Tribunal de Justiça Militar
do Estado de Minas Gerais

PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Maio/2024

COMITÊ DE GOVERNANÇA DE TIC

Osmar Duarte Marcelino
Desembargador

Daniela de Freitas Marques
Presidente do Comitê Gestor da Política de Atenção ao Primeiro Grau de Jurisdição

George Walter Barreto Paviotti
Juiz de Direito Substituto da 5ª AJME

Roselmiriam Rodrigues dos Santos
Diretora de Tecnologia da Informação e Comunicação

Cecília Tereza Gomes Costa dos Santos
Diretora de Recursos Humanos

Luiza Viana Torres
Diretora Administrativa

Leonardo Vaz de Melo
Coordenador do Escritório de Projetos

COMITÊ DE GESTÃO DE TIC

Roselmiriam Rodrigues dos Santos
Diretora de Tecnologia da Informação e Comunicação

Edivaldo Pereira dos Santos
Gerente de Desenvolvimento de Software

William Marcondes de Freitas Santos
Coordenador de Serviços - Infraestrutura

Maurício de Campos Prado
Coordenador de Serviços - Manutenção e Suporte ao usuário

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
Março/2024	1.0	Elaboração	Comitê Gestor de TIC
Maio/2024	1.0	Avaliação e aprovação	Comitê de Governança de TIC

SUMÁRIO

1. Introdução 52. Objetivo
53. Metodologia
54. Estrutura e contexto
55. Competências e responsabilidades
66. Processo de gestão de riscos
76.1. Identificação de riscos
86.2. Análise de riscos
86.3. Avaliação de riscos
106.4. Tratamento de riscos
116.5. Tolerância a riscos
116.6. Comunicação e Consulta
116.7. Monitoramento e análise crítica
117. Vigência e revisão
12

1. Introdução

A Tecnologia da Informação e Comunicação (TIC) configura-se como ativo estratégico para as organizações de forma geral. No contexto do Poder Judiciário, essa relevância estratégica foi reconhecida por meio de objetivos estabelecidos na Estratégia Nacional de TIC (ENTIC-Jud) pelo Conselho Nacional de Justiça. Em sintonia com as diretrizes do CNJ, o Tribunal de Justiça Militar Minas Gerais (TJMMG) evidenciou o caráter estratégico da Tecnologia da Informação e Comunicação, estabelecendo objetivos para fortalecimento de TIC em seu Planejamento Estratégico Institucional.

Nesse contexto, a gestão de riscos assume papel relevante, na medida em que auxilia as organizações no alcance de seus objetivos e na tomada de decisões fundamentadas. Por sua vez, o Plano de Gestão de Riscos em Tecnologia da Informação representa uma sistematização da gestão de riscos e busca auxiliar gestores e partes interessadas, de maneira a viabilizar o alcance dos objetivos de TIC.

2. Objetivo

O objetivo deste Plano de Gestão de Riscos em TIC é orientar a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação dos riscos inerentes aos recursos, serviços e sistemas de TIC do TJMMG.

3. Metodologia

O presente Plano de Gestão de Riscos em TIC foi elaborado baseado nas diretrizes definidas pela norma ABNT NBR ISO 31000:2018 e adicionalmente nas seguintes normas:

- Resolução CNJ n. 370/2021;
- Resolução CNJ n. 396/2021;
- Resolução TJMMG n. 244/2021.

4. Estrutura e contexto

A governança e a gestão de TIC, no âmbito da Justiça Militar, estão estruturadas nos termos estabelecidos na Resolução TJMMG n. 292/2023.

São responsáveis pela governança de TIC, atuando como instâncias deliberativas da política e do processo de gestão de riscos de TIC, o:

- Comitê de Governança de Tecnologia da Informação (CGTIC);
- Comitê Gestor do Processo Judicial Eletrônico (Eproc);
- Comitê Gestor de Proteção de Dados Pessoais e Governança de Segurança de Tecnologia da Informação.

A Diretoria de Tecnologia da Informação e Comunicação (DIRTIC) é a unidade responsável pela gestão e por prover as soluções e serviços de TIC que dão suporte ao desenvolvimento das atividades da Justiça Militar de Minas Gerais. A DIRTIC conta com 12 servidores efetivos em seu corpo funcional, que são responsáveis por prover as soluções e serviços de TIC na instituição, distribuídos entre quatro áreas de atuação:

- governança e gestão de TIC;
- desenvolvimento e manutenção de sistemas;
- infraestrutura;
- atendimento e suporte.

Os gestores dessas quatro áreas compõem o Comitê Gestor de TIC, instituído pela Portaria TJMMG n. 1.564/2023, e são responsáveis pela coordenação e supervisão do processo de gestão de riscos de TIC. Têm o papel de coordenar as atividades de gestão de riscos, ajudar a desenvolver controles e monitorar riscos e controles.

Nesse contexto, a gestão de riscos em TIC no TJMMG possui foco na continuidade de negócios e na manutenção dos serviços, e o seu escopo inclui a identificação, a avaliação, a priorização, o tratamento e o monitoramento dos riscos associados às atividades operacionais, táticas e estratégicas da DIRTIC, abrangendo projetos, iniciativas estratégicas, ativos de TI e processos de contratação de soluções de TIC. Para a gestão de riscos de TIC, são consideradas as seguintes categorias de riscos:

I. **estratégicos**: riscos identificados e analisados no escopo da elaboração dos artefatos e nos sistemas e serviços estratégicos para o Tribunal. Após o levantamento, os riscos serão atribuídos a uma área proprietária, ainda que outras áreas possam estar envolvidas na sua mitigação e no controle. Os gestores destas áreas serão os proprietários destes riscos;

II. **de segurança da informação e comunicação**: riscos identificados e analisados no escopo de segurança da informação ou normas relacionadas, considerando-se principalmente os sistemas e serviços críticos de TIC para o Tribunal e aqueles identificados no Plano de Continuidade de Serviços de TIC. Os responsáveis pelos sistemas, serviços e pelos ativos que os suportam são identificados juntamente com a avaliação de cada controle, cabendo a estes o monitoramento do risco residual após seu tratamento;

III. **de contratações**: riscos identificados, avaliados, tratados e monitorados no âmbito de cada contratação, desde a fase de planejamento até a fase de execução, incluindo a vigência contratual da solução ou serviço de TIC. Com o término da vigência do contrato, os riscos serão avaliados quanto à pertinência de serem mantidos na base de riscos de TIC. A equipe de planejamento da contratação é responsável por identificar e monitorar os riscos referentes ao processo licitatório (contratação) até a etapa de homologação, enquanto o gestor do contrato é responsável por gerenciar os riscos inerentes à execução do contrato;

IV. **de projetos**: são gerenciados no âmbito de cada projeto de TIC, devendo ser identificados e monitorados pelo responsável direto ou líder de projeto;

V. **de processos**: riscos identificados nos processos mapeados e/ou instituídos pela DIRTIC. Os riscos em processos de TIC são monitorados pelos donos do processo ou, na falta destes, pelo gestor principal da área responsável.

5. Competências e responsabilidades

Compete às instâncias de governança de TIC do TJMMG, quanto à gestão de riscos de TIC, no âmbito de suas atribuições:

I. promover a revisão periódica e a atualização da Política de gestão de riscos de TI;
II. avaliar a adequação, a suficiência e a eficácia da estrutura de gestão de riscos de TI;
III. garantir o apoio institucional para promover a gestão de riscos e controles internos, em especial os seus recursos, e o relacionamento entre as partes interessadas;
IV. deliberar sobre a Política de Gestão de Riscos de TIC e o Plano de Gestão de Riscos de TIC, os níveis de apetite e tolerância a riscos, bem como avaliar seu desempenho;
V. aprovar os ativos, processos de trabalho, projetos e ações que terão os riscos gerenciados com prioridade;

VI. aprovar o relatório de análise crítica, o mapa de riscos de TIC e os planos de resposta/tratamento aos riscos mapeados;
VII. deliberar sobre os riscos considerados extremos e os riscos residuais considerados altos, que lhe forem submetidos;
VIII. deliberar sobre os riscos considerados médios e altos que, eventualmente, lhes forem apresentados pelos proprietários de risco;
IX. assegurar que os riscos identificados pelo processo de gestão de riscos serão tratados por meio de ações a curto, médio ou longo prazos ou de aperfeiçoamento contínuo;
X. decidir a respeito da solução mais adequada quando o risco for avaliado em nível superior à tolerância estabelecida e o custo para reduzi-lo ou eliminá-lo for desproporcional aos benefícios a serem obtidos;
XI. deliberar acerca de eventuais casos omissos e excepcionalidades.

Compete ao Comitê de Gestão de Tecnologia da Informação, com relação à gestão de riscos de TIC:

I. coordenar o processo e acompanhar a execução das atividades relacionadas à gestão de riscos de TIC;
II. acompanhar a execução dos planos de ação para implementação da gestão de riscos de TIC e zelar pela sua adequada comunicação;
III. acompanhar e consolidar as informações pertinentes à gestão de riscos de TIC;
IV. revisar os relatórios de análise crítica e o mapa de riscos de TIC;
V. revisar e monitorar os planos de respostas a riscos relacionados à estratégia;
VI. estabelecer controles proporcionais aos riscos mapeados, considerando suas causas, suas consequências e a relação custo-benefício;
VII. aperfeiçoar o processo de decisão baseado em riscos;
VIII. subsidiar o Comitê de Governança de TIC com informações técnicas, visando auxiliá-lo no processo de tomada de decisão;
IX. dar conhecimento às instâncias pertinentes quando o risco for avaliado em nível superior à tolerância estabelecida e o custo para reduzi-lo ou eliminá-lo seja desproporcional aos benefícios a serem obtidos;
X. avaliar e divulgar as melhores práticas de gestão de riscos para utilização no âmbito da DIRTIC;
XI. validar o estabelecimento de metodologias específicas de gestão de riscos, quando exigidas por Órgãos Superiores ou decorrentes de especificidades técnicas;
XII. elaborar e manter atualizado o Manual de Gestão de Riscos de TIC do TJMMG;
XIII. zelar pelo estrito cumprimento da Política de Gestão de Riscos do TJMMG;
XIV. fomentar a cultura de gestão de riscos e propor ações de sensibilização e capacitação;
XV. estimular a cultura de gestão de riscos em suas equipes e participar de ações de sensibilização e capacitação.

6. Processo de gestão de riscos

De acordo com as diretrizes estabelecidas na NBR ISO 3100:2018, o processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as

atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos, conforme ilustrado na Figura 1.

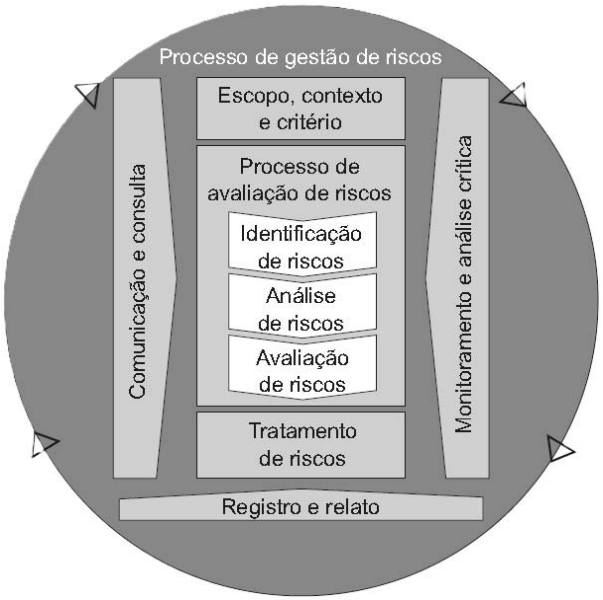

Figura 1 - Processo de Gestão de Riscos (ISO 31000:2018)

Seguindo essas diretrizes, o processo de gestão de riscos de TIC do TJMMG foi estabelecido, de acordo com o que se segue.

6.1. Identificação de riscos

A identificação de riscos tem o objetivo de determinar eventos e incertezas que podem afetar um ou mais objetivos institucionais. Para isso, deverão ser adotadas técnicas que permitam fornecer informações pertinentes, apropriadas e atualizadas para identificação de eventos, suas causas e consequências. Os riscos associados a serviços e ativos de TIC deverão ser identificados, ainda que as fontes não estejam sob controle do TJMMG.

6.2. Análise de riscos

A etapa de análise de riscos tem o objetivo de tornar explícitas a natureza do risco e suas características, permitindo o detalhamento de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia.
Para a análise de riscos associados a serviços e ativos de TIC no TJMMG, a técnica a ser utilizada é a que combina a análise quantitativa e a qualitativa.

Escala de probabilidade			
Nível	**Aspectos avaliativos**	**Histórico de ocorrências do**	**Definição**

		evento em 12 meses	
5	Evento de frequência alta, provavelmente irá ocorrer	Acima de 6	Muito alta
4	Evento com histórico de ocorrência amplamente conhecido	De 5 a 6	Alta
3	Evento de frequência reduzida, e com histórico de ocorrência parcialmente conhecido	De 3 a 4	Média
2	Evento casual e inesperado com pouco histórico de ocorrência	De 1 a 2	Baixa
1	Evento extraordinário, com nenhum histórico de ocorrência	0	Muito baixa

Tabela 1 - Escala de probabilidade

Ressalta-se que a avaliação da probabilidade dos riscos de TIC envolve uma análise qualitativa e, em alguns casos, quantitativa. A combinação de informações, conhecimento especializado e análise criteriosa ajuda a estimar a probabilidade de riscos específicos. Essa avaliação permite direcionar os recursos adequados para mitigar os riscos mais relevantes e tomar decisões controladas na gestão dos riscos de TIC.

Escala de impacto		
Nível	**Aspectos avaliativos**	**Definição**
5	Danos severos em equipamentos com perda de dados estratégicos da instituição / Interrupção que afete serviços ao público externo ou em sistemas estratégicos como Eproc, Internet, sistemas administrativos, servidor de e-mail / Paralisação de sistemas por mais de 24 horas.	Muito alto
4	Danos severos em equipamentos com perda de dados estratégicos da instituição com recuperação de dados entre 4 e 24 horas / Impactos relevantes nos processos que afetem a instituição como um todo / Paralisação de sistemas entre 4 e 24 horas.	Alto
3	Danos médios com perda ou recuperação de dados entre 1 e 4 horas / Sem impactos relevantes nos processos da instituição que afetem mais de um grupo específico ou área / Paralisação de sistemas entre 1 e 4 horas.	Médio
2	Danos leves com perda ou recuperação de dados em até 1 hora / Paralisação parcial de sistemas que afetem um grupo específico, uma única área (ex.: 1 departamento, 1 cartório, uma área de um andar, etc.), 1 sistema departamental ou localizado.	Baixo

1	Danos leves sem perda de dados / Sem paralisação de sistemas, que afetem um único usuário ou equipamento.	Muito baixo

Tabela 2 - Escala de impacto

A avaliação do impacto dos riscos de TIC deve considerar uma combinação de fatores financeiros, operacionais, legais e reputacionais. A compreensão completa do potencial de impacto permite priorizar ações de mitigação e alocar recursos adequados para proteger os sistemas de TIC e minimizar os efeitos negativos dos riscos mapeados.
Após estabelecer os níveis de probabilidade e impacto, conforme tabelas acima, é realizado o cálculo (PxI) para encontrar o nível de risco, conforme Tabela 3.

Matriz de risco de TIC - nível de risco						
		Probabilidade				
		Muito baixo 1	Baixo 2	Médio 3	Alto 4	Muito Alto 5
Impacto	Muito Alto 5	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito baixo 1	1	2	3	4	5

Tabela 3 - Probabilidade x Impacto - Nível de risco

Nível (n)	Descrição
n ≥15	Risco Crítico
8 ≤ n <15	Risco Alto
3 ≤ n <8	Risco Moderado
n <3	Risco Baixo

Tabela 4 - Classificação nível de risco

6.3. Avaliação de riscos

O objetivo da avaliação de riscos é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da etapa de análise de riscos com os critérios de risco

estabelecidos para determinar onde é necessária ação adicional. A partir dos riscos identificados e classificado o nível do risco inerente, o gestor dos riscos de TIC descreve as medidas de controle implementadas, ou a definição de novas medidas de controle a serem implementadas para redução da classificação do nível do risco inerente, tendo como resultado a classificação do nível do risco residual.

6.4. Tratamento de riscos

O objetivo do tratamento de riscos é selecionar e implementar ações para abordar os riscos avaliados. Os gestores dos riscos de TIC impactados deverão estruturar um plano de ação visando a atividades que possibilitem a reclassificação e projeção futura de probabilidade e/ou impacto. O mapa dos riscos de TIC e o plano de ações para o tratamento serão submetidos à apreciação e aprovação do Comitê de Governança de TIC.

6.4.1. Tolerância a riscos

O nível de tolerância a riscos de TIC é definido pelo Comitê de Governança de TIC, em alinhamento à política de gestão de riscos definida pelo TJMMG.
Sendo assim, foi estabelecido que os riscos avaliados como nível baixo poderão ser aceitos. Para os riscos avaliados como nível moderado ou alto, deverá ser estabelecido plano com ações de mitigação a ser apreciado pelo CGTIC. Para os riscos avaliados como nível crítico, deverá haver submissão para análise e decisão do CGTIC quanto à resposta a ser adotada.

Nível (n)	Descrição	Resposta
n ≥15	Risco Crítico	A ser avaliada pelo CGTIC
8 ≤ n <15	Risco Alto	Mitigar
3 ≤ n <8	Risco Moderado	Mitigar
n <3	Risco Baixo	Aceitar

Tabela 5 - Resposta ao risco

6.5. Comunicação e Consulta

O objetivo da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão. A comunicação e consulta deve ocorrer durante todo o processo de gestão de riscos.

6.6. Monitoramento e análise crítica

O objetivo do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, da implementação e dos resultados do processo. Compreende o acompanhamento e a verificação dos indicadores ou da situação de elementos da gestão

dos riscos de TIC, podendo abranger a política, as atividades, os riscos de TIC, os planos de tratamento dos riscos de TIC, os controles e outros assuntos de interesse.

O monitoramento das ações de tratamento dos riscos envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras, devendo considerar o tempo necessário para que essas medidas produzam seus efeitos. O monitoramento consiste na atualização da análise e avaliação do risco, assim como do estágio de execução das medidas de tratamento do risco e dos resultados dessas medidas.

É necessário que os responsáveis pelo monitoramento e análise crítica se atentem que a realização do tratamento pode gerar novos riscos que também necessitam ser acompanhados. O risco remanescente deve ser documentado e submetido a monitoramento, análise crítica e, quando apropriado, tratamento adicional.

A medição dos indicadores de controle dos riscos de processos de TIC, unidades e projetos de TIC será realizada pelo respectivo gestor do risco de TIC. O monitoramento contínuo será acompanhado pelo Comitê de Governança de TIC.

7. Vigência e revisão

Este plano possui vigência até dezembro de 2026, devendo ser revisto quando necessário pelo Comitê de Governança de TIC.