# PROCESSO DE GESTÃO DE RISCOS DE TIC

## 1. Introdução

Este processo tem como objetivo aumentar as chances de o TJPA atingir seus objetivos relacionados aos assuntos de TIC da instituição, por meio do uso de abordagens sistematizadas de Gestão de Risco, a qual consiste em um conjunto de atividades que visam identificar, analisar, tratar e monitores os riscos inerentes às ações do Tribunal.

## 2. Atividades

### 2.1. Definir objeto da Gestão de Riscos

O objeto que será alvo dessa Gestão pode ser qualquer processo de trabalho, atividade, projeto, iniciativa ou ação do plano de TIC, assim como os recursos que dão suporte à realização dos objetivos cotidianos das áreas interessadas nesse Processo. O objeto da gestão de riscos proposto deve ser aprovado pela Secretaria de Informática.

### 2.2. Definir responsável pela gestão dos riscos do objeto

Uma equipe deve ser constituída para a execução da gestão de riscos, a qual será responsável pelas principais etapas da Gestão de Riscos do objeto em questão, durante todo o ciclo de vida do processo.

### 2.3. Definir contexto dos riscos

Aqui o responsável pela Gestão de Riscos do objeto em questão deve cumprir uma sequência de passos para submeter esse contexto à aprovação da Secretaria de Informática:

- Identificar os ativos que suportam o objeto: o objeto da gestão de riscos, via de regra possui um ou mais ativos tangíveis e/ou intangíveis que o suportam, e que podem ser classificados como potenciais fontes de risco.
- Identificar as partes interessadas do objeto e do resultado: após essa identificação é também necessário que essas partes sejam consultadas a respeito de suas necessidades e expectativas em relação aos objetivos e resultados do objeto. Como parte desse levantamento deve-se utilizar certas ferramentas do processo, como a análise de stakeholders, matriz RACI e matriz de responsabilidades;
- Identificar os fatores do ambiente que podem afetar o alcance dos objetivos ou dos resultados: o ambiente no qual a organização procura definir e alcançar os objetivos e resultados do objeto é composto pelos contextos externo e interno

em que o mesmo está inserido, e que podem afetar a definição e o alcance desses objetivos e resultados.

- Identificar quais objetivos ou resultados devem ser alcançados pelo objeto: essencial para a definição do contexto já que a Gestão de Riscos deve estar sempre alinhada com os objetivos da instituição;
- Estabelecer critérios para analisar e avaliar os níveis de risco do objeto: é importante que se estabeleça critérios iniciais para avaliar a relevância dos riscos e para apoiar a definição do limite de exposição de cada risco analisado, e que os critérios sejam alinhados à estrutura da Gestão de Riscos, bem como personalizados conforme o escopo e objetivos específicos do objeto em questão.

## 2.4. Homologar contexto

Para que o contexto de riscos de aprovado, é necessário a inclusão de, pelo menos, os seguintes elementos essenciais:

- Descrição concisa dos objetivos-chave e dos fatores críticos: essencial para que se tenha êxito. Aqui é importante também que se faça uma análise dos fatores do ambiente interno e externo (ex.: análise SWOT);
- Análise de partes interessadas e seus interesses: a exemplo das análises de stakeholders, RACI e matriz de responsabilidades;
- Critérios bem definidos: com base nos quais os riscos serão analisados, avaliados e priorizados

## 2.5. Identificar riscos

A identificação dos riscos de TIC compreende o reconhecimento e descrição dos riscos relacionados a um determinado objeto de gestão, envolvendo a identificação de possíveis fontes de riscos, eventos, causas e consequências. Como parte da atividade, uma lista abrangente de todos os riscos identificados deve ser criada, incluindo, para cada risco, as fontes e eventos que podem ter algum impacto na consecução dos objetivos e resultados identificados na etapa de estabelecimento do contexto.

## 2.6. Analisar riscos

O propósito da análise de riscos é compreender a natureza do risco e suas características. Essa análise envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidades, eventos, cenários, controles e sua eficácia. Essa análise deve conter pelo menos as seguintes ações:

- Avaliar a probabilidade de ocorrência do risco: de maneira complementar ao item anterior, essa avaliação é essencial para a definição dos limites de exposição de cada risca.
- Avaliar o impacto: a avaliação do impacto do risco na realização dos objetivos e dos resultados do objeto, constitui uma das dimensões de base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos.
- Determinar o nível do risco: o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos e nos resultados do objeto.
- Propor o limite de exposição ao risco: o limite trata-se do nível de risco ao qual a Secretaria de Informática entende como nível máximo aceitável para o objeto alvo da Gestão de Riscos

## 2.7. Definir limite de exposição ao risco

Esse limite deverá ser apreciado e definido pela Secretaria de Informática, especialmente para os casos em que as análises realizadas indicarem riscos em assuntos estratégicos à Instituição. Essa definição serve de base para as ações de monitoramento dos riscos em questão.

## 2.8. Definir plano de ação

O objetivo aqui é definir os procedimentos a serem realizados em situações em que as ameaças previstas na Gestão de Riscos forem materializadas, de maneira a mitigar eventuais impactos, de forma clara e passível de monitoramento pelas áreas envolvidas. É interessante que esse plano identifique claramente a ordem em que os passos do tratamento de riscos deverão ser implantados.

## 2.9. Monitorar riscos

O monitoramento e análise crítica é etapa essencial da gestão de riscos e tem por finalidade detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco, o que pode requerer revisão dos tratamentos de riscos e suas prioridades, bem como identificar riscos emergentes. O monitoramento de riscos deve:

- Ser contínuo, por parte da área responsável;
- Ser objeto de auditorias por áreas que forneçam avaliações independentes;
- Assegurar que o registro de riscos esteja sempre atualizado, e possua os documentos que formalizem a sua realização.

## 3. Relacionamentos

O processo de Gestão de Riscos tem interface com os seguintes processos:

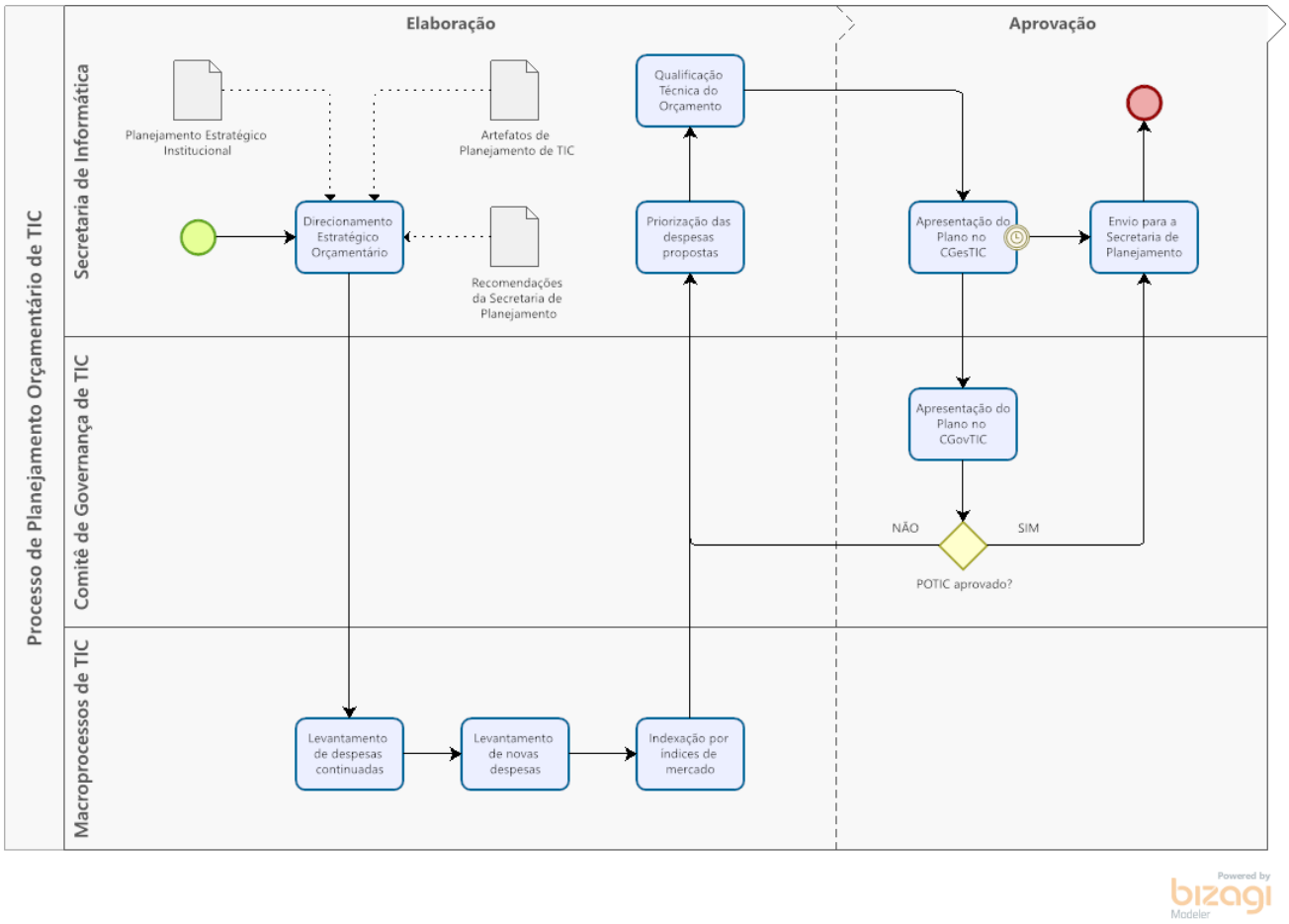
### 3.1 Gerenciamento de incidentes

De maneira complementar à Gestão de Riscos, o gerenciamento de incidentes visa mitigar fatores que podem levar o negócio a ter ocorrências que levam a prejuízos financeiros e comerciais.

### 3.2 Gerenciamento de mudanças

Sempre que há mudanças em ativos ou serviços de TIC, é comum que haja riscos associados, os quais são também analisados do Gerenciamento de Mudanças. Cabe destacar que nesse quesito os processos em questão não são redundantes, e sim complementares.

## 4. O Processo


Processo de Planejamento Orçamentário de TIC
Secretaria de Informática
Comitê de Governança de TIC
Macroprocessos de TIC
Elaboração
Aprovação
Planejamento Estratégico Institucional
Artefatos de Planejamento de TIC
Direcionamento Estratégico Orçamentário
Recomendações da Secretaria de Planejamento
Qualificação Técnica do Orçamento
Priorização das despesas propostas
Apresentação do Plano no CGesTIC
Envio para a Secretaria de Planejamento
Apresentação do Plano no CGovTIC
NÃO
SIM
POTIC aprovado?
Levantamento de despesas continuadas
Levantamento de novas despesas
Indexação por índices de mercado
Powered by bizagi Modeler

## 5. Papéis e Responsabilidades

| Papel | Quem exerce | Responsabilidades |
|---|---|---|
| Secretaria de Informática | Secretário de Informática ou servidor indicado por este | • Analisar relatórios e acompanhar indicadores de desempenho;<br>• Definir objetos da Gestão de Riscos;<br>• Homologar contexto da Gestão de Riscos;<br>• Definir limite de exposição ao risco;<br>• Propor e autorizar mudanças no processo;<br>• Prover recursos para a execução das atividades do processo, bem como contribuir para a resolução de eventuais problemas com o processo. |
| Responsável pela Gestão do Risco | Servidor da área de TIC do TJPA responsável pelo gerenciamento operacional das atividades do processo, garantindo a sua correta execução e desempenho. | • Produzir relatórios e indicadores;<br>• Garantir a boa execução do processo;<br>• Registrar as ocorrências da execução do processo;<br>• Interagir com os demais gerentes de processos, a fim de manter o alinhamento com estes;<br>• Ajudar com a resolução de problemas com a execução do processo.<br>• Definir contexto dos riscos;<br>• Identificar e analisar os riscos;<br>• Definir plano de ação;<br>• Monitorar riscos. |