ESTADO DO RIO GRANDE DO SUL
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA MILITAR (TJMRS)

Coordenadoria de Tecnologia da Informação e Comunicação

Plano de Ação para Implementação do Manual de Proteção de Infraestruturas Críticas de TIC

Versão: 1.0

Período de Execução: Julho de 2024 a Dezembro de 2025
Responsável: Coordenadoria de TIC + Comitê de Segurança da Informação (CGSI)

1. Introdução

Este plano visa operacionalizar as orientações do **Manual de Proteção de Infraestruturas Críticas de TIC (PICTIC)** do Poder Judiciário, elaborado pelo CNJ, para garantir **resiliência, segurança e continuidade dos ativos tecnológicos essenciais ao funcionamento do TJMRS**.

A infraestrutura crítica compreende os sistemas, servidores, redes e pessoas cuja indisponibilidade compromete diretamente a prestação jurisdicional e a integridade institucional do Tribunal.

2. Objetivo Geral

Implementar controles, processos e estruturas de proteção e resposta para as infraestruturas críticas de TIC do TJMRS, conforme recomendações do CNJ, com foco em:

- **Prevenção de falhas e ataques**,
- **Resposta estruturada a incidentes graves**,
- **Continuidade dos serviços judiciais e administrativos**.

3. Etapas do Plano de Ação

Etapa 1: Identificação e Classificação de Infraestruturas Críticas

Prazo: Jul–Ago/2024
Responsável: Coord. de TIC / Infraestrutura
Atividades:

- Levantamento dos ativos críticos de TIC (servidores, sistemas, links, serviços).
- Classificação por criticidade e impacto (matriz C×I×P).
- Elaboração do Inventário de Infraestruturas Críticas de TIC (IIC-TIC).

Etapa 2: Avaliação de Vulnerabilidades e Riscos

Prazo: Set–Out/2024
Responsável: CGSI / Segurança
Atividades:

- Realização de varredura técnica nos ativos críticos.
- Avaliação de dependências técnicas e operacionais.
- Atualização do Plano de Gestão de Riscos com foco nos ativos críticos.

Etapa 3: Adoção de Controles de Proteção Física e Lógica

Prazo: Nov/2024 – Mar/2025
Responsável: Infraestrutura / Segurança Institucional
Atividades:

- Fortalecimento do controle de acesso físico a datacenters e salas técnicas.
- Implantação de autenticação forte para acessos privilegiados.
- Revisão de permissões e segregação de funções administrativas.
- Atualização de firewall, regras de rede e políticas de acesso externo.

Etapa 4: Integração com o Plano de Continuidade e DRP

Prazo: Mar–Mai/2025
Responsável: Coord. de TIC / CGSI
Atividades:

- Validação cruzada entre os ativos críticos e o PCN de TIC.
- Planejamento de recuperação de cada ativo (servidor, sistema, link).
- Atualização do DRP com cenários de indisponibilidade direcionados.

Etapa 5: Testes, Simulações e Treinamentos

Prazo: Jun–Ago/2025
Responsável: CGSI / Escola Judicial / TIC
Atividades:

- Realização de simulação de ataque cibernético com foco nos ativos críticos.
- Testes de restore de servidores e bancos de dados do eproc e SEI.
- Capacitação dos responsáveis por operação e contenção.

Etapa 6: Monitoramento e Auditoria

Prazo: Set–Dez/2025
Responsável: Coord. de TIC / Auditoria Interna
Atividades:

- Implantação de dashboards com alertas em tempo real (Zabbix, Power BI).
- Avaliação técnica e gerencial dos indicadores de resiliência.
- Auditoria final de aderência ao Manual do CNJ e elaboração de relatório conclusivo.

4. Indicadores de Sucesso

Indicador	Meta até Dez/2025
% de ativos críticos com plano de contingência documentado	100%
% de testes de restore realizados com sucesso	≥ 90%
% de pessoal crítico treinado em resposta a incidentes	≥ 85%
Inventário de Infraestruturas Críticas atualizado	100%
Relatório de auditoria final com avaliação positiva	100%

5. Governança e Monitoramento

- O plano será acompanhado **mensalmente pelo CGSI**.
- As principais ações constarão nos **relatórios trimestrais ao CGTIC**.
- Resultados e falhas serão tratados com base em planos de ação corretiva e preventiva.