TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

# Plano de Gestão de Riscos de Tecnologia da Informação (2023/2024)

## JULHO/2023

***Controle de Versões***

| *Versão* | *Data* | *Responsável* | *Descrição* |
|---|---|---|---|
| *1.0* | *02/06/2022* | *Elinete Nunes Freitas (CSC/STI)* | *Versão inicial* |
| *1.2* | *02/08/2022* | *Emanoel Flexa (STI)* | *Revisão do Plano.*<br>*Ajustes de Processos e Datas* |
| *1.1* | *22/08/2022* | *Emanoel Flexa (STI)*<br>*Elinete Freitas (CSC)*<br>*Jimmy Almendra (CINF)* | *Tratamento de Riscos* |
| *1.2* | *19/07/2023* | *Emanoel Flexa (STI)*<br>*Helder Andrade (CSC)*<br>*Jimmy Almendra (CINF)*<br>*Marcos Tork (APGTIC)* | *Levantamento de novos riscos dos Processos da STI*<br>*Revisão dos riscos anteriormente*<br>*Retirada dos riscos de processos de S.I da tabela de riscos de TIC* |

# Sumário

## 1. Introdução

A sistematização da gestão de riscos em nível institucional constitui estratégia que aumenta a capacidade da organização para lidar com incertezas, es mula a transparência, contribui para o uso eficiente de recursos públicos e melhora a entrega de serviços ao cidadão (TCU, 2018). As organizações não podem ser avessas ao risco e ter sucesso, pois o risco é inerente a tudo o que fazemos para oferecer serviços de alta qualidade.

Este documento visa orientar as atividades a serem conduzidas de forma coletiva em reuniões de planejamento da área de Tecnologia da Informação (TI), de forma a prever eventos ou situações que possam comprometer a execução dos objetivos estratégicos definidos no Plano Diretor de TI (2020-2026). Com isso, espera-se aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos, e orientar a equipe de TI sobre como os riscos deverão ser gerenciados.

Sendo assim, o Plano de Gestão de Riscos de Tecnologia da Informação do TRE-AP contribui para a identificação de possíveis ameaças que poderão afetar o dia a dia organizacional, possibilitando agir proativamente, o que reduzirá os impactos negativos na missão e nos objetivos estratégicos de TI.

### 1.1. Objetivo

O Plano de Gestão de Riscos em Tecnologia da Informação tem o objetivo de ser parte integrante da tomada de decisão informada desde o início da política ou do projeto, passando pela implementação até a entrega diária de serviços de Tecnologia da Informação. Este documento fornece uma abordagem para a gestão de riscos relacionados à Tecnologia da Informação por meio de um conjunto de atividades e tarefas que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Este documento estabelece um plano de ação contendo o processo de gestão de riscos para a área de TI de forma a orientar a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação dos riscos inerentes aos recursos, serviços e sistemas informatizados do TRE-AP.

Para que o objetivo geral seja alcançado, foram definidos os seguintes objetivos específicos:

a) Definir as atividades e tarefas que compõem o processo de gestão de riscos;

b) Definir as técnicas e ferramentas para identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos para a área de TI do TRE-AP;

c) Definir os papéis e responsabilidades de cada envolvido na gestão de riscos.

### 1.2. Escopo e Abrangência

O Plano de Gestão de Riscos em Tecnologia da Informação proposto neste documento permeia todo o ciclo de vida das iniciativas para desenvolvimento, implementação e gestão de

soluções que envolvem as áreas de Tecnologia da Informação do TRE-AP. Abrange as áreas de infraestrutura de TI, manutenção de equipamentos de TI, suporte operacional, desenvolvimento de sistemas, governança e gestão de TI, redes e segurança da informação.

### 1.3. Referências

As referências para a construção do Plano de Gestão de Riscos em Tecnologia da Informação são:

1. Processo de Gestão de Riscos de TI do TRE-AP.
2. Política de Gestão de Riscos do TRE-AP (Resolução 522/2018).
3. Norma Técnica ABNT NBR ISO 31000**:** 2018 *Risk management: guidelines, provides principles, framework and a process for managing risk*.
4. Norma Técnica ABNT 31010:2019. *Risk Management: Risk assessment techniques.*

### 1.4. Vigência

O atual Plano de Gestão de Riscos de Tecnologia da Informação terá validade de 2 (dois) anos e está alinhado ao PDTIC da Secretaria de Tecnologia da Informação.

## 2. Metodologia

A metodologia para construção deste Plano baseia-se nas ferramentas de gestão conhecidas por Ciclo de Deming, para melhoria contínua de processos e produtos (PDCA), e a ferramenta para construção de plano de ação 5W2H. O Quadro 1 apresenta as fases da metodologia utilizada para a construção deste documento.

| Fase | Atividades |
|---|---|
| Planejamento | Planejar o processo de gestão de riscos com suas atividades, tarefas, ferramentas e técnicas. |
| Desenvolvimento | Definir papéis e responsabilidades bem como as atividades e tarefas a serem executadas por cada papel. |
| Checagem | Definir como será o monitoramento e o controle do plano de ação a ser seguido. |
| Ação | Comunicar o cronograma para a execução do plano. |

## 3. Processo de Gerenciamento de Riscos

De acordo com os princípios e diretrizes dispostos na Política de Gestão de Riscos do TRE-AP (Resolução nº 522/2018), a gestão de riscos deve ser parte integrante dos processos organizacionais, de forma sistemática, estruturada e oportuna, visando, sobretudo, subsidiar a tomada de decisão e a elaboração do planejamento estratégico, assim como promover a melhoria contínua dos processos organizacionais.

A gestão de riscos deve ser utilizada ainda como instrumento para promover a simplificação de procedimentos associados à prestação de serviços públicos, de modo a assegurar que somente sejam utilizados os controles indispensáveis, de acordo com os limites de exposição a riscos institucionalmente definidos, e que sejam eliminados controles desnecessários ou economicamente desvantajosos. A partir das orientações e determinações constantes na Resolução nº 522/2018 do TRE-AP a operacionalização da gestão de riscos deve seguir as etapas da figura abaixo. Observe-se que essas etapas não são obrigatoriamente sequenciais.

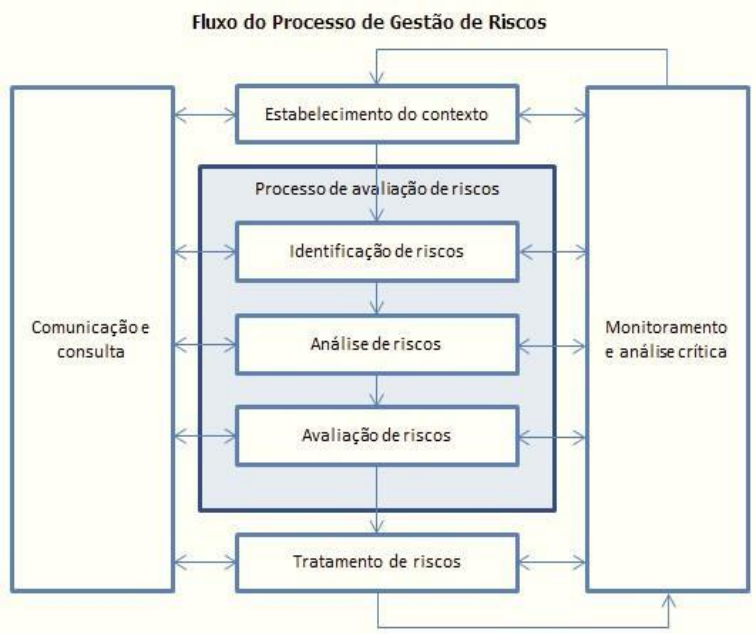


**Figura 1 – Processo de Gestão de riscos de TI**

A Figura 1 apresenta as atividades executadas para a realização da gestão de riscos relacionados aos projetos de TI. São elas: estabelecimento do contexto, processo de avaliação de riscos (identificação de riscos, análise de riscos e avaliação de riscos), tratamento de riscos, monitoramento e análise crítica, e comunicação e consulta com as partes interessadas.

Todos os passos para o gerenciamento de Riscos da STI estão dispostos no Manual do Processo de Gestão de Riscos de TI.

## 4. Papéis e Responsabilidades

Para realizar a gestão de riscos na área de TI, serão definidos papéis e responsabilidades, conforme apresenta o Quadro 2.

| Papel | Responsabilidade |
|---|---|
| Comitê de Gestão de TIC | Identificar ou propor o plano de Gestão de Riscos de Tecnologia da Informação |
| Comitê de Governança de Segurança da Informação | Aprovar o plano de Gestão de Riscos de Tecnologia da Informação |
| Secretário de Tecnologia da Informação | ○ Associar um agente responsável para cada risco mapeado e avaliado, identificado nos projetos ou projetos de contingência e resposta aos riscos. |

| | |
|---|---|
| | ○ Assegurar que o risco seja gerenciado de acordo com as diretrizes estabelecidas neste documento.<br>○ Garantir que as informações adequadas sobre o risco estejam disponíveis e atualizadas.<br>○ Gerenciar e reportar informações adequadas sobre o gerenciamento de riscos.<br>○ Organizar o mapeamento dos riscos e propô-lo ao Comitê de Governança de TIC. |
| Gestor do Ativo<br>Gestor do Processo<br>Gestor de Riscos | ○ Realizar identificação e avaliação de riscos no âmbito das atividades desenvolvidas pela área de Tecnologia da Informação.<br>○ Elaborar e manter atualizado o Mapa de Gerenciamento de Riscos de TI e o plano de ação para tratamento de riscos.<br>○ Monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos.<br>○ Atuar na primeira linha de defesa, com a implementação de ações corretivas para resolver deficiências nos mapas e nos planos de ação de riscos.<br>○ Manter controles eficazes e conduzir procedimentos de resposta aos riscos.<br>○ Observar a inovação e a adoção de boas práticas no gerenciamento de riscos de TI. |

**5. Monitoramento e Controle**

Este documento será revisado anualmente ou quando necessário. Todas as situações ou atividades não previstas neste documento deverão ser submetidas à Secretaria de TI que juntamente com sua equipe irão avaliá-las e aprová-las.

O Plano de Gestão de Riscos deve ser revisado ainda ao final de cada novo ciclo de planejamento estratégico e, a qualquer tempo, se houver alteração significativa no padrão de riscos do Tribunal, devendo o Plano refletir essa mudança.

O Plano de Gestão de Riscos de Tecnologia da Informação e os Mapas de Gerenciamento de Riscos serão atualizados com o devido registro das alterações e encaminhados para o Comitê de Governança de TIC para validação e aprovação.

**6. Cronograma de Ações**

A aplicação deste plano deve abranger, direta ou indiretamente, todas as áreas da STI até o final de 2024, podendo o período ser estendido, de acordo com a necessidade.

Para este período serão mapeados os riscos associados aos serviços essenciais de TI (Portaria 9/2022) e processos estratégicos de TI.

Os riscos de segurança da informação serão tratados de forma isolada e tratados pelo Comitê de Governança de Segurança da Informação.

| Ação | Descrição | Responsável pelo levantamento dos riscos | Prazo |
|---|---|---|---|
| Identificação dos Riscos dos sites de Intranet e Internet | Serviço essencial de TI | Coordenadoria de Infraestrutura (CINF) | Agosto / 2022 |
| Mapeamento dos Riscos de correio eletrônico | Serviço essencial de TI | Coordenadoria de Infraestrutura (CINF) | Agosto / 2022 |
| Mapeamento dos riscos de comunicação de dados | Serviço essencial de TI | Coordenadoria de Infraestrutura (CINF) | Agosto / 2022 |
| Mapear riscos relacionados ao Banco de dados Corporativo | Serviço essencial de TI | Coordenadoria de Soluções Corporativas (CSC) | Agosto / 2022 |
| Mapear riscos relacionados aos serviços de armazenamento Corporativo | Serviço essencial de TI | Coordenadoria de Infraestrutura (CINF) | Agosto / 2022 |
| Mapear riscos relacionados aos serviços relacionados à Sessão Plenária | Serviço essencial de TI | Coordenadoria de Infraestrutura (CINF) | Agosto / 2022 |
| Gerenciamento de riscos do processo de Gestão de Contratos de TI | Processo impacta a TI no atendimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Fevereiro / 2023 |
| Gerenciamento de riscos do processo de Backup e Restore | Processo estratégico para validar a capacidade de recuperação de dados. | Coordenadoria de Infraestrutura (CINF) | Fevereiro / 2023 |
| Gestão de Riscos do processo gerenciamento Contínuo de Vulnerabilidade | Processo impacta diretamente na segurança da informação | Comitê de Governança de Segurança da Informação | Fevereiro / 2023 |
| Gestão de Riscos do processo Gerenciamento de Incidentes de Segurança da Informação | Processo impacta a organização no atendimento de seus objetivos | Comitê de Governança de Segurança da Informação | Agosto / 2022 |
| Gestão de Riscos do processo | Processo estratégico que | Coordenadoria de Infraestrutura (CINF) | Agosto /2023 |

| | | | |
|---|---|---|---|
| Gerenciamento de Ativos de Hardware de TIC | impacta a TI no atingimento de seus objetivos | | |
| Gestão de Riscos do processo Gerenciamento de Incidentes | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento de Problema | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento de Ativos de TIC | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |
| Gestão de Riscos do processo Desenvolvimento de sistemas | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Soluções Corporativas (CSC) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento de Mudanças | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento de Projetos de Disponibilidade e Capacidade | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento de Liberação e Implantação | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento de Projetos | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Soluções Corporativas (CSC) | Agosto / 2023 |
| Gestão de Riscos do processo Gerenciamento da Central de Serviço | Processo estratégico que impacta a TI no atingimento de seus objetivos | Coordenadoria de Infraestrutura (CINF) | Agosto / 2023 |

| | | | |
|---|---|---|---|
| Gestão de Riscos do processo Elaboração e Gestão Orçamentária de TIC | Processo estratégico que impacta a TI no atingimento de seus objetivos | Secretaria de Tecnologia e Informática (STI) | Agosto / 2024 |