ESTADO DO RIO GRANDE DO SUL
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA MILITAR

PORTARIA Nº 097/2025

Institui o Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGR-TIC) do Tribunal de Justiça Militar do Estado do Rio Grande do Sul e estabelece princípios, diretrizes, responsabilidades, governança, metodologia, mecanismos de execução e revisão anual.

A PRESIDENTE DO TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DO RIO GRANDE DO SUL, no uso das atribuições legais e regimentais,

CONSIDERANDO a Resolução CNJ nº 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Portaria CNJ nº 101/2025, que define o Índice de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário (iGovTIC-JUD), cujo item Q17 exige a formalização do Plano de Gestão de Riscos de TIC, sua execução e revisão anual;

CONSIDERANDO as normas ISO 31000 (Gestão de Riscos), ISO/IEC 27005 (Riscos de Segurança da Informação), ISO/IEC 27001 (Segurança da Informação), NIST SP 800-30 e demais boas práticas internacionais;

CONSIDERANDO a necessidade de identificar, avaliar, tratar e monitorar riscos relacionados à continuidade dos serviços, segurança da informação, infraestrutura tecnológica, sistemas, dados, contratos, fornecedores e ferramentas críticas;

CONSIDERANDO a importância da cultura institucional de prevenção, redução de incidentes, fortalecimento da resiliência cibernética e mitigação de impactos operacionais e jurídicos,

RESOLVE:

CAPÍTULO I — DA INSTITUIÇÃO DO PLANO

Art. 1º Fica instituído o Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGR-TIC) no âmbito do Tribunal de Justiça Militar do Estado do Rio Grande do Sul, documento oficial que estabelece a metodologia, os processos, os controles e a governança para identificação,

análise, avaliação, tratamento, monitoramento e comunicação de riscos relacionados à TIC.

Art. 2º O PGR-TIC aplica-se:

I – à Coordenadoria de TIC;

II – ao CGTIC e Comitê de Gestão de TIC (CGESTIC);

III – à ETIR/ETIS;

IV – à Comissão de Segurança da Informação;

V – a magistrados, servidores, estagiários, terceirizados e fornecedores que utilizem ativos de TIC.

CAPÍTULO II — DOS PRINCÍPIOS E DIRETRIZES

Art. 3º O PGR-TIC observará os seguintes princípios:

I – prevenção;

II – melhoria contínua;

III – visão integrada e institucional;

IV – gestão baseada em evidências;

V – proporcionalidade;

VI – transparência e rastreabilidade;

VII – conformidade com normas CNJ, LGPD e ISO 31000.

CAPÍTULO III — DO ESCOPO E DOS TIPOS DE RISCOS

Art. 4º O PGR-TIC abrange, no mínimo, os seguintes tipos de riscos:

I – riscos de segurança da informação;

II – riscos cibernéticos;

III – riscos operacionais;

IV – riscos de infraestrutura e continuidade;

V – riscos de sistemas e aplicações;

VI – riscos de dados, integridade, privacidade e LGPD;

VII – riscos de fornecedores, contratos e terceiros;

VIII – riscos de inovação e dependência tecnológica;

IX – riscos de pessoas e capacitação;
X – riscos regulatórios e de conformidade.

CAPÍTULO IV — DA GOVERNANÇA DO PGR-TIC

Art. 5º Compete à Presidência:
I – aprovar o PGR-TIC e suas revisões;
II – prover recursos necessários;
III – garantir prioridade institucional à gestão de riscos.

Art. 6º Compete ao Comitê de Governança de TIC (CGTIC):
I – supervisionar a execução do PGR-TIC;
II – aprovar matriz de riscos críticos;
III – deliberar sobre riscos estratégicos e severos;
IV – definir apetite e tolerância a riscos.

Art. 7º Compete ao CGESTIC:
I – acompanhar riscos operacionais;
II – monitorar mitigadores;
III – consolidar relatórios trimestrais.

Art. 8º Compete à Coordenadoria de TIC:
I – executar o processo contínuo de gestão de riscos;
II – aplicar metodologia e ferramentas definidas;
III – manter documentação atualizada;
IV – registrar riscos, eventos e mitigadores;
V – comunicar riscos relevantes ao CGESTIC e CGTIC.

Art. 9º Compete à ETIR/ETIS:
I – avaliar riscos relacionados a incidentes de segurança;
II – apoiar análise pós-incidente;
III – emitir recomendações técnicas.

Art. 10. Compete à Comissão de Segurança da Informação:
I – validar controles de mitigação;
II – revisar riscos de SI.

CAPÍTULO V — DO PROCESSO DE GESTÃO DE RISCOS
Art. 11. O processo seguirá a metodologia baseada na ISO 31000:

I - Identificação de riscos:
a) análise de processos;
b) inventário de ativos;
c) histórico de incidentes;
d) auditorias;
e) entrevistas e *workshops*;
f) requisitos legais;
g) riscos emergentes.

II - Análise de riscos:
a) probabilidade;
b) impacto operacional;
c) impacto jurídico;
d) impacto na imagem;
e) impacto financeiro;
f) impacto sobre continuidade.

III - Avaliação e priorização:
a) matriz de calor (*heatmap*);
b) níveis: baixo, médio, alto, crítico;
c) definição de prioridade.

IV - Tratamento:
a) mitigação;
b) aceitação;
c) transferência;

d) eliminação;
e) registro de responsáveis, prazos, evidências e *status*.

V - Monitoramento contínuo:
a) indicadores;
b) métricas;
c) *SLAs*;
d) revisão periódica de controles.

VI - Comunicação:
a) relatórios trimestrais (CGESTIC);
b) relatórios semestrais (CGTIC);
c) comunicação imediata de riscos críticos.

VII - Todos os riscos deverão ser registrados em:
a) sistema próprio ou planilha institucional;
b) matriz de riscos;
c) plano de ação;
d) níveis, responsáveis e status.

CAPÍTULO VI — DA EXECUÇÃO

Art. 12. O PGR-TIC deverá ser executado por meio de:
I – campanhas de conscientização;
II – avaliações periódicas de riscos;
III – testes de segurança e resiliência (*pentest* e vulnerabilidades);
IV – simulações de incidentes (*tabletop exercises*);
V – auditorias internas e externas;
VI – análises pós-incidente (RPI);
VII – atualizações do inventário de ativos;
VIII – relatórios de conformidade e governança.

CAPÍTULO VII — DA REVISÃO E MELHORIA CONTÍNUA

Art. 13. O PGR-TIC será revisado:

I – anualmente, obrigatoriamente;

II – sempre que houver mudanças tecnológicas significativas;

III – após incidentes de grande impacto;

IV – quando solicitado pelo CGTIC.

Art. 14. A revisão deverá conter:

I – lições aprendidas;

II – nova matriz de riscos;

III – indicadores;

IV – lista de riscos emergentes;

V – eficácia das ações mitigadoras.

CAPÍTULO VIII — DISPOSIÇÕES FINAIS

Art. 15. O PGR-TIC deverá ser disponibilizado na intranet institucional, em seção própria de governança de TIC.

Art. 16. Os casos omissos serão decididos pela Presidência.

Art. 17. Esta Portaria entra em vigor na data de sua publicação.

Gabinete da Presidência do Tribunal de Justiça Militar, em Porto Alegre, 17 de dezembro de 2025.

MARIA EMÍLIA MOURA DA SILVA

DESEMBARGADORA MILITAR PRESIDENTE

REGISTRE-SE E PUBLIQUE-SE.

Herbert Schonhofen
Diretor-Geral

Disponibilizada no Diário da Justiça Eletrônico nº 8.051, de 18 de dezembro de 2025, como se confere clicando aqui.