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

Coordenadoria de Tecnologia da Informação e Comunicação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Versão: 1.0

Aprovação:

- Herbert Schonhofen – Diretor-Geral
- Eduardo Severo – Coordenador de TIC

1. OBJETIVO

Estabelecer princípios, diretrizes e responsabilidades para garantir a proteção das informações institucionais do TJMRS contra acessos não autorizados, uso indevido, perda, destruição, alteração ou divulgação indevida. A PSI visa assegurar a continuidade institucional, a confiança da sociedade e o cumprimento das legislações vigentes.

2. FUNDAMENTAÇÃO LEGAL E NORMATIVA

Esta política está baseada nas seguintes normas e diretrizes:

- Constituição Federal de 1988;
- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução CNJ nº 370/2021 – Estratégia Nacional de Segurança da Informação do Poder Judiciário;
- ISO/IEC 27001 e 27002 – Normas internacionais de gestão da segurança da informação;
- Demais normativos internos e externos aplicáveis.

3. ABRANGÊNCIA

Esta política se aplica a:

- Magistrados e servidores do TJMRS;
- Estagiários e colaboradores terceirizados;
- Fornecedores, consultores e quaisquer terceiros com acesso às informações ou recursos computacionais do Tribunal.

4. PRINCÍPIOS NORTEADORES

- **Confidencialidade**: Garantir que a informação esteja acessível apenas a quem tenha autorização.
- **Integridade**: Assegurar a exatidão e a completude da informação e seus métodos de processamento.

- **Disponibilidade**: Garantir o acesso à informação por usuários autorizados quando necessário.
- **Autenticidade**: Confirmar a identidade de usuários, dispositivos e sistemas envolvidos.
- **Legalidade**: Observar a legislação e normativas aplicáveis.
- **Responsabilidade**: Todos os envolvidos devem adotar conduta ética e responsável no uso da informação.
- **Proporcionalidade**: As medidas de proteção devem ser proporcionais ao valor e criticidade da informação.

5. DIRETRIZES GERAIS

5.1 Classificação da Informação

As informações institucionais devem ser classificadas, no mínimo, nos seguintes níveis:

- **Pública**: Acessível a qualquer cidadão.
- **Restrita**: Acessível apenas a determinados grupos internos.
- **Confidencial**: Acesso restrito a um número reduzido de usuários com necessidade de conhecimento.

5.2 Controle de Acesso

- O acesso aos ativos de informação deve ser autorizado, registrado e periodicamente revisado.
- Princípio do **menor privilégio**: usuários devem ter acesso apenas ao necessário para seu trabalho.
- Senhas devem ser fortes, individuais, e trocadas periodicamente.

5.3 Segurança Física e Ambiental

- Ambientes de TIC devem ser protegidos contra acessos físicos indevidos.
- Equipamentos devem estar localizados em áreas seguras, com controle de entrada.

5.4 Backup e Recuperação

- Backups devem ser realizados periodicamente e armazenados em local seguro.
- Devem existir procedimentos formais de recuperação de dados em caso de falhas.

5.5 Gestão de Incidentes de Segurança

- Todos os incidentes devem ser reportados imediatamente à área de TIC.
- Deve haver um plano de resposta a incidentes com responsáveis definidos.

5.6 Continuidade de Serviços

- Deve existir um Plano de Continuidade e Recuperação de Desastres (PCN), atualizado e testado.

5.7 Uso Aceitável dos Recursos de TIC

- É vedado o uso dos recursos tecnológicos do TJMRS para fins particulares, ilícitos ou que comprometam a imagem institucional.
- Todos os acessos e usos dos recursos podem ser auditados.

5.8 Segurança na Contratação de Terceiros

- Contratos devem prever cláusulas de confidencialidade e conformidade com esta política.
- Terceiros devem receber treinamento mínimo sobre segurança da informação.

5.9 Treinamento e Conscientização

- A capacitação periódica em segurança da informação é obrigatória para todos os públicos-alvo desta política.
- A cultura de segurança deve ser disseminada de forma contínua.

6. ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

6.1 Comitê de Governança de TIC e Segurança da Informação (CGovTI-SI)

- Responsável por aprovar diretrizes, revisar políticas, supervisionar planos e garantir alinhamento institucional.

6.2 Área de TIC

- Responsável pela implementação das diretrizes técnicas, monitoramento, resposta a incidentes e suporte à continuidade.

6.3 Usuários

- Responsáveis pelo uso adequado dos recursos, pela proteção das informações sob sua guarda e pela notificação de incidentes.

7. SANÇÕES

O descumprimento das normas desta política poderá sujeitar o infrator a:

- Advertência ou suspensão;
- Responsabilização civil, administrativa e penal;
- Rescisão contratual (no caso de terceiros).

8. REVISÃO E APERFEIÇOAMENTO

Esta política deve ser revista, no mínimo, anualmente ou sempre que houver:

- Alterações significativas na estrutura tecnológica;
- Incidentes relevantes;
- Mudanças na legislação aplicável.

HERBERT SCHONHOFEN
Diretor Geral

EDUARDO DE BORBA SEVERO
Coordenador de TIC