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

PORTARIA Nº 095/2025

Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR/ETIS) no âmbito do Tribunal de Justiça Militar do Estado do Rio Grande do Sul e estabelece sua estrutura, competências, papéis, responsabilidades, governança e fluxo de resposta a incidentes.

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

CONSIDERANDO a necessidade de aprimorar o nível de maturidade em segurança da informação do TJMRS, em conformidade com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário – ENTIC-JUD;

CONSIDERANDO a Portaria CNJ nº 101/2025, que estabelece o Índice de Governança, Gestão e Infraestrutura de TIC (iGovTIC-JUD), o qual exige a existência formal de uma Equipe de Resposta a Incidentes de Segurança da Informação para fins de pontuação plena;

CONSIDERANDO as normas ISO/IEC 27001 e ISO/IEC 27035, que estabelecem padrões internacionais para gestão de incidentes de segurança;

CONSIDERANDO o aumento dos riscos cibernéticos e a necessidade de resposta rápida, organizada, contínua e integrada a incidentes de segurança da informação;

CONSIDERANDO a necessidade de integração com o CTIR Gov, Plataforma de Incidentes do CNJ, CSJT, órgãos de investigação e demais entidades externas competentes,

RESOLVE:

CAPÍTULO I — DA INSTITUIÇÃO

Art. 1º Fica instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR/ETIS) do Tribunal de Justiça Militar do Estado do Rio Grande do Sul, vinculada diretamente à Coordenadoria de Tecnologia da Informação e Comunicação (CTIC).

Art. 2º A ETIR/ETIS tem caráter permanente, técnico e multidisciplinar, atuando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados, mediante regime de plantão, sobreaviso e prontidão.

CAPÍTULO II — DAS FINALIDADES E OBJETIVOS

Art. 3º São finalidades da ETIR/ETIS:

I – atuar na prevenção, detecção, análise, resposta e recuperação de incidentes de segurança da informação e cibersegurança;

II – minimizar os impactos operacionais, jurídicos, reputacionais e de continuidade dos serviços;

III – atuar como ponto focal do TJMRS perante o CTIR Gov, CNJ, CSJT e autoridades externas;

IV – garantir conformidade com a PSI, LGPD, ENSEC-PJ, ISO 27001 e normas correlatas;

V – promover cultura de segurança e conscientização dos usuários;

VI – apoiar auditorias internas e externas em temas de segurança e incidentes.

CAPÍTULO III — DA COMPOSIÇÃO E PAPÉIS

Art. 4º A ETIR/ETIS será composta por:

I – Coordenador da ETIR/ETIS (Chefe da Unidade de Segurança da Informação):

a) liderar incidentes críticos;

b) comunicar Presidência, Direção-Geral e magistrados quando necessário;

c) coordenar contato com CTIR Gov, CNJ, CSJT;

d) declarar severidade do incidente;

e) emitir relatórios pós-incidente (RPI).

II – Analistas de Resposta a Incidentes (Analistas ETIR):

a) análise técnica, contenção, erradicação, recuperação;

b) coleta e preservação de evidências;

c) acompanhamento de logs, *SIEM*, *firewall*, *IPS/IDS*, antivírus, *EDR*;

d) acionamento de plantonistas.

III – Equipe de Infraestrutura:

a) restabelecimento de serviços;

b) bloqueio de acessos;

c) contenção de ataques;

d) análise de rede.

IV – Equipe de Sistemas e Desenvolvimento:

a) validação de integridade de sistemas;

b) *rollback* e restauração;

c) análise de códigos afetados;

d) mitigação de vulnerabilidades.

V – Equipe Jurídica/Corregedoria (quando aplicável):

a) suporte em impactos legais e de LGPD;

b) comunicação a órgãos oficiais;

c) apoio à investigação.

VI – Comissão de Segurança da Informação:

a) apoio estratégico;

b) recomendações pós-incidente.

CAPÍTULO IV — DO FLUXO DE RESPOSTA A INCIDENTES (24×7)

Art. 5º O fluxo oficial da ETIR/ETIS será composto por 7 fases:

I - Identificação

a) alerta via SIEM, firewall, e-mail, usuário ou fornecedor;

b) classificação preliminar (evento x incidente);

c) registro inicial no Sistema de Gestão de Incidentes.

II - Classificação e Severidade

A ETIR/ETIS classificará como:

a) nível 1 – Baixo impacto;

b) nível 2 – Médio impacto;

c) nível 3 – Alto impacto;

d) nível 4 – Crítico / Ataque em curso / indisponibilidade sistêmica.

Parágrafo único. Para níveis 3 e 4, o Coordenador da ETIR é acionado imediatamente.

III - Contenção Imediata (Short-term Containment)

Medidas típicas:

a) isolar máquinas;

b) bloquear IPs;

c) suspender credenciais;

d) retirar sistemas do ar;

e) ativar redundâncias;

f) interromper tráfego suspeito.

IV - Erradicação

a) remoção de *malware*;

b) aplicação de *patches*;

c) eliminação de *backdoors*;

d) redefinição de credenciais;

e) validação de *logs*.

V - Recuperação

a) restauração de *backups*;

b) verificação de integridade;

c) retorno gradual dos sistemas;

d) monitoramento pós-recuperação por 72h.

VI - Comunicação Institucional e Externa

Deverão ser notificados quando aplicável:

a) Presidência do Tribunal;

b) Direção-Geral;

c) CGTIC;

d) CNJ (Plataforma de Incidentes);

e) CTIR Gov;

f) CSJT (quando envolver magistratura/judiciário);

g) Autoridades policiais (cibercrimes);

h) NUGEP e Comitês internos.

VII - Relatório Pós-Incidente (RPI)

Emitido em até 10 dias, contendo:

a) descrição do incidente;

b) linha do tempo;

c) sistemas afetados;

d) impactos e severidade;

e) causa raiz (*root cause analysis*);

f) evidências preservadas;

g) medidas adotadas;

h) recomendações;

i) plano de prevenção.

CAPÍTULO V — DOS NÍVEIS DE SEVERIDADE

Art. 6º A ETIR/ETIS utilizará a seguinte matriz:

Nível	Descrição	Ação Obrigatória
1	Baixo impacto	Registro e acompanhamento
2	Médio impacto	Intervenção remota e mitigação
3	Alto impacto	Acionamento integral da ETIR
4	Crítico / Ataque	Comunicação à Presidência + CNJ + CTIR Gov

CAPÍTULO VI — DA INTEGRAÇÃO COM CNJ, CSJT E CTIR GOV

Art. 7º A ETIR/ETIS deverá atuar de forma integrada com:

I – CTIR Gov, conforme padrões do Governo Federal;

II – Plataforma Nacional de Gestão de Incidentes do CNJ;

III – CSJT, no tocante a alertas de segurança de sistemas judiciais;

IV – Autoridades policiais em caso de crimes cibernéticos.

CAPÍTULO VII — DA PRESERVAÇÃO DE EVIDÊNCIAS

Art. 8º A ETIR/ETIS deverá seguir procedimentos formais de cadeia de custódia, garantindo:

I – integridade de logs;

II – rastreabilidade;

III – coleta padronizada;

IV – armazenamento seguro;

V – documentação para auditorias.

CAPÍTULO VIII — DO TREINAMENTO E CAPACITAÇÃO

Art. 9º Os membros da ETIR/ETIS devem receber capacitação continuada nas áreas:

I - resposta a incidentes;

II - forense digital;

III - SIEM/SOC;

IV - LGPD;

V - análise de *malware*;

VI - normas ISO 27001 / 27035;

VII - análise de risco cibernético.

CAPÍTULO IX — DISPOSIÇÕES FINAIS

Art. 10. O fluxo da ETIR/ETIS poderá ser complementado por Procedimentos Operacionais Padrão (POPs).

Art. 11. Casos omissos serão resolvidos pela Presidência.

Art. 12. 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.