PODER JUDICIÁRIO
DO ESTADO DO ACRE

Tribunal de Justiça do Estado do Acre

PLANO DE GESTÃO DE RISCOS DE TIC

Edição
2026

Elaboração
SETIC

PRESIDENTE
Desembargador Laudivon de Oliveira Nogueira

VICE-PRESIDENTE
Desembargadora Regina Célia Ferrari Longuini

CORREGEDOR GERAL DE JUSTIÇA
Desembargador Raimundo Nonato da Costa Maia

SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Elson Correia de Oliveira Neto

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Resolução Nº 291/2023

PLANO DE RISCO DO PODER JUDICIÁRIO RESOLUÇÃO
TPADM - Nº268/2022

Elaboração:
Assessoria da Secretaria de Tecnologia da Informação e Comunicação

SUMÁRIO

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
01/06/2023	1.0	1ª Revisão do Plano de Riscos de TIC 2023	Assessoria de Governança de TIC
05/07/2024	2.0	2ª Revisão do Plano de Riscos de TIC 2024	Assessoria de Governança de TIC
01/04/2025	3.0	3ª Revisão do Plano de Riscos de TIC 2025	Assessoria da SETIC
10/03/2026	4.0	4ª Revisão do Plano de Riscos de TIC 2026	Assessoria da SETIC

APRESENTAÇÃO

A Tecnologia da Informação e Comunicação (TIC) desempenha um papel fundamental na consecução dos objetivos estratégicos do Tribunal de Justiça do Estado do Acre (TJAC). Nesse contexto, a gestão eficaz e eficiente dos riscos associados à TIC torna-se imperativa.

Este documento apresenta o Plano de Gestão de Riscos de TIC (PGRTIC) a ser executado no âmbito da Secretaria de Tecnologia da Informação e Comunicação (SETIC).

O presente plano está em consonância com a Resolução nº 370/2021 do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o ano de 2026. Conforme preconiza o art. 37 da referida norma:

> *"Cada órgão deve desenvolver um Plano de Gestão de Riscos de TIC, focado na continuidade dos negócios, na manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, com o objetivo de mitigar as ameaças identificadas e agir de maneira preditiva e preventiva diante das incertezas."*

Neste sentido, este Plano estabelece diretrizes para a identificação, análise, avaliação e tratamento de riscos, visando fortalecer a Governança de TIC, subsidiar a tomada de decisão segura e assegurar o alcance dos objetivos institucionais.

REFERENCIAL NORMATIVO

Para elaboração deste plano foram utilizados os seguintes documentos de referência:

- Resolução CNJ 370/2021 – Institui a Estratégia Nacional de TIC do Poder Judiciário (ENTIC-JUD);
- Resolução CNJ 396/2021 - Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Portaria CNJ 162/2021 - Aprova Protocolos e Manuais criados pela ENSEC-PJ;
- Resolução TPADM nº 268/2022 - Institui a política de gestão de riscos do Poder Judiciário do Estado do Acre.
- Manual de Procedimentos – Realizar Gestão de Riscos Estratégicos – MAP-DIGES-006 (Versão 00). Emissão: 29/07/2022.
- Manual de Gestão de Riscos do TCU (2ª edição, 2020)
- ABNT NBR ISO 31000:2018 – Gestão de Riscos
- ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação

1. INTRODUÇÃO

A Tecnologia da Informação e Comunicação (TIC) é elemento essencial para o funcionamento das atividades jurisdicionais e administrativas do Tribunal de Justiça do Estado do Acre (TJAC). Nesse cenário, a gestão estruturada dos riscos associados à TIC torna-se fundamental para assegurar a continuidade dos serviços, a segurança da informação e o alcance dos objetivos institucionais.

O ambiente tecnológico é marcado por constantes mudanças, aumento das ameaças cibernéticas, exigências normativas e restrições operacionais e orçamentárias, fatores que ampliam as incertezas e demandam uma abordagem sistemática para o gerenciamento de riscos. Assim, a identificação, análise, avaliação, tratamento e monitoramento dos riscos de TIC são práticas indispensáveis à boa governança e à tomada de decisão responsável.

Este Plano de Gestão de Riscos de TIC (PGRTIC) estabelece diretrizes, responsabilidades e metodologias para orientar a atuação da Secretaria de Tecnologia da Informação e Comunicação (SETIC) na gestão dos riscos que possam impactar serviços, processos, projetos e ativos de TIC do TJAC.

O Plano está alinhado às normas ABNT NBR ISO 31000:2018 e ABNT NBR ISO/IEC 27005:2019, às diretrizes do Conselho Nacional de Justiça, em especial às Resoluções CNJ nº 370/2021 (ENTIC-JUD) e nº 396/2021 (ENSEC-PJ), bem como à Política de Gestão de Riscos do Poder Judiciário do Estado do Acre, instituída pela Resolução TPADM nº 268/2022.

Dessa forma, o PGRTIC consolida-se como instrumento de apoio à governança de TIC, contribuindo para a prevenção de incidentes, a mitigação de impactos e o fortalecimento da resiliência institucional, em suporte à missão do TJAC.

2. CONTEXTUALIZAÇÃO E JUSTIFICATIVA

A Gestão de Riscos de TIC é um pilar essencial para garantir a segurança, a continuidade dos serviços e o êxito institucional em um cenário de crescente dependência tecnológica.

A capacidade de reconhecer e gerenciar incertezas é uma competência crítica na gestão pública moderna e a implementação de estratégias de mitigação, aliada ao aprendizado contínuo, justifica-se pelos seguintes benefícios estratégicos:

1. **Proteção dos Ativos de Informação:** Salvaguarda da integridade, confidencialidade e disponibilidade dos dados.
2. **Continuidade de Negócios:** Minimização de interrupções na prestação jurisdicional.
3. **Conformidade Normativa:** Aderência às regulações do CNJ e legislação vigente (LGPD, entre outras).
4. **Eficiência Operacional:** Otimização de recursos e redução de custos decorrentes de incidentes.
5. **Reputação Institucional:** Fortalecimento da confiança da sociedade no Poder Judiciário.

Este plano visa conferir resiliência e sustentabilidade às operações da SETIC, oferecendo uma abordagem estruturada para lidar com a complexidade e a imprevisibilidade de eventos futuros.

2.1 Escopo e Abrangência

Este documento é aplicável a todos os processos envolvendo Tecnologia da Informação e Comunicação (TIC), abrangendo não somente a SETIC, mas todas as unidades do Tribunal com impacto nas áreas de Governança, Planejamento, Gestão e Infraestrutura de TIC, Segurança da Informação e Atendimento aos Usuários.

Desta forma, a Gestão de Riscos de TIC amplia a abrangência na análise de potenciais riscos relacionados aos processos, projetos, estratégias e ativos de TIC que possam impactar os objetivos estratégicos do TJAC.

3. CONCEITOS E DEFINIÇÕES

Na definição trazida pelo Manual de gestão de Riscos do Tribunal de Contas da União (2020):

> ***Risco*** *é a possibilidade de que um evento afete negativamente o alcance dos objetivos.*

Os riscos são, portanto, eventos que podem vir a acontecer no futuro, ou seja, ainda não ocorreram. E para que não se concretizem, exigem uma ação preventiva.

Para evitar confusão entre os significados, é válido ressaltar que **riscos** não se confundem com:

- **Oportunidades** – possibilidade de que um evento afete positivamente o alcance de objetivos. Não existe "risco" de algo dar certo.
- **Problemas** – eventos decorrentes da concretização de um risco iminente. Ocorrem no presente e requerem uma solução imediata.

Os riscos, então, devem ser avaliados para garantir esses dois pressupostos:

- As soluções de TIC colaboram para que o PJAC ofereça à sociedade efetivo acesso à Justiça; e
- A aplicação dos recursos orçamentários é compatível com os objetivos/missão do PJAC.

Com o intuito de alinhar os conhecimentos, este Plano adota os seguintes **conceitos** teóricos:

- **Apetite a Risco:** nível de risco que a instituição está disposta a aceitar para atingir os objetivos identificados no contexto analisado;
- **Atividade:** agrupamento de tarefas (rotinas) complementares, caracterizada pelo consumo de recursos e orientada para um objetivo definido;
- **Causa de Risco:** razão que pode promover a ocorrência do risco;
- **Controle:** ações estabelecidas por meio de políticas e procedimentos que ajudem a garantir o cumprimento das diretrizes determinadas pela administração para dar resposta adequada ao risco;
- **Evento:** incidente ou ocorrência originada a partir de fontes internas ou externas que afetem a implementação da estratégia ou a realização dos objetivos;
- **Fonte de Risco:** elemento que, individualmente ou combinado, tem potencial para dar origem a um risco específico, podendo ou não estar sob

controle;

- **Gerenciamento de Risco:** adoção de um conjunto de técnicas e metodologias que ajudem a identificar, analisar e gerir os riscos de maneira efetiva;
- **Gestão de Riscos:** processo contínuo aplicado a toda a instituição que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, tratar e monitorar eventos em potencial, contribuindo para a sua redução ou neutralização;
- **Gestor de Risco:** pessoa ou estrutura organizacional responsável por processo de trabalho, atividade, tarefa ou projeto institucional;
- **Gestor do Processo de Trabalho:** pessoa responsável pelo processo, por sua operação, gerenciamento, desempenho e melhoria contínua, interagindo com todas as áreas da instituição que dele participam;
- **Impacto:** efeito resultante da ocorrência do evento;
- **Incerteza:** é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade de ocorrência no atingimento de objetivos e/ou resultados;
- **Macroprocesso:** consiste em um agrupamento lógico de processos de trabalho, cujos produtos (entregas) guardam afinidade de matéria, clientes ou de produção;
- **Matriz de Riscos:** representação formal na qual são registrados os riscos identificados, considerando as probabilidades e os impactos, de forma a permitir a definição das ações necessárias ao seu gerenciamento;
- **Nível de Risco:** representação numérica da magnitude do risco, que é expressa pelo produto das variáveis "impacto" e "probabilidade";
- **Objeto de Gestão de Riscos:** qualquer processo de trabalho, atividade, projeto, iniciativa ou recurso, de plano institucional ou de suporte, para a realização dos objetivos e metas da instituição;
- **Objetivos:** finalidade para qual o negócio, processo ou projeto foi criado, sendo uma declaração do que se pretende alcançar;
- **Pessoa chave:** indivíduo que está de alguma forma envolvido com as atividades e com os resultados do processo, podendo afetar positivamente ou negativamente o resultado de uma atividade ou projeto;
- **Plano de Contingência:** documento que apresenta detalhadamente os procedimentos e recursos a serem utilizados em caso de ocorrência de eventos que possam afetar a segurança de pessoas, do patrimônio ou de sistemas de informação bem como outros que possam interromper a continuidade da prestação de serviços jurisdicionais;
- **Plano de Tratamento de Riscos-Chave:** documento que apresenta o processo de seleção e implementação das medidas necessárias para modificar um risco-chave, especificando os controles a serem implantados

ou aprimorados, prazos e recursos necessários;

- **Probabilidade:** possibilidade de ocorrência do evento;
- **Processo de Trabalho:** conjunto de atividades relacionadas e sequenciais que recebe entradas, agrega valor e produz saídas;
- **Proprietário do Risco:** pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco;
- **Resposta a risco:** qualquer ação adotada para lidar com risco;
- **Risco:** evento capaz de afetar positiva ou negativamente os objetivos e as metas do Poder Judiciário do Estado do Paraná (sic - nota: texto original mantido);
- **Risco-Chave:** risco com elevado impacto nos objetivos da instituição;
- **Risco Inerente:** é aquele ao qual a instituição está exposta, considerando os controles existentes, mas quando não são estabelecidos nem adotados tratamentos para alterar a probabilidade ou o impacto dos eventos;
- **Risco Residual:** risco remanescente após estabelecimento e adoção de tratamento;
- **Tarefa:** meio pelo qual se materializa cada atividade, subdividida em passos ou operações, indispensável à obtenção de produto ou prestação de serviço;
- **Tolerância ao Risco:** grau de quantidade e nível de risco a que a SETIC ou Tribunal está disposto a se expor dentro de padrões considerados institucionalmente razoáveis;
- **Vulnerabilidade:** ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.

4 OBJETIVOS

Este Plano visa estabelecer a sistemática para que a SETIC gerencie seus riscos de TIC em conformidade com as normas ABNT NBR ISO 31000:2018 – Gestão de Riscos e NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação. Além destas, a Resolução CNJ 370/202 (ENTIC-JUD), a Resolução CNJ 396/2021 (ENSEC-PJ) e a Política de Gestão de Riscos do TJAC (Resolução n° 268/2022.

O objetivo primordial é agir preventivamente sobre eventos que possam comprometer o Plano Diretor de TIC (PDTIC), minimizando perdas e maximizando oportunidades.

De forma específica, os objetivos almejados com este Plano são:

- Identificar os riscos de TI que podem impactar os objetivos da SETIC;
- Avaliar a probabilidade e o impacto desses riscos;
- Definir ações de tratamento para mitigar ou evitar os riscos;
- Monitorar continuamente os riscos e a eficácia das ações de tratamento.

5 METODOLOGIA

A Metodologia adotada pela SETIC para condução deste Plano baseia-se nas boas práticas empregadas pelos órgãos de controle e fiscalização, além do que preconizam as normas de Gestão de Riscos, tais como as NBR antes mencionadas.

As atividades de levantamento e tratamento dos riscos podem utilizar de modo homogêneo e como instrumentos de auxílio algumas ferramentas e artefatos conhecidos na área de gestão e governança, tais como:

- Ciclo PDCA: para melhoria contínua

Fase	Atividade	Graficamente
Planejamento	Planejar o processo de gestão de riscos com suas atividades, tarefas, ferramentas e técnicas.	
Desenvolvimento	Definir papéis e responsabilidades bem como a serem executadas por cada papel.	
Checagem	Definir como será o monitoramento e o controle do plano de ação a ser seguido com monitoramento dos prazos.	

Figura 1 – Ciclo PDCA

- Análise de SWOT: para mapeamento de contexto

Figura 2. Análise de SWOT

6 GESTÃO DE RISCOS NO PODER JUDICIÁRIO DO ACRE

6.1 Política de Gestão de Riscos do TJAC

A Resolução Nº 268, de 23 de fevereiro 2022 institui a política de gestão de riscos do Poder Judiciário do Estado do Acre.

Os pressupostos chave desta Resolução com impacto na área de TIC podem ser assim resumidos:

a) **Alinhamento explícito à estratégia institucional**

O plano de riscos de TIC **não é técnico-isolado**, ele existe para proteger e viabilizar os objetivos estratégicos do TJAC.

Logo, deve estar vinculado ao **Planejamento Estratégico institucional**, demonstrar como riscos de TIC afetam objetivos estratégicos, táticos e operacionais e considerar que riscos de TIC **não são apenas operacionais**, mas também estratégicos, de imagem, conformidade, comunicação e orçamento.

b) **Integração total com a governança e a gestão institucional**

A Gestão de Riscos de TIC **não pertence só à área de tecnologia**, sendo sua responsabilidade **compartilhada** entre gestores de TIC, gestores de processos e a alta administração;

As decisões de aceitação, tolerância e priorização de riscos **não são técnicas**, mas de governança;

c) **Definição clara de apetite e tolerância a riscos de TIC**

Nem todo risco de TIC será eliminado — alguns serão aceitos conscientemente. Logo, o plano precisa traduzir o **apetite a risco institucional** para o contexto de TIC, distinguindo riscos aceitáveis, toleráveis e inaceitáveis.

d) **Abordagem sistêmica e orientada a processos de TIC**

O risco está nos **processos, serviços e ativos de TIC**, não apenas na tecnologia. Assim, o plano deve mapear riscos por processos de TIC, serviços críticos e projetos de TIC, usando análise de contexto, como previsto em seus Anexos.

e) **Metodologia formal, padronizada e documentada**

Não existe gestão de riscos "informal" ou "de cabeça". O plano de TIC deve adotar integralmente o **processo cíclico** previsto, ou seja: escopo → identificação → análise → avaliação → tratamento → monitoramento → comunicação;

Podem ser utilizadas as matrizes, formulários e relatórios previstos nos Anexos, o que auxilia a auditoria, rastreabilidade e prestação de contas.

f) Monitoramento contínuo e revisão periódica

O Risco de TIC muda muito rapidamente, logo, o plano não pode ser estático e deve prever ciclos anuais mínimos de revisão, possibilidade de ciclos menores para áreas críticas, indicadores e mecanismos de acompanhamento dos riscos e controles e integração com auditorias baseadas em risco.

g) Comunicação e cultura de riscos em TIC

A Gestão de Riscos só funciona se for **compreendida e praticada**. Logo, é necessário que o plano preveja comunicação estruturada com áreas de negócio, estimule capacitação e conscientização em Riscos de TIC e garanta transparência das informações relevantes.

Por fim, a leitura atenta da Resolução nos faz vislumbrar as partes envolvidas no processo, estabelecendo a seguinte **Matriz de Responsabilidades (Papéis):**

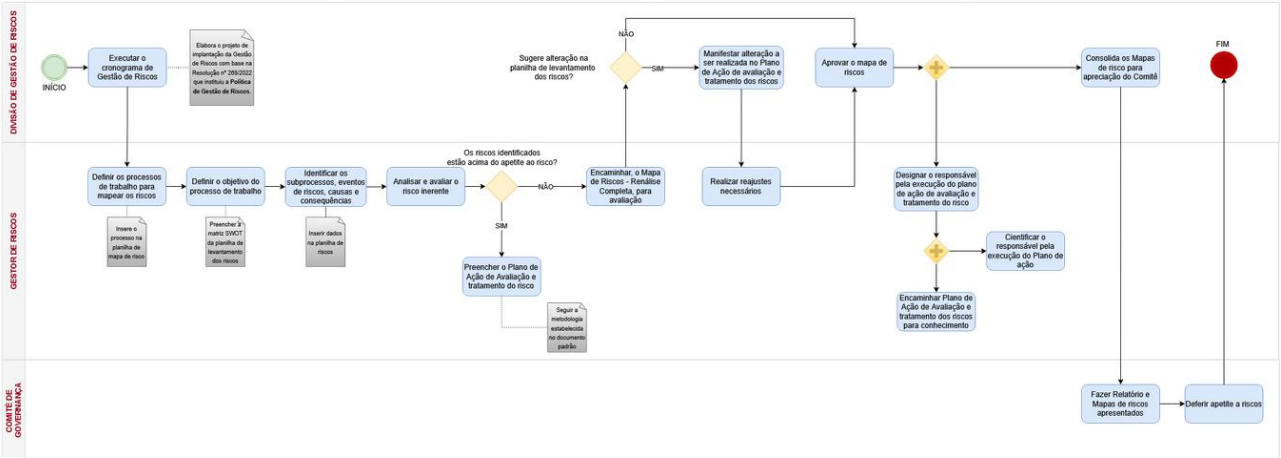
Ator	Papel	Responsabilidades Principais
Administração Superior do TJAC (Presidente, Vice-Presidente e Corregedor-Geral da Justiça)	Liderança máxima e instância decisória final	● Aprovar a política de gestão de riscos; ● Definir **apetite e tolerância a riscos**; ● Analisar o mapa de riscos e relatórios críticos; ● Decidir prioridades e providências institucionais; ● Patrocinar a **cultura de gestão de riscos**. *Quem diz "esse risco é aceitável" ou "isso é inaceitável".*
Comitê de Governança e Estratégia (CGOVE)	Instância de coordenação, supervisão e articulação estratégica.	● Monitorar e revisar a política de gestão de riscos; ● Acompanhar o tratamento dos riscos; ● Propor níveis de aceitabilidade e tolerância; ● Analisar e encaminhar o mapa de riscos à Administração Superior.

		Faz a ponte entre estratégia, gestão e decisão superior.
Secretaria de Governança e Gestão Estratégica (SEGOV)	Órgão técnico-metodológico central da gestão de riscos	● Disseminar a política de gestão de riscos; ● Elaborar e atualizar a **metodologia** de gestão de riscos; ● Coordenar o processo no nível estratégico; ● Elaborar relatórios e mapas de riscos estratégicos; ● Apoiar tecnicamente os gestores; ● Promover capacitação e cultura de riscos. *É quem "faz o método funcionar" e garante padronização.*
Auditoria Interna (AUDIN)	Avaliação independente e fiscalização baseada em riscos.	● Realizar auditorias internas baseadas em riscos; ● Avaliar a eficácia da gestão de riscos; ● Avaliar controles internos; ● Reportar resultados à Administração Superior; ● Diagnosticar fragilidades nos controles administrativos. *Não gerencia riscos, mas verifica se eles estão sendo bem geridos.*
Gestores de Riscos (Administração Superior, Magistrados, Secretários, Assessores, Diretores de Secretarias e Coordenadores).	Donos institucionais dos riscos dentro de suas áreas.	● Escolher os processos que terão riscos gerenciados; ● Propor níveis aceitáveis de exposição ao risco; ● Definir ações de tratamento dos riscos; ● Estabelecer prazos e avaliar resultados. *São os "donos do risco" — respondem por ele.*
Gestores de Processos (Magistrados e Servidores responsáveis por processos, projetos e ações.)	Gestão operacional dos riscos.	● Identificar e avaliar riscos dos processos; ● Gerenciar riscos no dia a dia; ● Implementar planos de ação; ● Comunicar novos riscos; ● Elaborar mapas e relatórios nos níveis tático e operacional. *São quem lida com o risco "no chão da fábrica".*
Escola do Judiciário (ESJUD)	Suporte à capacitação institucional.	● Promover capacitação anual em gestão de riscos. *Garante que as pessoas saibam aplicar o modelo.*
Comunidade	Corresponsabilidade	*Todos participam, ainda que não decidam.*

institucional ampliada (Magistrados; Servidores; Estagiários, Prestadores de serviço)	pela gestão de riscos.	

6.2 Processo de Mapeamento e Tratamento de Riscos

O Tribunal de Justiça do Estado do Acre (TJAC), por meio de sua Secretaria de Governança e Gestão Estratégica (SEGOV), estabeleceu o Processo de Mapeamento e Tratamento de Riscos institucional, consignado no Processo SEGOV-004, disponibilizado na Intranet do Tribunal, no endereço: https://link.tjac.jus.br/f5c90.



Este modelo servirá de fonte para a elaboração do processo de gestão de riscos específico da TIC e também pode ser assim representado em suas etapas.

7 PROCESSO DE GESTÃO DE RISCOS DE TIC

Devido às especificidades inerentes à Tecnologia da Informação e Comunicação (TIC), foi desenhado o Processo de Gestão de Riscos específico da TIC, em consonância com o Processo SEGOV-004 antes apresentado.

As atividades de Gestão de Riscos de TIC contemplam um macroprocesso que deve ser composto de etapas bem definidas, tais como:

I. Estabelecimento do contexto

II. Identificação dos riscos

III. Análise dos riscos

IV. Avaliação dos riscos

V. Tratamento dos riscos

VI. Comunicação e consulta

VII. Monitoramento e análise crítica

É comum que as etapas II, III e IV sejam realizadas ao mesmo tempo, quando dos mapeamentos e classificação dos riscos.

Estruturado como processo, as etapas acima seguem um fluxo padronizado, que pode ser assim representado:

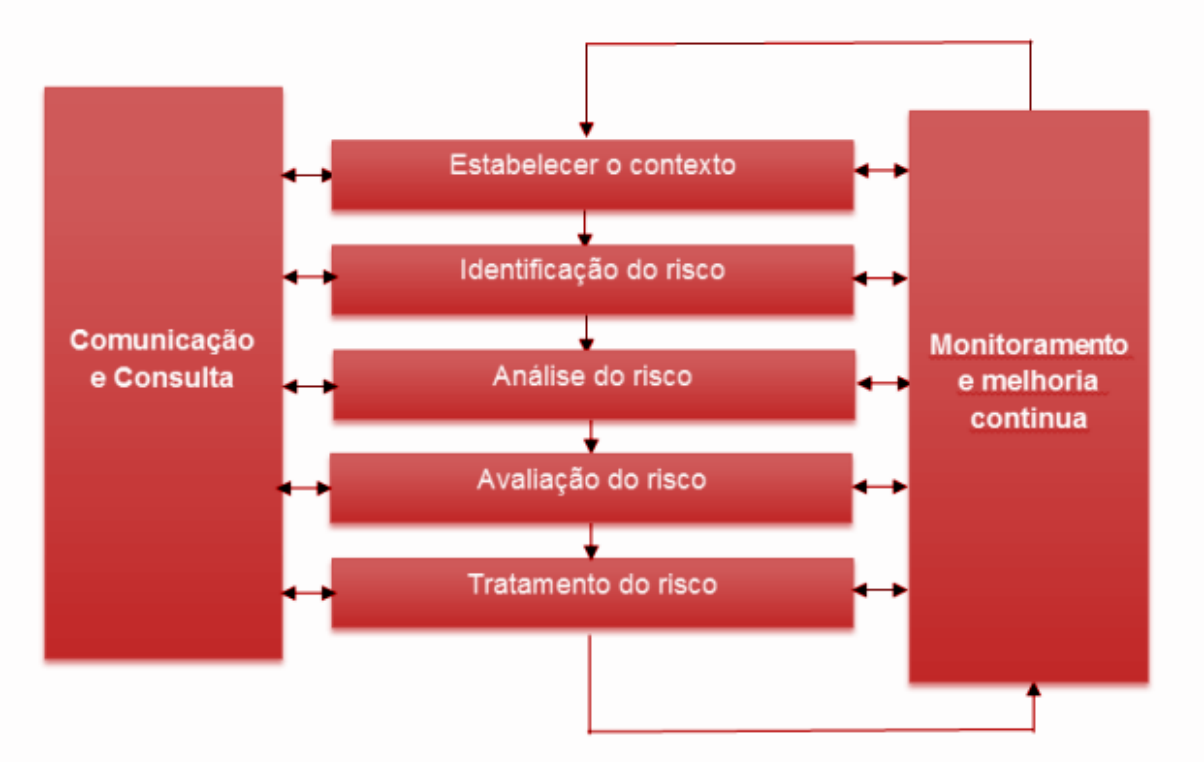


Figura 3. Processo de Gestão de Riscos (ISO 31000 – Adaptado)

Passamos a detalhar as etapas do Processos de Gestão de Riscos de TIC do TJAC.

7.1 Estabelecimento do Contexto

Etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os fatores externo e interno que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.) e os critérios de riscos a serem levados em consideração ao gerenciar riscos.

A título de exemplo, alguns dos aspectos a serem levantados são:

- Identificar **objetivos e resultados** da SETIC;
- Identificar os **processos de trabalho relevantes** para o alcance dos objetivos/resultados;
- Identificar as **pessoas envolvidas** nesses processos e especialistas na área;
- Definir os **fatores externos e internos** que podem afetar o alcance dos objetivos (pessoas, sistemas, infraestrutura, legislação, etc.);
- Definir os **critérios de riscos** a serem considerados;

Para auxiliar no estabelecimento do contexto, pode-se utilizar, por exemplo, o modelo abaixo:

Contexto Interno	Contexto Externo
Principais resultados:	Principais stakeholders e seus interesses:
Pessoas chave:	Recursos externos:
Processos de trabalho mais importantes:	Relevância dos resultados/entregas para o TCU:
Atividades que mais agregam valor:	Relevância dos resultados/entregas para a sociedade:
Recursos tecnológicos necessários:	Setores ou entidades parceiros:

7.2 Identificação dos Riscos

Compreende o reconhecimento e a descrição dos riscos relacionados aos objetivos/resultados de um objeto de gestão de riscos, envolvendo a identificação de possíveis fontes de riscos.

Aqui, é preciso identificar os riscos que podem causar perdas e como, onde e por que a perda pode acontecer. É necessário considerar riscos cujas fontes estejam ou não sob controle da organização.

Para fins de padronização., serão adotadas as seguintes Categorias de Riscos com impacto no negócio da área de TIC do Tribunal.

Categoria de Risco	Descrição
Estratégico	eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da unidade/órgão
Operacional	eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e a eficiência dos processos organizacionais
Orçamentário	eventos que podem comprometer a capacidade da instituição de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária
Imagem/Reputação	eventos que podem comprometer a confiança da sociedade em relação à capacidade da instituição em cumprir sua missão, interferem diretamente na imagem do órgão
Integridade	eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos
Fiscal	eventos que podem afetar negativamente o equilíbrio das contas públicas
Conformidade	eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis
Comunicação	eventos de falhas na troca, clareza ou tempestividade das informações, comprometendo decisões, alinhamento e execução das ações.
Sustentabilidade	eventos que podem impactar o tripé da sustentabilidade (social, ambiental e econômico).

7.3 Análise dos Riscos

Esta é a etapa que se refere ao desenvolvimento da compreensão sobre o risco, determinado pela Matriz de **Probabilidade x Impacto**, que resultará na determinação dos Níveis de Risco, tanto inerente quanto residual. Assim, deve-se proceder:

- Atribuição de **Probabilidade (GP)** a cada evento de risco, conforme escala abaixo:

Descrição	Chance de ocorrer	Definição	Valor
Muito Baixa	< 10%	Evento pode ocorrer apenas em **circunstâncias excepcionais**	1
Baixa	>=10% <= 30%	Evento **pode** ocorrer em **algum momento**	2
Possível	>=30% <= 50%	Evento **deve** ocorrer em **algum momento**	3
Alta	>=30% <= 50%	Evento provavelmente ocorra na **maioria das circunstâncias**	4
Muito Alta	>90%	Evento esperado que ocorra na **maioria das circunstâncias**	5

- Definição do **Impacto (GI),** segundo a natureza e os tipos de consequências, conforme escala abaixo:

Descrição	Definição	Valor
Irrelevante	Evento cujo impacto pode ser **absorvido** por meio de atividades normais	1
Pequeno	Evento cujo impacto pode ser **absorvido e minimizado**, mas carecem de esforço da gestão	3
Moderado	Evento significativo que pode ser **gerenciado** em circunstâncias normais	5
Alto	Evento **crítico**, Risco inaceitável com necessidade de **monitoramento e controles robustos**	7
Muito Alto	Evento com **potencial** para levar o negócio ou serviço ao **colapso**	10

Tanto a Probabilidade quanto o Impacto recebem um valor de **Peso**.

- Cálculo da **Probabilidade (GP) x Impacto (GI)**, que resulta no **Nível de Risco Inerente (NRI)**:

NRI = GI x GP
(Nível de Risco Inerente = Grau de Impacto x Grau de Probabilidade)

O **NRI** pode ser resumido com a Matriz abaixo:

GP / GI	1	3	5	7	10
1	1	3	5	7	10
2	2	6	10	14	20
3	3	9	15	21	30
4	4	12	20	28	40
5	5	15	25	35	50

Figura 4. Matriz de Risco: Probabilidade x Impacto

7.4 Avaliação dos Riscos

Aqui são estimados os níveis dos riscos identificados para determinar se é tolerável de acordo com o limite de exposição a riscos estabelecido.

Envolve a classificação do **Nível de Risco Inerente (NRI)**, conforme a seguinte escala:

Nível de Risco	Interpretação	Valor (GP x GI)
Baixo	Risco aceitável	**1 – 2 – 3 – 4**
Médio	Risco inaceitável com necessidade de monitoramento	**5 – 6 – 7 - 9**
Alto	Risco inaceitável com necessidade de monitoramento e controles robustos	**10 – 14 – 15 – 20 – 21 - 25**
Extremo	Risco absolutamente inaceitável	**28 – 30 – 35 – 40 - 50**

Após a determinação NRI, devem ser aplicadas as estratégias de **Controle**, que, após levantadas, serão avaliadas, segundos os seguintes critérios:

Nível de Confiança	Fator de Controle (FC)	Descrição
1 Inexistente	**0,0**	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais
2 Fraco	**0,2**	Controles têm abordagens *ad hoc*, tendem a ser aplicados caso a caso; a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas
3 Mediano	**0,4**	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
4 Satisfatório	**0,6**	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
5 Forte	**0,8**	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.

Após a adoção dos controles, deve-se reavaliar o nível de risco, resultando no **Nível de Risco Residual (NRR)**, cujo cálculo usa a seguinte fórmula:

NRR = NRI x FC
(Nível de Risco Inerente x Fator de Avaliação dos Controles)

7.5 Tratamento dos Riscos

Para cada risco identificado, é importante definir ações práticas para dar uma resposta adequada ao risco que foi detectado.

Esta etapa consiste em definir as respostas aos riscos, de forma a adequar seus níveis e ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas.

Resposta a Riscos		
Resposta	**Risco negativo**	**Risco positivo**
Evitar	Eliminar incertezas; impedir o início ou descontinuar atividades que geram os riscos	Eliminar incertezas
Transferir/ Compartilhar	Transferir ou compartilhar o risco com outra parte interessada	Repassar a propriedade para terceiros para melhor capturar as oportunidades
Reduzir/ Mitigar	Reduzir o impacto e/ou a probabilidades de ocorrência do risco	Identificar e maximizar as oportunidades de ocorrência
Aceitar	Tolerar o risco, pois o nível é baixo, o tratamento é limitado ou o custo é desproporcional ao benefício	Não aproveitar a oportunidade

Alguns exemplos práticos de resposta a risco incluem:

- **Implementar Controles de Acesso** para proteger os dados e sistemas contra acesso não autorizado;
- **Realizar Backups Regulares** para garantir a recuperação em caso de perda de dados;
- **Implementar Firewalls e Sistemas de Detecção de Intrusão** para proteger a rede contra-ataques cibernéticos;
- **Realizar Testes de Segurança** periódicos para identificar vulnerabilidades nos sistemas e na infraestrutura;
- **Fornecer Treinamento de Segurança** regular aos funcionários da SETIC para conscientizá-los sobre as ameaças cibernéticas e as melhores práticas de segurança.
- **Implementar Políticas de Segurança**: Implementar políticas de segurança claras e abrangentes para orientar o comportamento dos funcionários e proteger os dados e sistemas.
- **Monitorar Logs de Auditoria**: Monitorar os logs de auditoria para identificar atividades suspeitas ou não autorizadas.
- **Implementar Planos de Recuperação de Desastres**: Implementar planos de recuperação de desastres para garantir a continuidade dos negócios em caso de eventos catastróficos.

Ao detalhar esses aspectos adicionais, o Plano de Gestão de Riscos de TIC se tornará mais completo, eficaz e adaptado às necessidades específicas do Tribunal, garantindo que os riscos de TIC sejam gerenciados de forma proativa e que a SETIC possa cumprir sua missão de forma segura e eficiente.

7.6 Comunicação e consulta

Esta etapa se refere à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo.

Podemos dividir esse fluxo de comunicação em duas direções: vertical e horizontal.

A **comunicação vertical** pode ser no sentido da base para a cúpula ou vice-versa, proporcionando que a cúpula da organização seja informada de riscos por todas as unidades organizacionais e que os servidores tenham ciência dos principais riscos que afetam a organização.

Por sua vez, a **comunicação horizontal** é importante para que os riscos de um processo que envolva diferentes unidades (processos transversais), às vezes, de diferentes Unidades, sejam conhecidos igualmente por todos os que trabalham nesse processo.

De igual modo, a sensibilização de todos os envolvidos é crucial para criar uma cultura de riscos em todo o Tribunal e potencializar o processo de Comunicação. Por isso, promover treinamentos e capacitações regulares ajuda que todos compreendam seu papel na segurança e continuidade dos serviços, promovendo uma mentalidade proativa e resiliente.

7.7 Monitoramento e Revisão Contínua

Esta etapa ocorre durante todo o processo de gerenciamento de riscos, sendo todos eles monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças de contexto da organização e de se manter uma visão geral dos riscos.

A ideia é monitorar e analisar criticamente os riscos para identificar mudanças no contexto e manter uma visão geral dos riscos.

O monitoramento e a revisão contínua são cruciais para garantir que o Plano de Gestão de Riscos de TIC permaneça eficaz e relevante ao longo do tempo. Isso inclui:

- **Monitoramento Regular:** Monitorar regularmente os riscos identificados, as ações de tratamento implementadas e os indicadores de desempenho para identificar quaisquer desvios ou problemas.
- **Revisão Periódica:** Revisar periodicamente o Plano de Gestão de Riscos de TIC para garantir que ele esteja atualizado e alinhado com as mudanças no ambiente de negócios, nas tecnologias e nas ameaças.
- **Auditoria Interna**: Realizar auditorias internas periódicas para avaliar a eficácia do Plano de Gestão de Riscos de TIC e identificar áreas de melhoria.
- **Relatórios de Desempenho**: Elaborar relatórios de desempenho periódicos para comunicar os resultados da gestão de riscos às partes interessadas.

7.8 Integração com os Planos da ENTIC-JUD

Em observância à Resolução CNJ nº 370/2021, o Plano de Gestão de Riscos de TIC

deve estar integrado aos processos previstos nos Planos que integram a ENTIC-JUD. Assim, deve-se adotar Gestão de Riscos em processos tais como:

- **Gestão de Projetos:** Considerar os riscos em todas as fases do ciclo de vida dos projetos;
- **Gestão de Mudanças**: Avaliar os riscos associados a todas as mudanças na infraestrutura e nos sistemas;
- **Gestão de Incidentes**: Utilizar as informações sobre riscos para prevenir e responder a incidentes de segurança da informação;
- **Continuidade de Negócios**: Integrar o Plano de Gestão de Riscos de TIC com o Plano de Continuidade de Negócios para garantir a resiliência da área de TIC;
- **Contratações de Soluções de TIC**: Analisar os riscos inerentes às atividades de contratações que podem impactar o suprimento de soluções para a área de TIC.
- **Planejamento Orçamentário**: Sondar os fatores internos e externos que podem prejudicar o provimento de recursos orçamentários para execução dos itens planejados para o exercício.
- **Aprendizado e Capacitação**: Verificar quais os riscos potenciais às atividades de desenvolvimento pessoal e aperfeiçoamento de habilidades funcionais;
- **Transformação Digital:** Avaliar os riscos envolvidas nas atividades de adoção ou implementação de soluções voltadas à inovação e modernização.

7.9 Exemplos de Riscos Comuns na SETIC

Para ilustrar a aplicação do Plano de Gestão de Riscos de TIC, é útil identificar alguns exemplos de riscos comuns na SETIC:

- **Falha de Infraestrutura:** Falha de servidores, redes, sistemas de armazenamento ou outros componentes críticos da infraestrutura de TIC.
- **Ataques Cibernéticos**: Ataques de hackers, malwares, phishing ou outras ameaças cibernéticas que podem comprometer a confidencialidade, integridade ou disponibilidade dos dados.
- **Erros Humanos**: Erros cometidos por funcionários da SETIC que podem causar perdas de dados, interrupções de serviço ou outros incidentes.
- **Não conformidade**: Não cumprimento de leis, regulamentos ou políticas internas que podem resultar em sanções legais ou financeiras.

- **Perda de Dados**: Perda de dados devido a falhas de hardware, erros humanos, ataques cibernéticos ou outros eventos.
- **Indisponibilidade de Sistemas**: Indisponibilidade de sistemas críticos devido a falhas de hardware, software, ataques cibernéticos ou outros eventos.

7.10 Responsabilidades e Funções

Definir claramente as responsabilidades e funções de cada membro da SETIC em relação à gestão de riscos é fundamental para garantir a eficácia do plano.

O processo de Gestão de Riscos de TIC do TJAC apresenta as seguintes funções:

- **Gestor de Riscos (Secretário de TIC):** Representado pelo titular da área de TIC, que possui a responsabilidade de escolher os processos de trabalho e fornecer informações essenciais sobre os riscos durante as etapas que compõem a Metodologia, além de supervisionar todo o processo de gestão de riscos, definir as políticas e diretrizes, e garantir que o plano seja implementado e monitorado.
- **Equipe de Segurança da Informação**: Responsável por identificar e avaliar os riscos de segurança da informação, implementar as medidas de segurança adequadas e monitorar a eficácia dessas medidas.
- **Equipe de Infraestrutura de TI**: Responsável por garantir a disponibilidade, confiabilidade e segurança da infraestrutura de TI, incluindo servidores, redes, sistemas de armazenamento e outros componentes críticos.
- **Equipe de Desenvolvimento de Sistemas**: Responsável por garantir que os sistemas sejam desenvolvidos e mantidos de forma segura, seguindo as melhores práticas de segurança e as políticas internas.
- **Todos os servidores da SETIC**: Responsáveis por seguir as políticas e procedimentos de segurança, relatar quaisquer incidentes de segurança e participar de treinamentos de conscientização sobre segurança.

No TJAC, o Secretário de Tecnologia da Informação e Comunicação da SETIC assume a responsabilidade por:

- Escolher os processos de trabalho que terão os riscos gerenciados;
- Propor níveis aceitáveis de exposição ao risco;
- Definir as ações de tratamento a serem implementadas;
- Supervisionar o processo e comunicar-se com as partes interessadas.

8 FERRAMENTAS E TECNOLOGIAS

A utilização de ferramentas e tecnologias adequadas pode facilitar a implementação e o monitoramento do Plano de Gestão de Riscos de TIC. Algumas soluções passíveis de uso são:

- **Softwares de Gestão de Riscos:** softwares especializados para automatizar o processo de identificação, avaliação, tratamento e monitoramento de riscos. O TJAC estabeleceu Acordo de Cooperação com a CGE-MG para uso da ferramenta **UAI Risk**.
- **Planilhas eletrônicas padronizadas:** planilhas pré-configuradas contendo os dados necessários para mapear e tratar os eventos em análise e calcular automaticamente os níveis de riscos. O TJAC utiliza o modelo disponível no endereço: https://docs.google.com/spreadsheets/d/1M2CmlPzkp3aa_Iwc_gYjHX__cEnWWbCH/edit?usp=drive_link&ouid=118219340064726769172&rtpof=true&sd=true
- **Ferramentas de Análise de Vulnerabilidades**: ferramentas de análise de vulnerabilidades para identificar vulnerabilidades nos sistemas e na infraestrutura.
- **Sistemas de Detecção de Intrusão**: Utilizar sistemas de detecção de intrusão para monitorar a rede e os sistemas em busca de atividades suspeitas ou maliciosas.
- **Ferramentas de Monitoramento de Logs:** Utilizar ferramentas de monitoramento de logs para coletar e analisar os logs de auditoria dos sistemas e aplicativos.

9 MAPEAMENTO DOS RISCOS DE TIC

Uma vez detalhado todo o processo Gestão dos Riscos, passaremos a aplicar os conceitos teóricos e mapear os riscos com potencial para impactar as atividades da unidade da área de Tecnologia da Informação e Comunicação (TIC).

9.1 Estabelecimento do contexto

Contexto Interno	Contexto Externo
Principais resultados Garantia da disponibilidade, integridade e confidencialidade dos serviços e sistemas de TIC que suportam a atividade jurisdicional e administrativa do TJAC.	**Principais stakeholders e seus interesses** Magistrados, servidores, administração superior, CNJ, TCU, órgãos de controle, fornecedores de TIC e sociedade, com interesse na eficiência, segurança, transparência e continuidade dos serviços.
Pessoas chave Gestores de TIC, líderes técnicos, analistas de sistemas, administradores de infraestrutura, equipe de segurança da informação e pontos focais das áreas de negócio.	**Recursos externos** Orçamento público, contratos com fornecedores, soluções tecnológicas de terceiros, normativos e diretrizes nacionais de TIC e governança pública.
Processos de trabalho mais importantes Governança de TIC, gestão de projetos e contratos, sustentação de sistemas, gestão de infraestrutura, segurança da informação, atendimento e suporte ao usuário.	**Relevância dos resultados/entregas para órgãos de controle** Conformidade com normas de governança e gestão de TIC, eficiência na aplicação dos recursos públicos, mitigação de riscos e evidências de controles internos adequados.
Atividades que mais agregam valor Manutenção da continuidade dos serviços críticos, entrega de soluções digitais, automação de processos judiciais e administrativos, e suporte à tomada de decisão institucional.	**Relevância dos resultados/entregas para a sociedade** Prestação jurisdicional mais célere, acessível e transparente, com uso eficiente da tecnologia e garantia da segurança das informações.
Recursos tecnológicos necessários Infraestrutura de redes e datacenter, sistemas corporativos e judiciais, plataformas de armazenamento e backup, ferramentas de segurança da informação, softwares de gestão e soluções em nuvem.	**Setores ou entidades parceiros** Conselho Nacional de Justiça (CNJ), outros tribunais, órgãos do Poder Executivo e Legislativo, instituições de controle, universidades, empresas e provedores de soluções de TIC.

9.2 Identificação, Análise e Avaliação dos Riscos

ID	Evento de Risco	NRI	NRR	Valor NRR	Resposta	Macroprocesso
1	Falta de Registro de Acesso ao Data Center	Extremo	Alto	11,2	Reduzir	Infraestrutura e Segurança
2	Acesso indevido de usuário interno ou externo a sistemas judiciais sem MFA	Alto	Médio	6	Evitar	
3	Não realização, ou realização insuficiente, de avaliações e testes semestrais de conformidade em segurança cibernética nas infraestruturas crítica	Médio	Baixo	3,6	Mitigar	
4	Uso indevido de dispositivos USB	Alto	Médio	6,0	Mitigar	
5	Falhas no gerenciamento de mudanças podem causar interrupções de sistemas críticos	Extremo	Alto	11,2	Mitigar	
6	Uso de contas de usuário com privilégios excessivos	Alto	Médio	8,4	Mitigar	
7	Usuários com permissões excessivas em pastas de rede	Alto	Médio	8,0	Mitigar	
8	Uso de senhas fracas ou reutilizadas, possibilitando acesso não autorizado aos sistemas	Alto	Médio	6,0	Mitigar	
9	Interrupção de energia elétrica na infraestrutura do interior	Alto	Médio	8,4	Mitigar	
10	Servidores com serviços legados	Extremo	Alto	11,2	Mitigar	
11	Excesso de acessos elevados concedidos a novos desenvolvedores	Alto	Médio	8,0	Mitigar	
12	Dependência do provedor de Nuvem	Alto	Médio	8,0	Mitigar	
13	Não conseguir monitorar os indicadores da estratégica de TIC do PJAC	Alto	Alto	12,6	Evitar	Planejamento e Monitoramento de Indicadores
14	Não atingimento do percentual mínimo de execução do PSTIC em razão de restrições	Alto	Baixo	2,0	Reduzir	Contratações de TIC

ID	Evento de Risco	NRI	NRR	Valor NRR	Resposta	Macroprocesso
	orçamentárias					
15	Impossibilidade de concluir contratações previstas no PSTIC dentro do exercício financeiro	Alto	Baixo	2,0	Aceitar	
16	Atraso na execução das contratações de TIC devido à represamento de processos em unidades intervenientes	Alto	Alto	12,0	Evitar	
17	Não atingimento do percentual mínimo de execução do Plano de Transformação Digital	Alto	Médio	8,4	Reduzir	Transformação Digital
18	Descontinuidade de iniciativas estratégicas do Plano de Transformação Digital por perda de capital intelectual	Extremo	Extremo	28,0	Evitar	
19	Indisponibilidade de espaço físico adequado para armazenamento de bens inativos de TIC	Alto	Médio	8,0	Evitar	Gerenciamento de Serviços de TIC
20	Atraso ou falha na elaboração da ata de registro de preços	Alto	Médio	6,0	Reduzir	
21	Sobrecarga da equipe terceirizada por demandas não planejadas	Alto	Baixo	4,0	Evitar	
22	Descontinuidade do Conhecimento Técnico	Extremo	Alto	21,0	Compartilhar/ Transferir	Sistemas de Informação
23	Redução de eficiência pela baixa disponibilidade de mão de obra qualificada	Extremo	Alto	22,4	Reduzir	
24	Sobrecarga da Equipe Técnica Interna	Alto	Alto	16,0	Evitar	
25	Dependência Excessiva de Fornecedores Externos	Alto	Alto	12,6	Compartilhar/ Transferir	
26	Implantação/Migração do Sistema Judicial Principal	Extremo	Extremo	30,0	Compartilhar/ Transferir	
27	Ausência de Governança Técnica Prévia nos Projetos Contratados	Alto	Alto	12,6	Compartilhar/ Transferir	
Nível de Risco Residual Médio (NRR-M)				**10,9**		

9.3 Tratamento dos riscos

Para cada um dos riscos mapeados no item 8.2, aplica-se tipo de Controle respectivo, conforme listado abaixo.

ID Risco	ID Controle	Controle	Responsável	Data Início	Data Conclusão	Status
1	1.1	Registrar entradas e saídas com carimbo de data e hora	Subsecretário SUSEG	02/02/2026	30/04/2026	Não iniciado
	1.2	Implementar sistema eletrônico de controle de acesso		02/02/2026	30/04/2026	Não iniciado
2	2.1	Implementação total do MFA	Chefia da DISEG	22/04/2024	20/12/2025	Atrasado
	2.2	Treinar usuários sobre uso do MFA e riscos de credenciais comprometidas.		22/04/2024	20/12/2025	Atrasado
3	3.1	Formalizar periodicidade, responsáveis e escopo dos testes	Subsecretário SUSEG	15/01/2026	30/03/2026	Não iniciado
	3.2	Capacitação de equipe para realizações de análises de vulnerabilidades e conformidade		15/01/2026	30/03/2026	Não iniciado
4	4.1	Implementação de um Antivírus com maiores funcionalidades	Subsecretário SUSEG	05/02/2026	15/05/2026	Não iniciado
	4.2	Iniciar a campanha com usuários do uso correto de tais mídias		05/02/2026	15/05/2026	Não iniciado
	4.3	Implementação do XDR com capacidade avançada de detecção e bloqueio de ameaças provenientes de mídias removíveis		05/02/2026	15/05/2026	Não iniciado
	4.4	Monitoramento contínuo de comportamentos suspeitos ao inserir dispositivos USB, com alertas e resposta rápida integrada ao XDR		05/02/2026	15/05/2026	Não iniciado
5	5.1	Definição obrigatória de janelas de manutenção, com proibição de	Subsecretário SUSEG	01/03/2026	30/08/2026	Não iniciado

ID Risco	ID Controle	Controle	Responsável	Data Início	Data Conclusão	Status
		mudanças fora do período aprovado, salvo exceções formalmente justificadas				
	5.2	Criar histórico de intervenções para auditoria e prevenção de erros		01/03/2026	30/08/2026	Não iniciado
6	6.1	Implementar ferramenta para controle centralizado de contas privilegiadas (PAM), rotacionar senhas automaticamente e registrar sessões	Chefia da DISEG	10/04/2026	30/06/2026	Não iniciado
	6.2	Mapear todas as contas privilegiadas existentes		10/04/2026	30/06/2026	Não iniciado
	6.3	Fornecer privilégios somente quando necessário e por tempo limitado, reduzindo a exposição a ataques		10/04/2026	30/06/2026	Não iniciado
7	7.1	Monitorar alterações indevidas em arquivos críticos	Chefia da DISEG	15/05/2026	30/09/2026	Não iniciado
	7.2	Controle de acesso baseado em grupos		15/05/2026	30/09/2026	Não iniciado
	7.3	Aplicar concessão mediante solicitação formal da chefia		15/05/2026	30/09/2026	Não iniciado
8	8.1	Implementar ferramenta de verificação de senhas fracas ou previsíveis, bloqueando uso de senhas baseadas em nomes, datas ou informações pessoais	Chefia da DISEG	01/06/2026	31/07/2026	Não iniciado
	8.2	Configurar checagem contra listas de senhas comprometidas		01/06/2026	31/07/2026	Não iniciado
	8.3	Forçar alteração de senhas previsíveis, aplicando auditoria periódica para identificar padrões fracos		01/06/2026	31/07/2026	Não iniciado

ID Risco	ID Controle	Controle	Responsável	Data Início	Data Conclusão	Status
9	9.1	Instalar Nobreak predial na infraestrutura das comarcas dos interiores.	Subsecretário SUSEG	15/07/2026	30/10/2026	???
10	10.1	Identificar o que pode ser atualizado, migrado ou descontinuado e planejar atualização ou migração gradual	Subsecretário SUSEG	01/08/2026	15/12/2026	Não iniciado
	10.2	Garantir que dados podem ser recuperados em caso de falha	Subsecretário SUSEG	01/08/2026	15/12/2026	Não iniciado
11	11.1	Implementar política formal de menor privilégio	Chefia da DISEG	02/03/2026	30/07/2026	Não iniciado
	11.2	Definir matriz de acesso por função (RBAC)		02/03/2026	30/07/2026	Não iniciado
	11.3	Treinamento obrigatório para novos desenvolvedores		02/03/2026	30/07/2026	Não iniciado
12	12.1	Avaliar estratégia multi-cloud ou híbrida	Chefia da DISEG	05/01/2026	15/04/2026	Em andamento
	12.2	Implementar plano de contingência e recuperação. 3.Criar mecanismos de redundância para serviços críticos		05/01/2026	15/04/2026	Em andamento
13	13.1	Concretizar a implementação do sistema CAPITEI, para uso no setor de TIC	Secretário SETIC	23/10/2025	20/02/2026	Em andamento
14	14.1	Acompanhamento da execução orçamentaria destinada as demandas de TIC	Subsecretario SUCTI	01/01/2026	31/12/2026	Não iniciado
	14.2	Comunicação à alta gestão de possíveis desvios entre o planejamento e o recurso disponível	Subsecretário SUCTI	01/01/2026	31/12/2026	Não iniciado
	14.3	Adoção de providências para		01/01/2026	31/12/2026	Não iniciado

ID Risco	ID Controle	Controle	Responsável	Data Início	Data Conclusão	Status
		adequações do plano de acordo com variações do orçamento				
15	Risco Aceitável – Não exige Plano de Ação					
16	16.1	Melhorar os processos de trabalho das unidades intervenientes	Subsecretária da SUTOR	01/01/2026	31/12/2026	Não iniciado
	16.2	Manutenção de um corpo técnico qualificado e permanente	Alta Administração	01/01/2026	31/12/2026	Não iniciado
17	17.1	Aprovação e adoção da metodologia de desenvolvimento de soluções de IA;	Presidência do CGTIC	01/01/2026	30/06/2026	Não iniciado
18	18.1	Ampliação e qualificação do um corpo técnico permanente.	Presidência do TJAC	01/01/2026	30/06/2026	Não iniciado
19	19.1	Nomear novos servidores para a DIGIT	Presidência do TJAC	01/01/2026	31/12/2026	Em andamento
	19.2	Não permitir acumulo de bens inativos no galpão em uso	Chefia da DIGIT	01/01/2026	31/12/2026	Em andamento
20	20.1	Nomear novos servidores para a DIATI	Presidência do TJAC	01/01/2026	31/12/2026	Em andamento
	20.2	Monitoramento periódico do consumo dos itens da ata para identificar a necessidade de nova licitação antes do exaurimento total do saldo remanescente	Chefia da DIATI	01/01/2026	31/12/2026	Em andamento
	20.3	Vinculação das datas de vencimento das atas ao calendário de novas licitações para garantir a sucessão de instrumentos contratuais sem lacunas temporal		01/01/2026	31/12/2026	Em andamento
21	21.1	Nomear novos servidores para a DICER	Presidência do TJAC	01/01/2026	31/12/2026	Em andamento

ID Risco	ID Controle	Controle	Responsável	Data Início	Data Conclusão	Status
	21.2	Estabelecimento de Fluxo de Demandas e Catálogo de Serviços com níveis de prioridade (SLA)	Chefia da DICER	01/01/2026	31/12/2026	Em andamento
	21.3	Adotar controles mais eficientes para atuar antes que ocorra a sobrecarga		01/01/2026	31/12/2026	Em andamento
22	22.1	Documentação sistemática	Chefias da DISSA, DIMAD, DIMJU, DISJU, DICSA e DIPOR	01/01/2026	31/12/2026	Em andamento
	22.2	Compartilhamento de conhecimento		01/01/2026	31/12/2026	Em andamento
	22.3	Rodízio controlado de atividades		01/01/2026	31/12/2026	Em andamento
23	23.1	Priorização institucional de demandas conforme capacidade da equipe	Chefias da DISSA, DIMAD, DIMJU, DISJU, DICSA e DIPOR	01/01/2026	31/12/2026	Em andamento
	23.2	Documentação e compartilhamento de conhecimento		01/01/2026	31/12/2026	Em andamento
	23.3	Exigência de transferência de conhecimento em contratos com terceiros		01/01/2026	31/12/2026	Em andamento
	23.4	Comunicação formal do risco residual à administração		01/01/2026	31/12/2026	Em andamento
24	24.1	Priorização formal de demandas	Chefias da DISSA, DIMAD, DIMJU, DISJU, DICSA e DIPOR	01/01/2026	31/12/2026	Em andamento
	24.2	Definição de níveis de serviço (SLA)		01/01/2026	31/12/2026	Em andamento
	24.3	Escalonamento à administração sobre riscos de capacidade		01/01/2026	31/12/2026	Em andamento
	24.4	Planejamento de reforço temporário de equipe		01/01/2026	31/12/2026	Em andamento
25	25.1	Exigir documentação técnica completa	Toda a SETIC	01/01/2026	31/12/2026	Em

ID Risco	ID Controle	Controle	Responsável	Data Início	Data Conclusão	Status
		como critério de aceite				andamento
	25.2	Prever cláusulas contratuais de transferência de conhecimento		01/01/2026	31/12/2026	Em andamento
	25.3	Realizar capacitações internas antes do encerramento dos contratos		01/01/2026	31/12/2026	Em andamento
26	26.1	Plano detalhado de migração e rollback	Chefias da DIMJU, DISJU e DICSA	01/01/2026	31/12/2026	Em andamento
	26.2	Execução de testes integrados e de carga		01/01/2026	31/12/2026	Em andamento
	26.3	Ambiente de homologação representativo		01/01/2026	31/12/2026	Em andamento
	26.4	Adotar melhorar práticas de tribunais parceiros		01/01/2026	31/12/2026	Em andamento
27	27.1	Instituir comitê ou parecer técnico obrigatório	Toda a SETIC	01/01/2026	31/12/2026	Em andamento
	27.2	Definir padrões mínimos de arquitetura, segurança e integração		01/01/2026	31/12/2026	Em andamento
	27.3	Registrar riscos formais quando não houver envolvimento prévio da unidade		01/01/2026	31/12/2026	Em andamento

9.4 Comunicação e consulta

Os riscos mapeados acima serão alvo de apreciação por parte dos membros dos Comitês estratégicos que tratam dos temas relacionados à Tecnologia de Informação e Comunicação do Tribunal, previstos na Estratégia de TIC do TJAC (Resolução nº 291/2023), quais sejam:

- Comitê de Gestão de Tecnologia da Informação e Comunicação – CGEST;
- Comitê Gestor de Segurança da Informação – CGESI;
- Comitê de Governança de Tecnologia da Informação e Comunicação – CGTIC.

Assim, o mapeamento de riscos aqui proposto será apresentado ao CGEST, CGESI e CGTIC, para devida validação formal, consolidando a comunicação dos riscos às partes envolvidas no processo.

9.5 Monitoramento e análise crítica

O monitoramento das ações de tratamento de riscos é uma etapa crítica da gestão de riscos, pois garante que as medidas adotadas estejam sendo implementadas conforme planejado e que estão produzindo os resultados esperados.

Nesta etapa, o Gestor de Riscos da SETIC é responsável por:

- Apresentar os resultados do monitoramento das ações de tratamento nas reuniões do CGEST, cientificando os membros sobre o status das medidas adotadas e permitindo a tomada de decisão a respeito do tema;

- Comunicar a Secretaria de Governança e Gestão Estratégica (SEGOV) sobre mudanças nos riscos sempre que um novo risco for identificado, um risco existente for excluído ou houver alterações significativas nos riscos;

- Avaliar regularmente a eficácia das ações de tratamento de riscos em vigor, verificando se as medidas estão atingindo os objetivos desejados e se estão contribuindo para a redução do impacto dos riscos identificados.

Colaborando para esta atividade, **anualmente**, deve ser elaborado o Relatório de

Execução de Gestão de Riscos de TIC, no qual se evidencia a situação atualizada dos eventos mapeados neste Plano de Riscos de TIC.

Os riscos analisados no Relatório de Execução devem ser alvo de nova avaliação crítica, visando proceder baixa dos riscos considerados mitigados, a atualização de status daqueles ainda existentes, bem como a inclusão de novos riscos que venham a ser detectados durante aquele ciclo de avaliação.

O mencionado Relatório deve ser apresentado aos membros do CGEST e, após aprovado, deve ser publicado no Portal G2TIC.

10 INDICADORES

Para um efetivo acompanhamento da execução do Plano de Gestão de Riscos de TIC, será adotada a prática de monitoramento regular de indicadores de desempenho, conforme detalhamento abaixo.

Nome do indicador	*Nível de Risco Residual Médio*
Código	***NRR-M***
Descrição do indicador	*Medida do Nível de exposição ao risco, mesmo após a aplicação dos controles devidos*
Pergunta-chave	*Qual o nível de riscos de TIC depois da aplicação dos controles?*
Fórmula de cálculo	***NRR-M** = [(GP x GI) x FC] / Quant. Total de Riscos Mapeados*
Unidade de medida	*Número inteiro (ex.: 1,00)*
Método de apuração	*Coleta da mensal*
Critérios de cálculo	*Regras, exceções, arredondamentos*
Meta	***10,00***
Linha de base	***10,90***
Faixa de desempenho	***Moderado***
Fonte de dados	*Planilha https://docs.google.com/spreadsheets/d/1M2CmlPzkp3aa_Iwc_gYjHX__cEnWWbCH/edit?usp=drive_link&ouid=118219340064726769172&rtpof=true&sd=true*
Periodicidade de coleta	*Mensal*
Periodicidade de revisão	*Anual*
Forma de apresentação	*Apresentação nas Reuniões Quinzenais do CGEST*
Ações corretivas	*O que fazer se a meta não for atingida*
Instância de acompanhamento	*Comitês CGEST, CGESI e CGTIC*

11 PROCESSO DE REVISÃO E ATUALIZAÇÃO

O Plano de Gestão de Riscos de TIC compõe o rol de planos exigidos pela ENTIC-JUD, além de ser previsto no Plano Diretor de TIC do TJAC (PDTIC 2021-2026.

Desta forma, é requisito obrigatório para sua regularidade a revisão e atualização periódica deste Plano.

Em atendimento aos ciclos do iGovTIC-JUD, **anualmente** deve-se proceder a revisão e atualização deste Plano, sendo registradas as suas versões no controle de revisões.

Assim, orienta-se que todo o conteúdo deste **Plano seja revisado anualmente**, devendo ser publicado juntamente com seu respectivo **Relatório de Execução de Riscos anual** em local próprio do Portal **G2TIC**, nas Plataformas **Connect-Jus** e **Integra**, ambas do CNJ.

Além disso, recomenda-se que cada revisão do Plano seja submetida aos Comitês previstos na Estratégia de TIC do TJAC (Resolução nº 291/2023), quais sejam:

- Comitê de Gestão de Tecnologia da Informação e Comunicação – CGEST;
- Comitê Gestor de Segurança da Informação – CGESI;
- Comitê de Governança de Tecnologia da Informação e Comunicação – CGTIC.

Por fim, recomenda-se prestar contas periodicamente sobre os riscos gerenciados neste Plano aos Comitê acima mencionados.

12 MODELOS DE DOCUMENTOS (Artefatos)

A SETIC deverá adaptar os modelos de documentos utilizados neste Plano de Gestão de Riscos de TIC, de forma a padronizar e alinhar o entendimento entre todos os envolvidos com as atividades de levantamento e tratamento dos riscos inerentes às suas áreas.

Desta forma, os documentos ou artefatos a serem adotados para a Gestão de Riscos de TIC incluem:

- Planilha de Identificação de Riscos - Conforme Capítulo 6.2;
- Cálculo da Matriz de Nível de Risco Inerente (Probabilidade x Impacto) – Conforme Capítulos 6.3 a 6.4;
- Plano de Tratamento de Riscos - Conforme Capítulo 6.5;
- Relatório de Execução de Gestão de Riscos de TIC.

O modelo de planilha a ser adotada para a identificação, análise e avaliação dos riscos está disponível no link:
https://docs.google.com/spreadsheets/d/1M2CmlPzkp3aa_Iwc_gYjHX__cEnWWbCH/edit?usp=drive_link&ouid=118219340064726769172&rtpof=true&sd=true

TRIBUNAL DE JUSTIÇA

Secretaria de Tecnologia da Informação e Comunicação

www.tjac.jus.br
Rua Desembargador Jorge Araken, s/n. Via Verde. 69.920-193
Rio Branco-AC | (68) 3302-0360 / 3302-0361