SETIC
Superintendência Estadual de
Tecnologia da Informação
e Comunicação

RONDÔNIA
Governo do Estado

# Modelo de Gestão de Riscos

2025

**GOVERNO DO ESTADO DE RONDÔNIA**

Marcos José Rocha dos Santos
Governador

Sérgio Gonçalves da Silva
Vice-Governador

**SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**

Delner Freire
Superintendente

Gabriel Carrijo Bento Teixeira
Diretor Técnico

**EQUIPE DE ELABORAÇÃO**

Tiago Lopes de Aguiar
Maria Gabriela dos Santos Galvão Almeida
Luáh de Oliveira Duarte

**EQUIPE DE REVISÃO**

Comissão de Supervisão de Gestão de Riscos CSGR da Setic
(Portaria Setic nº 41, de 11 de fevereiro de 2025)

**Coordenação do CSGR**

Tiago Lopes de Aguiar – Titular
Pedro Alexandre de Sá Barbosa – Suplente

**Secretariado do CSGR**

Maria Gabriela dos Santos Galvão Almeida – Titular
Ana Paula da Silva Rodrigues – Suplente

| **Membros Titulares – CSGR** | **Membros Suplentes – CSGR** |
|---|---|
| Ronald Lázaro Borges Ribeiro | Sâmara Ascoli de Queiroz |
| Luma Damon de Oliveira Melo | Regiane Nogueira Frota |
| Daltro Barbosa Filho | André Luíz da Silva Cruz |
| Frederico Nakahara Silva | José Severino dos Santos |
| Raul Chiullo Silva | Ramissés Evangelista Araújo |
| Diêgo Alexandre Duarte | Celso Dias de Oliveira Junior |
| João Thomas de Souza Telles | Henrique Ferreira Guimarães |

# VERSÃO

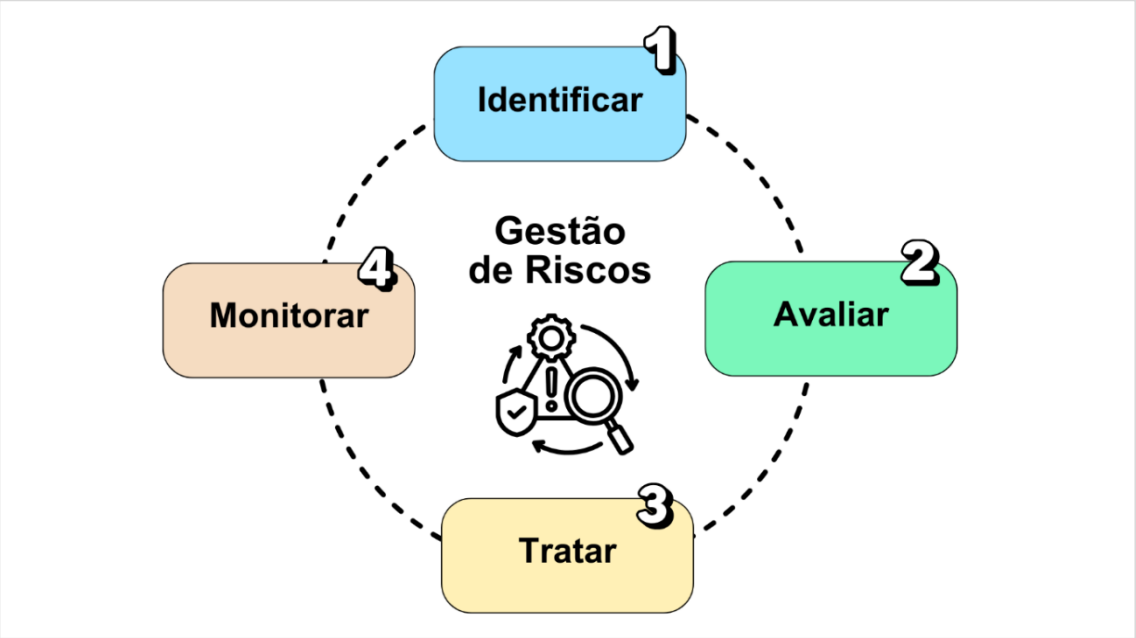
| VERSÃO | DATA | AUTOR | AÇÃO |
|---|---|---|---|
| 1.0 | 01/10/2025 | Equipe de Elaboração | Primeira versão do Modelo de Gestão de Riscos (MGR) da Setic. |

# SUMÁRIO

# INTRODUÇÃO

A gestão de riscos consiste no processo para **identificar, avaliar, tratar e monitorar** potenciais eventos ou situações para aumentar a chance de alcance dos objetivos institucionais. Passou a ser considerada estratégia fundamental para a efetivação das atividades de negócios dentro de ambientes corporativos, não sendo diferente na Administração Pública. A Figura 1 apresenta o diagrama do processo de gestão de riscos, facilitando a identificação de seus processos.

Figura 1 - Diagrama do processo de gestão de riscos.




Fonte: Elaboração própria.

Os órgãos e entidades públicas devem se preocupar em gerir seus riscos em prol da sociedade a qual servem, visando ofertar serviços de melhor qualidade para seus usuários, buscando a eficiência e a efetividade em seus processos de negócios.

Nessa seara é importante salientar que a gestão de riscos se apresenta como instrumento de suma importância para a promoção da qualidade na prestação de seus serviços, buscando mitigar impactos negativos e agir de forma proativa para evitar impasses e prejuízos ao erário.

Portanto, a Superintendência Estadual de Tecnologia da Informação e Comunicação (Setic), procurando se organizar e promover medidas eficazes de controle de riscos, institui a sua Política de Gestão de Riscos por meio da Portaria nº 151, de 17 de junho de 2025, que prevê, como um dos seus objetivos, a implantação do Modelo de Gestão Riscos (MGR), que se traduz no presente documento.

Dessa forma, o presente instrumento, elaborado com base em modernas práticas de gestão de riscos como normas da série ABNT NBR ISO/IEC 31000, *Enterprise Risk Management* elaborado pelo *Committee of Sponsoring Organization of the Treadway Commission* (COSO-ERM) e *Project Management Institute* (PMI), tem por objetivo traçar diretrizes sobre a gestão de riscos no âmbito da Setic, orientando e promovendo medidas de boas práticas para os gestores de riscos.

# 1 DEFINIÇÃO DE RISCO

O presente Modelo de Gestão de Riscos (MGR) estabelece que risco é:

> 🚩 **Qualquer evento** que, se ocorrer,
> **afeta** o alcance de algum **objetivo** organizacional.

Os riscos podem ser identificados a partir da seguinte pergunta:

> Quais eventos podem afetar o
> alcance dos objetivos organizacionais?

# 2 GESTÃO DE RISCOS

## 2.1 ASPECTOS GERAIS

No âmbito da Superintendência Estadual de Tecnologia da Informação e Comunicação (Setic), a gestão de riscos é coordenada pela Comissão de Supervisão e Gestão de Riscos (CSGR), criada por meio da Portaria Setic nº 41, de 11 de fevereiro de 2025, que institui o seu sistema de Governança. A CSGR tem por objetivo avaliar, planejar e orientar ações de gestão de riscos, bem como assessorar em tais atividades, especialmente quanto à implementação de diretrizes, políticas, normas e procedimentos, dando suporte aos diversos níveis hierárquicos da Setic na integração de suas atividades e processos à gestão de riscos (arts. 1ª e 2º do Apêndice II). Além disso, funciona como unidade de apoio ao Comitê Gestor para tratar de temas correlatos (§ 4º do art. 17).

A referida Comissão é composta pelas seguintes setoriais:

1. Assessoria de Conformidade;
2. Coordenadoria de Gestão Estratégica;
3. Gerência de Projetos;
4. Coordenadoria de Segurança da Informação;
5. Coordenadoria Administrativa e Financeira;
6. Coordenadoria de Infraestrutura e Serviços;
7. Coordenadoria de Desenvolvimento de Sistemas; e
8. Coordenadoria de Análise e Gestão de Dados.

De acordo com o art. 9º do Apêndice II da Portaria Setic nº 41, de 11 de fevereiro de 2025, são competências da CSGR:

1. Elaborar e propor ao CGGE políticas, planos, diretrizes, metodologias e mecanismos de comunicação e monitoramento relacionados à gestão de riscos;

2. assessorar as unidades internas da SETIC, na implementação das metodologias e dos instrumentos para gestão de riscos;

3. atuar como facilitador na integração dos agentes responsáveis pela gestão de riscos e prestar assessoria técnica sobre regulamentos e padrões exigidos na condução das atividades correlatas;

4. propor a capacitação e a disseminação da cultura nos assuntos de gestão de riscos;

5. orientar e emitir recomendações sobre gestão de riscos;

6. propor método de priorização de processos e categorias de riscos para gestão de riscos;

7. propor limites de exposição a riscos e níveis de conformidade, bem como limites de alçada para exposição a riscos;

8. dar conhecimento ao CGGE, quando tiver ciência, dos riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público que ainda não foram relacionados;

9. articular a troca de informações sobre a gestão de riscos entre todos os níveis no âmbito da SETIC;

Dentre as ações da CSGR, destaca-se a elaboração da Política de Gestão de Riscos, instituída pela Portaria Setic nº 151, de 17 de junho de 2025, cujos objetivos, destacados em seu art. 4º, são:

1. fortalecer a imagem institucional, promover a eficiência processual e monitorar os ambientes internos e externos que interferem no alcance dos objetivos;
2. implantar modelo de gestão de riscos;
3. implementar governança para a manutenção e contínuo aperfeiçoamento do modelo de gestão de riscos;
4. identificar, avaliar, tratar e monitorar os principais riscos a que a Setic está exposta; e
5. auxiliar o gestor de riscos no processo de tomada de decisões.

A Política de Gestão de Riscos também prevê que a Assessoria de Conformidade, em articulação com a CSGR, elaborará a definição e implantação do presente Modelo de Gestão de Riscos (MGR). Consolida ainda que a gestão de riscos compete aos gestores de riscos em suas esferas de atuação.

Ressalta-se que a identificação dos riscos está diretamente condicionada ao momento em que ocorre a sua avaliação, pois os mesmos riscos podem assumir características distintas conforme o período em que são analisados.

Outro fator importante é que os riscos que já foram tratados ou que possuem controles efetivos podem ser desconsiderados, desde que sejam verificados se os controles ainda são adequados ao cenário atual, podendo exigir aprimoramento, expansão ou até sua eliminação. Controles ineficazes ou mal dimensionados podem criar a falsa percepção de que o risco está mitigado, afastando-o indevidamente do acompanhamento contínuo pelo gestor de riscos.

## 2.2 PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades na aplicação deste Modelo de Gestão de Riscos (MGR) se mostram importantes para que tenha efetividade. Dessa forma, o Quadro 1, a seguir, detalha sua operacionalização:

Quadro 1 - Papéis e responsabilidades no Modelo de Gestão de Riscos (MGR).

| Papel | Responsável | Responsabilidades |
|---|---|---|
| Instância máxima na Gestão de Riscos | Comitê de Governança e Gestão Estratégica (CGGE) | • subsidiar a alta gestão na avaliação e aprovação das iniciativas de gestão de riscos. |
| Instância intermediária na Gestão de Riscos | Comissão de Supervisão de Gestão de Riscos (CSGR) | • assessorar as unidades internas da Setic na implementação das metodologias e instrumentos para gestão de riscos;<br>• orientar e emitir recomendações sobre gestão de riscos;<br>• propor método de priorização de processos e categorias para a gestão de riscos;<br>• propor limites de exposição a riscos e níveis de conformidade;<br>• dirigir, avaliar e monitorar a gestão de riscos na Setic, com o auxílio dos Comitês e Comissões setoriais; e<br>• aprovar e monitorar os Plano de Respostas a Riscos (PRRs). |

| | | |
|---|---|---|
| Gestor de Riscos | Titular da respectiva unidade ou coordenadoria | • elaboração do Plano de Respostas a Riscos (PRR);<br>• escolher os planos, processos de trabalho e projetos, conforme dimensão dos seus impactos cujos riscos deverão ser gerenciados e tratados prioritariamente;<br>• definir o escopo da gestão de riscos;<br>• tomar ciência e aprovar a identificação, análise e tratamento dos riscos (Plano de Respostas a Riscos - PRR);<br>• acompanhar o monitoramento dos riscos;<br>• estabelecer prazos para a implementação da gestão dos riscos identificados; e<br>• submeter às instâncias superiores os riscos ou ações de tratamento que ultrapassem sua alçada. |
| Responsáveis designados no Plano de Respostas a Riscos (PRR) | Pessoa responsável pelo cumprimento das determinações do Plano de Respostas a Riscos (PRR) | • fornecer informações sobre o escopo da gestão de riscos;<br>• reunir a documentação relevante sobre o escopo;<br>• identificar a avaliar os riscos;<br>• propor tratamento aos riscos, juntamente com o responsável pelo objetivo da gestão de riscos;<br>• executar as ações de tratamento das propostas;<br>• fornecer informações sobre a execução. |

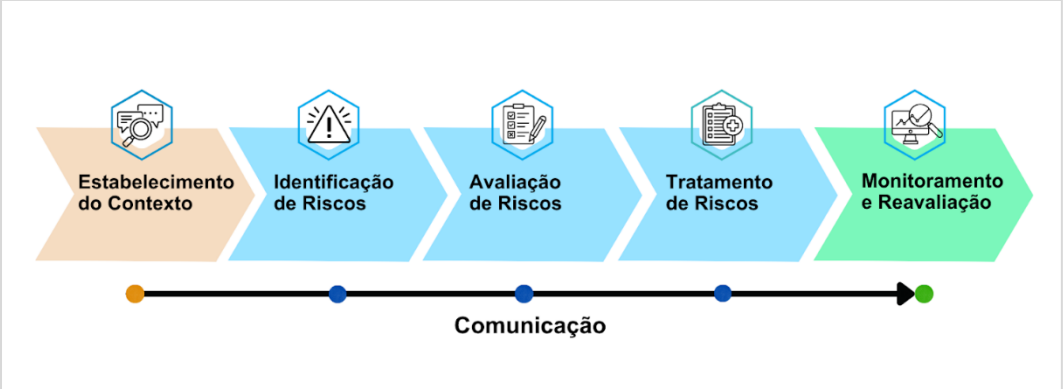
| | | |
|---|---|---|
| Responsáveis pela aplicação transdisciplinar da gestão de riscos | Servidores e Coordenadorias | • apoiar as ações de gestão de riscos em suas esferas de competência. |
| Responsável pela elaboração do Modelo de Gestão de Riscos (MGR) | Assessoria de Conformidade (ASCF) | • elaborar o Modelo de Gestão de Riscos (MGR), em articulação com o CSGR. |

Fonte: Elaboração própria.

# 3 DETALHAMENTO DO MODELO DE GESTÃO DE RISCOS (MGR)

O presente Modelo de Gestão de Riscos (MGR) propõem um processo dividido em 5 (cinco) fases, todas conectadas entre si e com sua respectiva relevância, conforme demonstrado no diagrama da Figura 2, a seguir:

Figura 2 - Diagrama do Modelo de Gestão de Riscos (MGR).




Fonte - Elaboração própria.

Cada uma dessas fases será detalhada nos subtópicos seguintes deste documento.

## 3.1 ESTABELECIMENTO DO CONTEXTO

O estabelecimento do contexto é uma das fases mais importantes do processo de gestão de riscos, pois é o momento em que as setoriais

responsáveis devem promover os ajustes necessários para tornar o Modelo de Gestão de Riscos (MGR) aderente à sua realidade.

Os envolvidos nessa fase do processo são o **gestor do risco e os responsáveis designados no Plano de Respostas a Riscos** (PRR), que devem:

a. **definir o escopo**
b. **apresentar o MGR à sua equipe.**

**a) Definir o escopo**

Momento em que o gestor de riscos deverá designar o responsável ou responsáveis pelo levantamento dos riscos e pela elaboração do Plano de Respostas a Riscos (PRR), estabelecendo as delimitações de sua área de atuação e definindo o escopo de implementação conforme competências legais de sua setorial. Deve-se ainda estabelecer um *roadmap* para a realização do levantamento dos riscos e elaboração do PRR, que proporcionará uma visão geral sobre os principais passos que as setoriais devem seguir para a implementação da gestão de riscos.

Dessa forma, a gestão dos riscos deve ficar ligadas às responsabilidades institucionais setoriais, devendo apresentar, como resultado, os seguintes entregáveis:

- definição do escopo de implementação do MGR; e
- designação de responsável ou responsáveis pelo levantamento dos riscos e elaboração do Plano de Respostas a Riscos (PRR); e
- criação de um *roadmap* para a realização do levantamento dos riscos e elaboração do PRR (Apêndice A).

No Apêndice A está disponível um exemplo de *roadmap* para a implementação da gestão de riscos.

**b) Apresentar o MGR à sua equipe**

Momento em que o gestor de riscos deverá se organizar e apresentar o MGR para a sua equipe, enfatizando a distribuição dos papeis e responsabilidades dos agentes, apresentando o *roadmap* que norteará a realização das atividades de levantamento dos riscos e elaboração do PRR. Destacam-se os seguintes entregáveis:

- apresentação do MGR à equipe; e
- apresentação da linha do tempo para implementação da gestão de riscos no setor.

## 3.2 IDENTIFICAÇÃO DE RISCOS

A identificação de riscos consiste em levantar os eventos que podem afetar negativamente o alcance dos objetivos organizacionais, partindo da análise e seleção prioritária de processos de trabalho, projetos, planos ou de ações pontuais em análise.

Os envolvidos nessa fase do processo são o **gestor do risco e os responsáveis designados no Plano de Respostas a Riscos** (PRR), que devem:

a. **Reunir informações; e**
b. **Identificar os riscos.**

**a) Reunir informações**

Consiste no processo de reunir as informações relevantes para a identificação dos riscos associados ao escopo de atuação da setorial. Deverão ser levantadas as ações já realizadas, promovendo um diagnóstico situacional dos processos de negócios que serão objeto de tal análise. Deve apresentar como resultado os seguintes entregáveis:

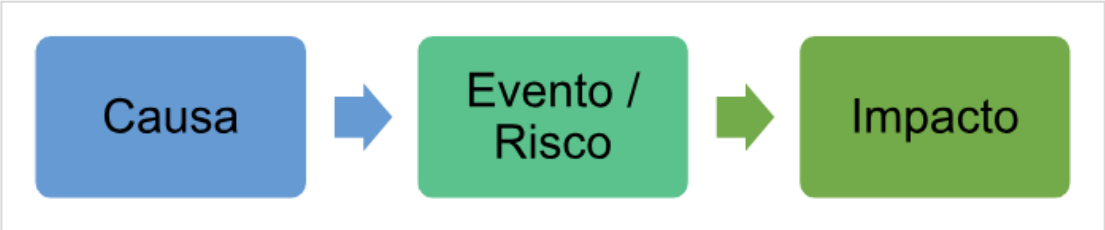
- informações relevantes para identificar os riscos.

**b) Identificar os riscos**

A identificação do risco pode estar associada a processos de trabalho, projetos, planos ou de ações pontuais, tratando-se do processo de determinar os eventos, internos ou externos, que possam impactar negativamente no alcance dos objetivos institucionais.

Nesse momento, é importante diferençar problemas de riscos. O problema é um fato, que está gerando impacto no alcance dos objetivos organizacionais. Já o risco é algo que pode ocorrer e impactar negativamente o objetivo em análise. O risco é formado por 3 (três) componentes, conforme ilustrado na Figura 3 a seguir:

Figura 3 – Composição do risco.




Fonte: Elaboração própria.

Dessa forma, um risco pode ser descrito da seguinte forma:

> Devido a **<CAUSA>**, poderá ocorrer **<EVENTO/RISCO>**, levando ao **<IMPACTO>** afetando o **<OBJETIVO INSTITUCIONAL>.**

**Exemplo:**

> *"Devido a **exploração de vulnerabilidades no Sistema X**, poderá ocorrer **o vazamento de dados pessoais**, levando **à aplicação de sanções administrativas e civis contra Governo do Estado** afetando a responsabilidade da Setic de **assegurar os sistemas sob sua responsabilidade, garantindo qualidade e rigor técnico**."*

Dentre as boas práticas na atividade de identificação dos riscos, é importante destacar a sua classificação em categorias, o que colabora com as ações de tratamento e consolidações das ações estratégicas nesse sentido. No Apêndice B estão descritas algumas abordagens que podem ser utilizadas para a identificação de riscos, bem como a divisão destes em categorias.

A presente etapa deve ser encerrada apresentando-se o seguinte entregável:

- Identificação e categorização dos riscos (Apêndice C).

## 3.3 AVALIAÇÃO DE RISCOS

A avaliação do risco deve resultar na determinação do seu nível de criticidade, que ocorre por meio da relação entre a probabilidade e o impacto, devendo considerar as ações de controle já existentes.

A criticidade é feita para cada risco, por meio da multiplicação do valor da probabilidade pelo favor do impacto, conforme indicado na Figura 4 a seguir:

Figura 4 – Fórmula para encontrar o nível de criticidade do risco.


Fonte: Elaboração própria.

Os envolvidos nessa fase do processo são o **gestor do risco e os responsáveis designados no Plano de Respostas a Riscos** (PRR), que devem:

a. **Avaliar a probabilidade;**
b. **Avaliar impacto;**
c. **Calcular o nível do risco; e**
d. **Elaborar mapa de riscos.**

**a) Avaliar probabilidade**

A probabilidade está relacionada com a possibilidade do risco se materializar, devendo ser atribuída observando os fatores analisados, a causa e a linha do tempo:

Qual a probabilidade da **<CAUSA>** desencadear
o **<EVENTO/RISCO>**,
na **<LINHA DO TEMPO DEFINIDA>**?

**Exemplo:**

*"Qual a probabilidade da **exploração de vulnerabilidades no Sistema X** desencadear **o vazamento de dados pessoais, considerando os últimos 12 meses**?"*

Para a definição da probabilidade, deve-se considerar o Quadro 2 a seguir:

Quadro 2 – Definição da probabilidade do risco

| Papel | Responsável | Responsabilidades |
|---|---|---|
| 5 | Praticamente certo | Evento **repetitivo e constante**, se reproduz muitas vezes, seguidamente, de maneira assídua, numerosa e não raro de modo acelerado. |
| 4 | Muito provável | Evento **usual**, corriqueiro. Devido à sua ocorrência habitual, seu histórico é amplamente conhecido por parte dos gestores e operadores do processo. |
| 3 | Provável | Evento **esperado**, de frequência reduzida, e com histórico de ocorrência parcialmente conhecido pelos gestores e operadores do processo. |
| 2 | Pouco provável | Evento **inesperado**, casual. Muito embora raro, há histórico de ocorrência parcialmente conhecido por parte dos gestores e operadores do processo. |
| 1 | Raro | Evento **extraordinário** para os padrões conhecidos da gestão e operação do processo. Não há histórico disponível para sua ocorrência. |

Fonte: Elaboração própria.

A presente etapa deve ser encerrada apresentando-se o seguinte entregável:

- Preenchimento da probabilidade na avaliação de riscos, planilha de identificação e avaliação de riscos (Apêndice C).

**b) Avaliar impacto**

O impacto está relacionado com as consequências negativas que podem ocorrer se o risco analisado se materializar:

Ocorrendo a **<CAUSA>** que originou o **<EVENTO/RISCO>**, qual impacto no alcance do **<OBJETIVO>**?

**Exemplo:**

*"Ocorrendo a **exploração de vulnerabilidades no Sistema X** que originou **o vazamento de dados pessoais**, qual impacto no alcance da responsabilidade da Setic de **proteger os sistemas sob sua responsabilidade, garantindo qualidade e rigor técnico**?"*

Para a definição do impacto, deve-se considerar o Quadro 3 a seguir:

Quadro 3 – Definição do impacto do risco.

| Papel | Responsável | Responsabilidades |
|---|---|---|
| 5 | Praticamente certo | Evento **repetitivo e constante**, se reproduz muitas vezes, seguidamente, de maneira assídua, numerosa e não raro de modo acelerado. |
| 4 | Muito provável | Evento **usual**, corriqueiro. Devido à sua ocorrência habitual, seu histórico é amplamente conhecido por parte dos gestores e operadores do processo. |

| | | |
|---|---|---|
| 3 | Provável | Evento **esperado**, de frequência reduzida, e com histórico de ocorrência parcialmente conhecido pelos gestores e operadores do processo. |
| 2 | Pouco provável | Evento **inesperado**, casual. Muito embora raro, há histórico de ocorrência parcialmente conhecido por parte dos gestores e operadores do processo. |
| 1 | Raro | Evento **extraordinário** para os padrões conhecidos da gestão e operação do processo. Não há histórico disponível para sua ocorrência. |

Fonte: Elaboração própria.

A presente etapa deve ser encerrada apresentando-se o seguinte entregável:

- **Preenchimento do impacto** na avaliação de riscos, planilha de identificação e avaliação de riscos (Apêndice C).

**c) Calcular o nível do risco**

O nível do risco será o resultado da multiplicação da probabilidade e do impacto, podendo variar de 1 a 25, conforme metodologia adotada neste Modelo de Gestão de Riscos (MGR):

O **<EVENTO/RISCO>** tem **<PROBABILIDADE>** e **<IMPACTO>**. Logo, o nível do risco é igual a **<PROBABILIDADE x IMPACTO>**.

**Exemplo:**

*"O **vazamento de dados pessoais** tem **probabilidade 2 (pouco provável** e **impacto 5 (muito alto)**. Logo, o nível do risco é igual a **10 (2x5)**."*

A presente etapa deve ser encerrada apresentando-se o seguinte entregável:

- **Preenchimento do nível do risco** na avaliação de riscos, planilha de identificação e avaliação de riscos (Apêndice C).

**d) Elaborar mapa de riscos**

O mapa de riscos consiste no enquadramento de cada um dos eventos encontrados dentro da matriz de riscos, facilitando a sua identificação de forma global. Deve considerar a definição de faixas de níveis de riscos e da criticidade de cada um deles, considerando a probabilidade e o impacto.

O presente Modelo de Gestão de Riscos (MGR) adotou a matriz apresentada na Figura 5 a seguir:

Figura 5 – Matriz de riscos.

| **NÍVEIS DE RISCO**<br>Extremo<br>Alto<br>Médio<br>Baixo<br>Irrelevante | | **PROBABILIDADE** | | | | |
|---|---|---|---|---|---|---|
| | | **1**<br>Raro | **2**<br>Pouco provável | **3**<br>Provável | **4**<br>Muito provável | **5**<br>Praticamente certo |
| **IMPACTO** | **5**<br>Muito alto | 5 | 10 | 15 | 20 | 25 |
| | **4**<br>Alto | 4 | 8 | 12 | 16 | 20 |
| | **3**<br>Médio | 3 | 6 | 9 | 12 | 15 |
| | **2**<br>Baixo | 2 | 4 | 6 | 8 | 10 |
| | **1**<br>Muito baixo | 1 | 2 | 3 | 4 | 5 |

Fonte: Elaboração própria.

Com base na matriz e considerando o nível de criticidade dos riscos identificados, é possível elaborar o mapa de riscos **conforme exemplo** retratado na Figura 6 a seguir, onde foram inseridos os Eventos de Riscos (ER) correspondentes:

**Exemplo:**

Figura 6 – Exemplo de mapa de riscos.

| **NÍVEIS DE RISCO**<br>Extremo<br>Alto<br>Médio<br>Baixo<br>Irrelevante | | **PROBABILIDADE** | | | | |
|---|---|---|---|---|---|---|
| | | **1**<br>Raro | **2**<br>Pouco provável | **3**<br>Provável | **4**<br>Muito provável | **5**<br>Praticamente certo |
| **IMPACTO** | **5**<br>Muito alto | ER.1 | | ER.10 | | ER.4<br>ER.9 |
| | **4**<br>Alto | | ER.7 | | | |
| | **3**<br>Médio | | | ER.3 | | |
| | **2**<br>Baixo | ER.6 | | | ER.4<br>ER.9 | |
| | **1**<br>Muito baixo | | ER.5 | | | |

Fonte: Elaboração própria.

Dependendo da classificação da criticidade dos riscos e de sua categorização, a Setic poderá regulamentar a sua disposição para aceitá-los, de acordo com o apetite a risco.

A presente etapa deve ser encerrada apresentando-se o seguinte entregável:

- **Mapa de riscos**, conforme a Figura 6.

## 3.4 TRATAMENTO DE RISCOS

Trata-se da fase em que os riscos deverão ser tratados, considerando o nível do apetite a risco definido, momento em que deverá ser elaborado o plano de respostas, definindo as medidas que serão adotadas visando o tratamento de cada um dos riscos identificados e selecionados.

Os envolvidos nessa fase do processo são o **gestor do risco, os responsáveis designados no Plano de Respostas a Riscos** (PRR) e **Comissão de Supervisão de Gestão de Riscos** (CSGR), que devem:

a. **Elaborar o Plano de Respostas a Riscos (PRR);**
b. **Aprovar o Plano de Respostas a Riscos (PRR); e**
c. **Executar o Plano de Respostas a Riscos (PRR).**

### a) Elaborar o Plano de Respostas a Riscos (PRR)

A elaboração do Plano de Respostas a Riscos (PRR) é de responsabilidade do gestor do risco, que deverá designar pessoal responsável por seu cumprimento e monitoramento.

O tratamento dos riscos pode se dar das seguintes formas:

- **Evitar:** promover ações para eliminar o risco;
- **Transferir:** promover ações que transfiram a consequência ou impacto de um risco para uma terceira parte, como no caso de uma apólice de seguro para veículos;
- **Mitigar**: promover ações que reduzam a probabilidade ou o impacto a um nível aceitável de criticidade, como no caso de implementar um mecanismo de análise periódica de vulnerabilidades em sistemas, buscando reduzir os riscos de invasão; ou

- **Aceitar:** trata-se de não promover ações para tratar o risco, sendo que o custo é inviável ou muito alto em relação ao benefício, ou o nível do risco (probabilidade x impacto) é reduzido, atentando-se às definições do apetite a risco.

O processo de tratamento de riscos deve considerar, dentre outras:

- a viabilidade e custo da solução proposta;
- a existência de restrições ou imposições legais;
- a disponibilidade de recursos financeiros, humanos e tecnológicos;
- o nível de criticidade do risco; e
- as causas que dão origem ao risco.

A presente etapa deve ser encerrada apresentando-se o seguinte entregável:

- Plano de Respostas a Riscos – PRR (Apêndice D).

**b) Aprovar o Plano de Respostas a Riscos (PRR)**

A aprovação do Plano de Respostas a Riscos (PRR) é de responsabilidade da Comissão de Supervisão de Gestão de Riscos (CSGR), que realizará a sua análise e emitirá parecer favorável ou não, apresentando as correções necessárias ou sugerindo melhorias.

Caso haja necessidade, o CSGR poderá solicitar a presença do gestor do risco para esclarecer pontos controvertidos.

## 3.5 MONITORAMENTO E REAVALIAÇÃO

O monitoramento e a reavaliação são ações contínuas que colaboram com a manutenção da gestão de riscos, promovendo a efetividade na condução das ações de tratamento dos riscos.

Os envolvidos nessa fase do processo são o **gestor do risco, os responsáveis designados no Plano de Respostas a Riscos** (PRR) e **Comissão de Supervisão de Gestão de Riscos** (CSGR), que devem:

a. **Monitorar o Plano de Respostas a Riscos (PRR); e**
b. **Reavaliar o Plano de Respostas a Riscos (PRR).**

**a) Monitorar o Plano de Respostas a Riscos (PRR)**

O monitoramento se refere à verificação contínua das ações propostas no Plano de Respostas a Riscos (PRR), tendo como referências as colunas "métrica" e "parâmetros", dispostas no Modelo de Plano de Respostas a Riscos – PRR (Apêndice D).

Deve ser realizado pelo gestor do risco em conjunto com os designados no PRR, sob supervisão da CSGR.

**b) Reavaliar o Plano de Respostas a Riscos (PRR)**

Para garantir a efetividade na gestão dos riscos, eles devem ser reavaliados sempre que preciso, considerando as competências legais e o ambiente em que a setorial está inserida. Dessa forma, destacam-se as seguintes situações em que os riscos podem ser reavaliados:

- novos riscos;
- mudança no nível de criticidade do risco;
- ocorrência de eventos de riscos;
- mudanças no Plano de Respostas a Riscos (PRR); e
- mudanças no processo de gestão de riscos.

## 3.6 COMUNICAÇÃO

No decorrer das 5 (cinco) fases deste Modelo de Gestão de Riscos (MGR) deve ser estabelecido um processo de comunicação que garanta a interação entre todos os envolvidos.

O resultado do trabalho é a entrega dos Planos de Respostas a Riscos (PRRs) que serão concatenados em um relatório, este último a ser elaborado pelo Comissão de Supervisão de Gestão de Riscos (CSGR), que deverá ser atualizado periodicamente, a cada ano.

# REFERÊNCIAS

ABNT. **NBR ISO 31000**:2018. Gestão de riscos - Diretrizes. Rio de Janeiro, 2018.

ASSI, Marcos. **Gestão de riscos com controles internos**: ferramentas, certificações e métodos para garantir a eficiência dos negócios. 2. ed. São Paulo: Saint Paul Editora, 2021.

BRASIL. **Modelo Corporativo de Gestão de Riscos (MCGR) da Câmara dos Deputados.** Disponível em: https://camaranet.camara.leg.br/documents/37194/47013538/Modelo+Corporativo+de+Gest%C3%A3o+de+Riscos+da+C%C3%A2mara+dos+Deputados.pdf. Acesso em: 14 ago. 2025.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Enterprise Risk Management Integrating with Strategy and Performance**. Disponível em: https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf. Acesso em: 14 ago. 2025.

EDSON, Antônio; BACCI, Luciana; ASSI, Marcos. **Transformando as Três Linhas em geração de valor**: com a gestão de riscos e o sistema de controles internos. São Paulo: Saint Paul Editora, 2022.

PROJECT MANAGEMENT INSTITUTE (PMI). **Business Solutions**. Disponível em: https://www.pmi.org/business-solutions. Acesso em: 14 ago. 2025.

## APÊNDICE A – Roadmap para implementação setorial da gestão de riscos

| Ação | Observações |
|---|---|
| 1. Designação do responsável ou responsáveis pelo levantamento dos riscos e elaboração do Plano de Respostas a Riscos (PRR). | Orienta-se que a designação seja realizada mediante expediente, em processo SEI próprio, enviando-o à mesa SETIC-CSGR. |
| 2. Definição do escopo da gestão de riscos. | Orienta-se que o escopo seja definido conforme competências de cada uma das setoriais da Setic, observado o seu Regimento Interno. |
| 3. Apresentação do MGR à equipe setorial | Orienta-se que seja realizada a apresentação em *slides*, enfatizando as normas que regulamentam a gestão de riscos no âmbito da Setic e como se dará a implementação setorial.<br>Entre as normas, destacam-se:<br>• Portaria 151/2025/SETIC (Política de Gestão de Riscos da Setic);<br>• Portaria 41/2025/SETIC (Sistema de Governança da Setic), no que se refere à Comissão de Supervisão e Gestão de Riscos (CSGR); e<br>• O próprio Modelo de Gestão de Riscos (MGR). |
| 4. Identificação dos riscos | Consiste em uma das fases da gestão de riscos no âmbito da Setic, e deve ser executada conforme orientações contidas no tópico “3.2 Identificação de riscos” deste Modelo de Gestão de Riscos (MGR). |
| 5. Avaliação dos riscos | Consiste em uma das fases da gestão de riscos no âmbito da Setic, e deve ser executada conforme orientações contidas no tópico “3.3 Avaliação de riscos” deste Modelo de Gestão de Riscos (MGR). |
| 6. Tratamento dos riscos | Consiste em uma das fases da gestão de riscos no âmbito da Setic, e deve ser executada conforme orientações contidas no tópico “3.4 Tratamento dos riscos” deste Modelo de Gestão de Riscos (MGR). |
| 7. Monitoramento e reavaliação | Consiste em uma das fases da gestão de riscos no âmbito da Setic, e deve ser executada conforme orientações contidas no tópico “3.5 Monitoramento e reavaliação” deste Modelo de Gestão de Riscos (MGR). |
| 8. Comunicação | Consiste em uma das fases da gestão de riscos no âmbito da Setic, e deve ser executada conforme orientações contidas no tópico “3.6 Comunicação” deste Modelo de Gestão de Riscos (MGR). |

## APÊNDICE B – Abordagens de apoio para identificação e categorização de riscos

| Identificação e Categorização de Riscos | |
|---|---|
| **Metodologia de Apoio** | No momento da identificação dos riscos, podem ser utilizadas diferentes técnica, com apoio de um facilitador, tais como:<br>• *Brainstorming*;<br>• Causa Raiz (Diagrama de Ishikawa, Diagrama de Pareto, 5 Porquês etc.);<br>• Entrevistas;<br>• Inspeções;<br>• Matriz SWOT;<br>• Revisão de documentações; e<br>• Técnica Delphi.<br><br>A Comissão de Supervisão de Gestão de Riscos (CSGR), após deliberação, recomenda a adoção da técnica *brainstorming*, por meio das seguintes etapas:<br>a. planejamento e divisão das equipes conforme responsabilidade e escopo de atuação;<br>b. reunião e apresentação para cada uma dessas equipes sobre gestão de riscos em seu contexto e sobre a técnica de *brainstorming*, enfatizando a importância da participação de cada um;<br>c. aplicação da técnica *brainstorming* para levantamento dos riscos apontados pela equipe, atribuindo para cada um dos servidores o levantamento de no máximo dois riscos que tenham conhecimento;<br>d. logo após, o mediador deverá abrir votação para classificar os riscos quanto a sua probabilidade e impacto; e<br>e. por fim, após o levantamento dos riscos e sua devida classificação, o gestor de riscos deverá analisar os resultados, avaliando, filtrando e priorizando o tratamento dos riscos identificados, considerando sua visão holística. |

| | |
|---|---|
| **Categorização do Risco** | Após a identificação, os riscos devem ser categorizados, facilitando o tratamento e a análise do nível de criticidade. São exemplos de categorização:<br>• atividades ou subprocessos ao qual está associado;<br>• elementos do diagrama do escopo (infraestrutura e serviços, desenvolvimento de sistemas, gestão de dados, segurança da informação, administrativo e financeiro etc.);<br>• fases do planejamento (estratégico, tático ou operacional); e<br>• temas ou assuntos relacionados ao risco (segurança, dados, sistemas, infraestrutura, pessoas, conformidade etc.).<br><br>A Comissão de Supervisão de Gestão de Riscos (CSGR), após deliberação, objetivando uma uniformização do processo, optou pela categorização em relação às setoriais da Setic, dividindo-a em:<br>1. ASCF;<br>2. Coge;<br>3. Code;<br>4. Cosegi;<br>5. Caf; e<br>6. Coinfra. |

# APÊNDICE C – Planilha identificação e avaliação de riscos

| **Setorial:** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Data:** | | | | | | | |
| **ID** | **IDENTIFICAÇÃO DE RISCOS** | | | | **AVALIAÇÃO DE RISCOS** | | |
| | Categorização | Causa | Risco (evento) | Impacto | Probabilidade | Impacto | Nível de risco |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

# APÊNDICE D – Modelo de Plano de Respostas a Riscos (PRR)

| Setorial: | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Data: | | | | | | | | | |
| ID | IDENTIFICAÇÃO DE RISCOS | | TRATAMENTO DE RISCOS | | | | | | |
| | Categorização | Risco (evento) | Controles Existentes | Ação Proposta | Métrica | Responsável | Parâmetros | | |
| | | | | | | | Crítico | Alerta | Ideal |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

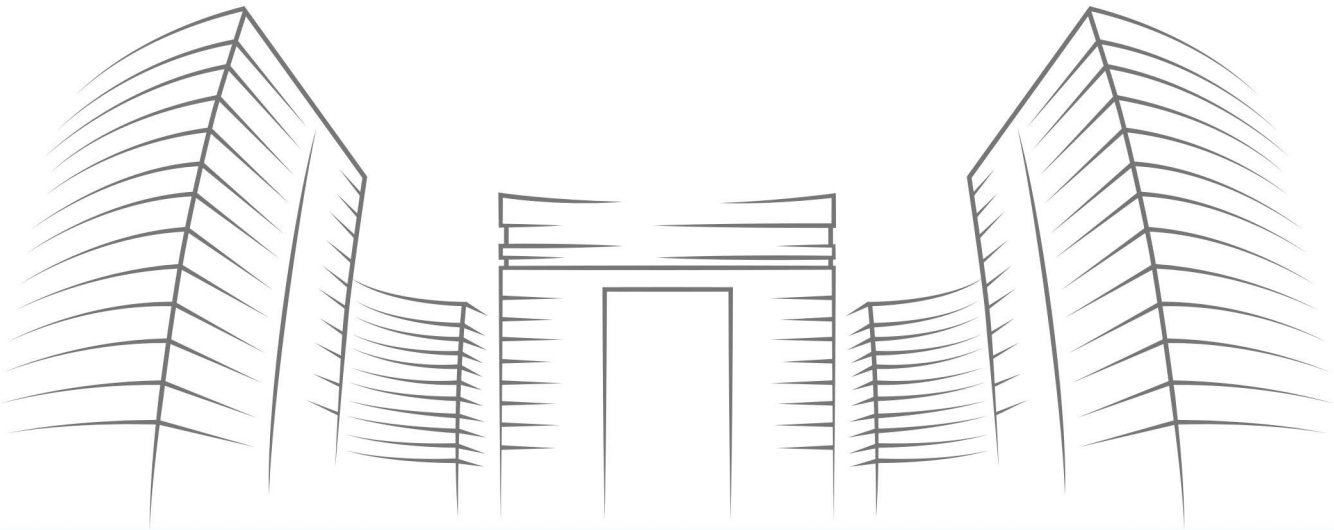
SETIC
Superintendência Estadual de
Tecnologia da Informação
e Comunicação

RONDÔNIA
Governo do Estado

Wiki.SETIC

*Plataforma de Documentação Operacional e Gerencial dos Serviços da SETIC*

wiki.setic.ro.gov.br




setic.ro.gov.br

@setic.rondonia

**Telefone:** 69 3212 9541
**Endereço:** Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470