devem ser apresentados a quantidade e o percentual de risco por nível, além de um breve comentário sobre as informações apresentadas. >>*

|  |  |  |
| --- | --- | --- |
| **NÍVEL** | **QUANTIDADE DE RISCOS** | **PERCENTUAL** |
| Muito Alto |  |  |
| Alto |  |  |
| Médio |  |  |
| Baixo |  |  |
| Muito Baixo |  |  |
| **TOTAL** |  |  |

## ANEXO VModelo de Matriz de Priorização dos Riscos

|  |  |  |
| --- | --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* | **Data:** |
| **Gestor de Risco:** | **Área:** |
|  |
|  |
| **Matriz de Priorização de Riscos** |
| **ID** | **Processo/Ativo** | **Evento de Risco** | **Causa** | **Consequência** | **Nível de Risco** | **Resposta ao Risco** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Nível de Risco: 1 – Muito Baixo, 2 – Baixo, 3 – Médio, 4 – Alto, 5 – Muito Alto
Resposta ao Risco: 1 – Evitar, 2 – Mitigar, 3 – Compartilhar, 4 - Aceitar

## ANEXO VIModelo de Plano de Tratamento de Riscos

|  |  |
| --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* |
| **GESTÃO DE RISCOS** |
| **PLANO DE TRATAMENTO DE RISCOS** | **Data:** |
| **Área:** *<< Informar da divisão responsável pela avaliação dos riscos. >>* |
| **Gestor de Risco:** |

1. **Apresentação**

*<< Apresentar de forma resumida o resultado da avaliação de riscos e demonstrar a importância do tratamento dos riscos priorizados >>*

1. **Tratamento dos Riscos**

*<< Apresentar o plano de tratamento de riscos >>*

|  |
| --- |
| **Matriz de Tratamento de Riscos** |
| **ID** | **Evento de Risco** | **Controles** | **Descrição** | **Monitoramento** | **Responsável** | **Prazo** | **Nível de Risco Pretendido** |
|  |  |  |  |  |  |  | AtualPretendido |
|  |  |  |  |  |  |  | AtualPretendido |

|  |
| --- |
| **Explicação sobre cada campo do plano de tratamento.** |
| Evento de Risco | Risco priorizado conforme tabela de priorização de riscos para tratamento. |
| Controles | Controles propostos para o risco em tratamento. |
| Descrição | Descrição detalhada dos tratamentos, incluindo os custos. |
| Monitoramento | Detalhes de como se dará o monitoramento e análise crítica do risco e seu tratamento após sua implementação. |
| Responsável | Servidor responsável pela implementação do tratamento. |
| Prazo | Prazo para a implementação dos controles. |
| Nível de Risco Pretendido | Informar se o tratamento atacou a probabilidade e/ou a consequência do risco, informando os novos valores do cálculo do risco e seu novo nível de risco. |

## ANEXO VIIModelo de Formulário de Comunicação e Consulta

|  |  |
| --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* |
| **GESTÃO DE RISCOS** |
| **FORMULÁRIO DE COMUNICAÇÃO E CONSULTA** | **Data:** |

1. **Atividades**

*<< Todas as atividades de comunicação e consulta durante o processo de avaliação e tratamento dos riscos devem ser descritas na matriz abaixo. >>*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Partes Interessadas e Envolvidas** | **Comunicador** | **Propósito** | **Conteúdo** | **Meio de Comunicação** | **Data** | **Frequência** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## ANEXO VIIIModelo de Relatório de Monitoramento e Análise Crítica

|  |  |
| --- | --- |
| **Gantry 5** | **Unidade Organizacional:***<<Informar a unidade organizacional/diretoria>>* |
| **GESTÃO DE RISCOS** |
| **MONITORAMENTO E ANÁLISE CRÍTICA** | **DATA:** |
| **Área:** *<< Informar da divisão responsável pela etapa de monitoramento e análise crítica. >>* |
| **Gestor de Risco:** |

|  |
| --- |
| **Descrição do Risco** |
| **ID** | **Causas** | **Evento** | **Consequências** |
|  |  |  |  |
| **Análise e Avaliação do Risco (Probabilidade, Impacto e NRI)** |
| **Ano** | **P** | **I** | **Fator do NRI**  | **Nível de Risco Inerente** |
|  |  |  |  |  |
| **Observações sobre a análise e avaliação do risco:***<< Explicar sobre a avaliação da probabilidade, severidade e relevância. >>*  |
| **Controle existente:** |
| **Resposta ao risco:***<< Definir uma resposta ao risco (evitar, mitigar, compartilhar ou aceitar) e justificar. >>* |
| **Controle Novo:***<< Novo controle sugerido após a definição da resposta ao risco. >>* |
| **Execução e Monitoramento do Controle Novo:***<< Breve descrição do novo controle implementado, o andamento da implementação e o responsável. >>* |
| **Apuração do Risco Residual** |
| **Risco Inerente** | **Risco de Controle** | **Risco Residual** |
|  |  |  |
| **Observação:***<< A atividade de Monitoramento e Análise Crítica pode gerar recomendações de melhorias para o tratamento do risco. >>* |

|  |  |
| --- | --- |
| **Avaliação dos controles** | **Risco de Controle** |
| Controles inexistentes. | Muito Alto1,0 |
| Controle fraco, tendem a ser aplicados caso a caso e a responsabilidade é individual, dependendo das pessoas envolvidas. | Alto0,8 |
| Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas. | Médio0,6 |
| Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente. | Baixo0,4 |
| Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco | Muito Baixo0,2 |

## ANEXO IXMapa de Risco



## ANEXO XFluxo do Processo de Trabalho da Gestão de Riscos do PJTO



## ANEXO XI - Atividades do Processo de Gestão de Riscos

|  |
| --- |
| 1. **ARTEFATOS**
 |
| Relatório de contextualização | Definição da abrangência da análise a ser realizada (quais ativos, serviços e processos serão analisados). |
| Relatório de processos/ativos | Lista de processos/ativos com riscos a serem gerenciados. |
| Matriz de identificação de riscos | Lista com os riscos identificados contendo causas e consequências. |
| Matriz de análise e avaliação de riscos | Documento que demonstra o nível de risco encontrado na análise e sua classificação. |
| Relatório de avaliação de riscos | Deve conter as informações da etapa de identificação, análise e avaliação dos riscos, levando em consideração os objetivos do levantamento e o resultado da identificação (quantidade de riscos, de causas e de consequências). |
| Matriz de priorização de riscos | Lista de riscos priorizada, de acordo com os critérios de avaliação de riscos. |
| Plano de tratamento de riscos | Definição de medidas para tratamento dos riscos identificados. |
| Relatório de monitoramento e análise crítica | Análise e definição de resposta ao risco |
| Plano de Comunicação | Estabelece a forma como a equipe envolvida deve se comunicar com as partes interessadas. |

|  |
| --- |
| 1. **FERRAMENTAS**
 |
| SEI | Sistema de processo administrativo eletrônico |
| GPWeb | Sistema de gestão estratégica e gerenciamento de projetos |

|  |
| --- |
| 1. **ATIVIDADES**
 |
| * 1. **Propor plano de gestão de riscos.**
 |
| Descrição | Compreende a proposição de um plano para identificar, avaliar e tratar riscos que podem impactar na atividade-fim do PJTO. |
| Papéis | Líderes do Planejamento Estratégico e/ou Diretor Geral |
| Entradas | Planejamento Estratégico, Processos de Negócio, entre outros. |
| Saídas | Solicitação para os gestores de riscos elaborarem plano de gestão de riscos para determinado processo de negócio ou ativo de informação. |
| Atividades | Formalizar proposta | Deverá ser aberto um processo administrativo para realização do plano. |
| Encaminhar proposta ao gestor de risco | Comitê de Gestão de Riscos |
| Ferramentas | SEI |
| * 1. **Definir o contexto.**
 |
| Descrição | Compreende a proposição dos objetivos, escopo e limites da avaliação de riscos a ser realizada, com a identificação das partes interessadas. |
| Papéis | Gestores de riscos. |
| Entradas | Solicitação para elaboração do plano de gestão de riscos. |
| Saídas | Definição do contexto.  |
| Atividades | Identificar o propósito da avaliação de riscos. |
| Definir o escopo da avaliação de riscos (processos, sistemas, ativos, ambientes). |
| Identificar as partes interessadas e envolvidas no processo. |
| Elaborar relatório de contextualização. |
| Ferramentas | SEI, GPWeb. |
| * 1. **Mapear Ativos/Processos**
 |
| Descrição | Atividade que consiste em elencar os processos e/ou ativos que compõem o escopo, suas características, relacionamentos com sistemas, processos de negócio, responsáveis, tecnologias envolvidas etc. |
| Papéis | Gestores de riscos. |
| Entradas | Escopo da avaliação de riscos; lista de processos/ativos com responsáveis, localidade e função; serviços; sistemas. |
| Saídas | Uma lista de processos/ativos com riscos a serem gerenciados e uma lista dos processos de negócio relacionados aos ativos. |
| Atividades | Identificar os processos e/ou ativos | Identificar quais processos/ativos fazem parte do escopo, quem é o responsável, sua localização e função. |
| Relacionar ativos com os processos de negócio | Relacionar processos/ativos com materiais, equipamentos, sistemas e serviços. |
| Elaborar relatório | Relatório de processos/ativos. |
| Ferramentas | SEI, GPWeb. |
| * 1. **Identificar os riscos**
 |
| Descrição | Atividade que consiste na identificação de ameaças, vulnerabilidades e dos controles já implementados, relacionados aos processos e ativos mapeados. |
| Papéis | Gestores de Riscos. |
| Entradas | Mapeamento dos processos e ativos. |
| Saídas | Lista de cenários de incidentes com suas consequências associadas aos ativos e processos de negócio. |
| Atividades | Coletar informações | Pode ser executada por meio de reuniões (ou outras técnicas recomendadas pela norma ABNT NBR ISO/IEC 31010) entre as equipes envolvidas e o objetivo é listar eventos que possam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto. |
| Identificar os riscos | Produzir uma lista abrangente de riscos, contendo causas e consequências. |
| Elaborar matriz de identificação de riscos. |
| Ferramentas | SEI, GPWeb. |
| * 1. **Analisar e Avaliar os riscos**
 |
| Descrição | Para essa atividade são informados os valores da probabilidade de ocorrência, severidade das consequências e relevância do processo/ativo, a fim de determinar o nível de risco inerente. Com isso, classificar cada risco analisado.  |
| Papéis | Gestores de riscos. |
| Entradas | Identificação de riscos. Avaliação da probabilidade, severidade e relevância. Escala de níveis de risco. |
| Saídas | Determinação do nível de risco inerente, classificação dos riscos, matriz de análise e avaliação de riscos. |
| Atividades | Definir valores para probabilidade e impacto. | Conforme critérios pré-estabelecidos para classificação da probabilidade e impacto. |
| Calcular nível de risco inerente | O nível de risco resulta da multiplicação dos fatores (Probabilidade x Impacto = NRI). |
| Classificar os riscos | Classificação de acordo com a escala de níveis de risco. |
| Elaborar relatório | Relatório de avaliação de riscos. |
| Ferramentas | SEI, GPWeb. |
| * 1. **Definir a prioridade dos riscos**
 |
| Descrição | Atividade que consiste em apresentar uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades. |
| Papéis | Gestores de riscos. |
| Entradas | Análise dos riscos. |
| Saídas | Lista de riscos priorizada, de acordo com os critérios de avaliação de riscos. |
| Atividades | Avaliar riscos | Avaliar os riscos a partir da classificação resultante da análise de riscos e das características dos processos de negócio e ativos envolvidos, bem como escopo definido. |
| Definir resposta ao risco | Definir os critérios para a proposição de tratamento dos riscos, considerando as restrições organizacionais, estruturais e tecnológicas, os requisitos normativos e/ou legais, os controles existentes e a análise custo/benefício. |
| Elaborar matriz de priorização de riscos. |
| Ferramentas | SEI, GPWeb. |
| * 1. **Definir o Apetite ao risco**
 |
| Descrição | Atividade que consiste em definir o nível de exposição e possíveis perdas que o Tribunal vê como aceitável, dados os objetivos e recursos empregados. |
| Papéis | Tribunal Pleno e Presidente. |
| Entradas | Análise dos riscos apresentada pelo Comitê Gestor de Riscos. |
| Saídas | Apetite ao Risco definido de acordo com os critérios de avaliação de riscos. |
| Atividades | Avaliar riscos priorizados | Avaliar os níveis de riscos a partir dos critérios utilizados na tabela de priorização e tratamento. |
| Definir resposta ao risco | Definir diretrizes de resposta ao risco, o nível de responsabilidade e poder de autorização para sua aceitação ou rejeição |
| Elaborar Documento Interno (portaria ou resolução) |
| Ferramentas | SEI, GPWeb, EPROC |
| * 1. **Indicar os tratamentos aos riscos**
 |
| Descrição | Atividade que compreende a elaboração de plano visando à definição das formas de tratamento dos riscos e de implantação de controles, dos responsáveis por sua implementação e prazos estabelecidos. |
| Papéis | Gestores de riscos. |
| Entradas | Lista de riscos priorizada, de acordo com os critérios de avaliação e apetite de riscos. |
| Saídas | Proposta do plano de tratamento de riscos. |
| Atividades | Elaborar plano de tratamento | Para cada risco levantado deve ser identificada a estratégia de tratamento (mitigar, evitar, aceitar ou compartilhar); para cada tratamento, deve ser informada a forma de implementação, o responsável e o prazo de execução. No caso de aceitação, deve ser indicada a justificativa. |
| Consolidar documentação | O relatório de avaliação de risco e a proposta de tratamento devem ser formalizados (SEI) para que sejam avaliados pelo Comitê Gestor de Riscos, que poderá solicitar ajustes ou validá-lo para posterior submissão à consideração superior. |
| Ferramentas | SEI, GPWeb. |
| * 1. **Validar os riscos identificados e as propostas de tratamento**
 |
| Descrição | Nessa etapa, o Comitê Gestor valida o plano de tratamento e pode tecer observações para auxiliar e/ou subsidiar o comitê gestor de riscos na avaliação do documento. |
| Papéis | Comitê Gestor de Riscos |
| Entradas | Plano de tratamento de riscos. |
| Saídas | Decisão aprovando a proposta de plano de tratamento ou determinando correções/ajustes. |
| Atividades | Avaliar a proposição encaminhada | Analisar os resultados da análise e avaliação de riscos realizada e o Plano de Tratamento de Riscos proposto, em especial no que diz respeito aos critérios de aceitação de riscos. |
| Aprovar a proposta | Aprovado o plano de tratamento, encaminha-se para o gestor de riscos aplicar o plano de tratamento. |
| Solicitar ajustes | Não aprovado o documento, devolver ao gestor de risco para correções/ajustes. |
| Ferramentas | SEI, GPWeb |
| * 1. **Avaliar quais processos identificados que impactam diretamente no atingimento dos objetivos estratégicos, táticos e operacionais**
 |
| Descrição | O Comitê de Gestor de riscos avalia a proposta de tratamento de riscos identificando os processos que impactam no atingimento dos objetivos estratégicos. Atividade que compreende a ciência sobre os resultados da análise e avaliação de riscos e a apreciação da proposta do Plano de Tratamento de Riscos. |
| Papéis | Comitê Gestor de Riscos |
| Entradas | Riscos identificados e proposta de tratamento. |
| Saídas | Manifestação do Comitê Gestor de Riscos |
| Atividades | Avaliar a proposta de tratamento de riscos e tecer observações para auxiliar e/ou subsidiar os Líderes do Planejamento Estratégico monitorar e revisar os riscos estratégico e o Diretor Geral para monitorar os riscos táticos e operacionais |
| Ferramentas | SEI, GPweb |
| * 1. **Comunicar ao Comitê de Gestão de Riscos do PJTO sobre quais processos identificados que impactam na gestão estratégica**
 |
| Descrição | As Diretorias e Unidades diversas comunicam o Comitê de Gestão de Riscos do PJTO quais foram os processos identificados que impactam na gestão estratégica. |
| Papéis | Diretorias e/ou Unidades de negócio |
| Entradas | Riscos identificados e proposta de tratamento. |
| Saídas | Manifestação das Diretorias e/ou Unidades de negócio. |
| Atividades | Comunicar ao Comitê de Gestão de Riscos do PJTO sobre quais processos identificados que impactam na gestão estratégica. |
| Ferramentas | SEI, GPWeb |
| * 1. **Analisar e comunicar à presidência do TJ**
 |
| Descrição | O Comitê de Gestão de Riscos do PJTO analisa o documento contendo a manifestação do Comitê Gestor de Riscos sobre quais processos impactam na gestão estratégica e comunica a Presidência do TJ. |
| Papéis | Comitê de Gestão de Riscos do PJTO. |
| Entradas | Manifestação das Diretorias e/ou Unidades de negócio. |
| Saídas | Manifestação do Comitê de Gestão de Riscos do PJTO. |
| Atividades | Analisar a manifestação das Diretorias e/ou Unidades de negócio podendo tecer observações para auxiliar e/ou subsidiar a Presidência na avaliação do documento.  |
| Manter a Presidência do TJ informada sobre os riscos que podem impactar a gestão estratégica. |
| Ferramentas | SEI, GPWeb |
| * 1. **Determinar a aplicação do plano de tratamento**
 |
| Descrição | Atividade que autoriza a execução do plano de tratamento.  |
| Papéis | Comitê de Gestão de Riscos do PJTO |
| Entradas | Riscos identificados e proposta de tratamento. |
| Saídas | Implementação do plano de tratamento. |
| Atividades | Determinar os gestores de riscos a aplicar o plano de tratamento. |
| Ferramentas | SEI, GPWeb |
| * 1. **Executar o plano de tratamento**
 |
| Descrição | Nessa atividade, as áreas da Diretorias e/ou Unidades de negócio implementam os controles para mitigar os riscos elencados, dentro de um prazo definido no plano de tratamento. |
| Papéis | Gestores de riscos. |
| Entradas | Plano de tratamento de riscos. |
| Saídas | Controles implementados. |
| Atividades | Delegar as atividades de implementação dos controles | A implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no plano de tratamento. |
| Gerenciar implementação | Cada área deverá planejar a execução das ações, a fim de executá-las no prazo e forma ajustados. |
| Registrar a execução das ações | No relatório de monitoramento e análise crítica deve ser registrada a execução das atividades, o que permitirá o acompanhamento da implementação do Plano. |
| Ferramentas | SEI, GPWeb |
| * 1. **Monitorar**
 |
| Descrição | Esta fase tem por objetivo monitorar a execução do Plano, com a finalidade de assegurar sua implementação dentro dos prazos definidos. Além disso, monitora também os riscos a fim de evitar que eles se concretizem. |
| Papéis | Gestores de riscos. |
| Entradas | Plano de tratamento de riscos, relatório de avaliação de riscos e relatório de respostas aos riscos. |
| Saídas | Implementação do plano e relatório de resposta ao risco. |
| Atividades | Monitorar o plano | O gestor de risco é o responsável por acompanhar o andamento das ações delegadas às equipes técnicas, a fim de aferir sua correspondência com a atividade definida no plano, bem como o cumprimento dos prazos ali estabelecidos. |
| Comunicação dos riscos | Informar às partes interessadas o nível de risco analisado e avaliado e possíveis alterações. |
| Monitorar os riscos | Analisar e monitorar os riscos já avaliados para verificar se alguma ocorrência pode ter modificado os níveis de risco, ensejando alguma ação para controlá-los. |
| Ferramentas | SEI, GPWeb |