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 Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

Versão: 1.0

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

1. Introdução

Este plano detalha a estratégia do TJMRS para **implementar práticas eficazes de prevenção, detecção e resposta a ameaças cibernéticas**, promovendo a **confiança digital institucional**, em conformidade com o **Manual do CNJ de Prevenção e Mitigação de Ameaças Cibernéticas (2023)**.

A crescente complexidade e sofisticação dos ataques exige uma abordagem preventiva, integrada e contínua, com foco na proteção dos dados judiciais, da infraestrutura crítica e da imagem institucional.

2. Objetivos

- Prevenir ameaças cibernéticas por meio de políticas e controles robustos;
- Reduzir a superfície de ataque por meio de boas práticas e conscientização;
- Mitigar rapidamente os efeitos de ataques quando ocorrerem;
- Estimular a confiança digital entre magistrados, servidores, jurisdicionados e parceiros;
- Integrar as ações locais às diretrizes do CNJ e da Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

3. Linhas de Ação

A estrutura do plano segue cinco pilares recomendados pelo CNJ:

1. Governança de Segurança Cibernética

Prazo: Ago–Out/2024
Ações:

- Atualização da Política de Segurança da Informação (PSI) com foco em cibersegurança.
- Criação de comitê técnico permanente de resposta a ameaças (subgrupo do CGSI).
- Definição formal de papéis e responsabilidades em incidentes cibernéticos.
- Registro do TJMRS como ponto de contato no CISPJ (Central de Incidentes do CNJ).

2. Fortalecimento de Controles Técnicos e Processos

Prazo: Out/2024 – Mar/2025
Ações:

- Reforço das configurações de firewall, segmentação de rede e VPN segura.
- Implantação de autenticação em dois fatores (2FA) para sistemas administrativos.
- Revisão periódica de permissões e credenciais de acesso.
- Verificação automática de atualizações de sistemas e SOs.

3. Conscientização e Cultura de Segurança

Prazo: Jan–Abr/2025
Ações:

- Realização de campanha anual de cibersegurança (internamente e no site).
- Treinamentos obrigatórios sobre phishing, senhas seguras, engenharia social.
- Simulado anual de tentativa de phishing (teste controlado).
- Criação de canal de denúncia de incidentes cibernéticos.

4. Detecção, Resposta e Recuperação

Prazo: Mar–Jun/2025
Ações:

- Integração entre Zabbix e ferramenta de SIEM/SOC para alertas correlacionados.
- Manualização dos procedimentos de resposta a incidentes (baseado na ISO 27035).
- Adoção de modelo de notificação automática ao CNJ em caso de evento grave.
- Testes semestrais de backup e restore de sistemas críticos (eproc, SEI).

🤝 5. Confiança Digital e Relacionamento com Usuários

Prazo: Mai–Dez/2025
Ações:

- Publicação de política de privacidade digital clara no portal institucional.

- Adoção de indicadores de transparência e disponibilidade digital.
- Divulgação ativa de boas práticas digitais nos canais internos e externos.
- Canal para avaliação de riscos por parceiros de tecnologia (fornecedores).

4. Cronograma Resumido (Gantt simplificado)

Ação	Início	Término
Governança	Ago/2024	Out/2024
Controles técnicos	Out/2024	Mar/2025
Conscientização	Jan/2025	Abr/2025
Detecção e resposta	Mar/2025	Jun/2025
Confiança digital	Mai/2025	Dez/2025

5. Indicadores de Monitoramento

Indicador	Meta
PSI atualizada com foco em cibersegurança	100% até out/2024
% de usuários com 2FA ativo	≥ 95% até mar/2025
% de pessoal treinado em boas práticas de cibersegurança	≥ 90% até abr/2025
Tempo médio de resposta a incidentes críticos (TTD)	≤ 30 min
Canal de privacidade e denúncia disponível no site	Até jul/2025

6. Integração com Outros Planos

Este plano está alinhado com:

- Plano de Continuidade de Serviços de TIC (PCN-TIC)
- Plano de Gestão de Riscos de TIC
- Política de Segurança da Informação (PSI)
- Plano de Transformação Digital (PTD)
- Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC-PJ)

7. Governança e Responsabilidade

Instância	Papel
CGSI	Gestão estratégica e aprovação das ações
Coordenadoria de TIC	Execução operacional e monitoramento técnico
Escola Judicial (EJM)	Apoio em campanhas e capacitação
Comunicação Social	Apoio à divulgação e cultura de segurança
Presidência e Direção-Geral	Suporte institucional e decisão em crises