Art. 18. A Secretaria de Tecnologia da Informação elaborará, em até 120 (cento e vinte) dias, os procedimentos operacionais para aplicação desta norma, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.
Art. 19. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado como incidente de segurança da informação, para apuração pela Comissão de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 20. Esta norma complementar deve ser revisada a cada 12 (doze) meses pelo(a) gestor(a) de Segurança da Informação e encaminhada para nova apreciação da Comissão de Segurança da Informação.
Art. 21. Esta portaria entra em vigor na data de sua publicação.
Campo Grande, na data da assinatura eletrônica.
Desembargador CARLOS EDUARDO CONTAR
Presidente

PORTARIA PRESIDÊNCIA Nº 86/2025 TRE/PRE/GABPRE

Estabelece norma de configuração segura de ambientes, referente à Política de Segurança da Informação da Justiça Eleitoral de Mato Grosso do Sul.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE MATO GROSSO DO SUL, DESEMBARGADOR CARLOS EDUARDO CONTAR, no uso de suas atribuições legais e regimentais; e
CONSIDERANDO a Resolução CNJ n.º 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO o disposto na Resolução CNJ n.º 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO o disposto na Resolução TSE n.º 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO as boas práticas de segurança da informação e privacidade previstas nas normas da Associação Brasileira de Normas Técnicas - ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002, complementadas pela norma ABNT NBR ISO/IEC 27701;
CONSIDERANDO a Resolução TRE/MS n.º 822, 9 de abril de 2024, que implementa, no âmbito do TRE/MS, a PSI da Justiça Eleitoral estabelecida pela Resolução TSE nº 23.644/2021; e
CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral de Mato Grosso do Sul.
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de configuração segura de ambientes, em consonância com a Política de Segurança da Informação da Justiça Eleitoral de Mato Grosso do Sul.
Art. 2º Para efeitos desta norma consideram-se os termos e definições previstos na Portaria DG /TSE n.º 444, de 8 de julho de 2021.
CAPÍTULO II
DA PREPARAÇÃO DA INSTALAÇÃO
Art. 3º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados na instalação de serviços ou sistemas de informação no ambiente da rede corporativa:
I - planejamento e documentação da instalação, definindo o seguinte conjunto mínimo de informações:
a) propósito do serviço ou sistema de informação a ser instalado;

b) funcionalidades que serão disponibilizadas;
c) configuração de segurança;
d) configuração de hardware;
e) estratégia de particionamento;
f) imagem da instalação utilizada.
II - obtenção prévia de todas as documentações, roteiros, matriz de compatibilidade, drives e mídias de instalação que serão utilizadas;
III - instalação preferencialmente a partir de dispositivos de armazenamento locais (p. ex. disco) desconectados da rede corporativa ou em um segmento isolado acessível apenas pela rede corporativa; e
IV - geração de registros de eventos (logs) das ações realizadas para instalação e configuração dos serviços ou sistemas de informação, identificados de forma distinta.
Art. 4º É recomendado evitar a concentração de serviços ou sistemas de informação em um único servidor, para aumentar sua disponibilidade na rede corporativa e reduzir a extensão de um eventual comprometimento a partir de um desses serviços ou sistemas.
CAPÍTULO III
DA ESTRATÉGIA DE PARTICIONAMENTO
Art. 5º A estratégia de particionamento deve ser definida conforme as necessidades e características dos serviços ou sistemas de informação, mas deve ser analisada com especial atenção nas seguintes situações:
I - quando os serviços ou sistemas de informação forem suscetíveis a problemas de esgotamento do espaço de armazenamento por usuário ou programa mal-intencionado que tenha permissão de escrita, como áreas temporárias e de armazenamento de registros de eventos (logs), a demandar, como forma de evitar o travamento do serviço ou sistema de informação, a instalação de programas de computador e o espaço de armazenamento em partições diferentes;
II - quando for necessário definir determinadas características individuais para cada partição, como o uso em modo somente leitura;
III - quando forem necessárias múltiplas operações de disco em paralelo, isolada ou conjuntamente com o uso de otimizações individuais para cada partição, o que pode aumentar significativamente o desempenho dos serviços ou sistemas de informação; e
IV - quando for necessário flexibilizar o procedimento de cópia de segurança (backup) dos serviços ou sistemas de informação, pois simplifica funções como copiar partições inteiras de uma só vez; excluir partições individuais do procedimento ou fazer cópia de segurança em intervalos diferentes para cada partição.
Art. 6º Na definição da estratégia de particionamento, é recomendado avaliar a conveniência dos seguintes controles:
I - divisão de disco em várias partições em vez de usar uma única partição ocupando o disco inteiro;
II - dimensionamento de cada partição de acordo com os requisitos de cada serviço ou sistema de informação, seguindo orientações de tamanho ocupado indicado na documentação do fornecedor;
III - dimensionamento da partição principal de estações de trabalho suficiente para o download dos pacotes de atualizações do sistema operacional; e
III - implementação de partições específicas para:
a) programas do sistema operacional;
b) dados dos usuários;
c) registros de eventos (logs);
d) arquivos temporários;
e) filas de envio e recepção de e-mails, quando for o caso;

f) filas de impressão;
g) repositórios de arquivos; e
h) páginas web.

CAPÍTULO IV

DAS SENHAS DE ADMINISTRADOR

Art. 7º Caso seja solicitada a criação de senha de administrador durante a instalação de um serviço ou sistema de informação, considerar, minimamente, as seguintes ações:

I - definição de senha tão cedo quanto possível, preferencialmente antes da instalação;

II - substituição de senha padrão do fabricante;

III - utilização de senha forte com base nos padrões estabelecidos pela Norma de Controle de Acesso Físico e Lógico;

IV - utilização de senhas que sejam únicas para o sistema em questão, quando a autenticação por múltiplos fatores não for suportada (como administrador local ou contas de serviço); e

V - deve ser considerada a utilização de recurso de Autenticação Multifator (MFA) e Cofre de Senhas, caso a senha esteja relacionada a credenciais de acesso privilegiado.

CAPÍTULO V

DA INSTALAÇÃO MÍNIMA

Art. 8º Os controles mínimos de proteção estabelecidos nos incisos deste artigo devem ser implementados para evitar que componentes e pacotes não utilizados pelos serviços ou sistemas de informação exponham o ambiente da rede corporativa a vulnerabilidades que possam vir a ser exploradas por um atacante, por falta de monitoramento regular ou pela não aplicação das correções previstas:

I - identificação de quais componentes e pacotes podem deixar de ser instalados sem comprometer a funcionalidade do serviço ou sistema de informação ou a estabilidade do ambiente da rede corporativa, via mecanismo de controle de dependências (que avisa quando determinado componente precisa de outro para funcionar), consulta à documentação ou apoio do suporte técnico do fornecedor;

II - abstenção de instalar componentes e pacotes cuja funcionalidade seja desconhecida ou cuja necessidade não seja justificada;

III - opção pela instalação personalizada, em detrimento da instalação típica, para instalar a base do serviço ou sistema de informação e selecionar cuidadosamente quais componentes extras serão adicionados;

IV - instalação do mínimo possível de componentes e pacotes, especialmente dos que implementam serviços de rede; e

V - limitação do acesso a ferramentas de scripting (instruções escritas) exclusivamente a usuários administrativos ou de desenvolvimento que necessitem acessar tais funcionalidades.

CAPÍTULO VI

DA DESATIVAÇÃO DE FUNCIONALIDADES NÃO UTILIZADAS

Art. 9º Os controles mínimos de proteção estabelecidos nos incisos deste artigo devem ser implementados nos casos de instalação completa de serviço ou sistema de informação e de seus componentes e pacotes para poder utilizar um subconjunto das funcionalidades:

I - desativação de serviços não essenciais e funcionalidades (locais e, principalmente, de rede) que não serão imediatamente utilizadas;

II - emprego de filtro de pacotes para definir as origens aceitáveis para os acessos às portas de comunicação/transporte (portas TCP/UDP) utilizadas, evitando assim a possibilidade de acesso a partir de equipamentos que não tenham uma necessidade legítima de uso do serviço disponibilizado; e

III - configuração de políticas de segurança e restrição de permissões, em conformidade com a política de privilégio mínimo.

CAPÍTULO VII

DAS IMAGENS DE INSTALAÇÃO

Art. 10. Imagens das instalações seguras pré-configuradas devem ser estabelecidas e mantidas para todos os dispositivos móveis, notebooks, estações de trabalho e servidores, com base nos padrões de configuração definidos pelas seções responsáveis pelas configurações dos respectivos ativos de processamento.

Art. 11. A quantidade de variações de imagens das instalações seguras pré-configuradas deve ser reduzida ao mínimo para melhor entendimento e gerenciamento dos requisitos de segurança de cada uma.

Art. 12. Os arquivos com imagens das instalações seguras pré-configuradas devem ser protegidos para que não seja possível o acesso e a alteração não autorizados das informações.

Parágrafo único. Os controles mínimos de proteção estabelecidos nos incisos deste artigo devem ser implementados:

I - armazenamento em local centralizado e resguardado de acessos indevidos;

II - armazenamento em segmento isolado da rede corporativa, com proteção de dispositivos de segurança, tais como firewall(monitor tráfego de rede), sistema de detecção e prevenção de intrusões, entre outros;

III - localização física em área de segurança;

IV - utilização de protocolos seguros para acesso remoto;

V - capacidade de assinatura digital ou resumo criptográfico para verificação da integridade;

VI - geração de registros de eventos (logs) para todos os trabalhos executados nos arquivos; e

VII - manutenção de documentação atualizada dos procedimentos de:

a) configuração, instalação e manutenção;

b) administração e operação; e

c) cópia de segurança e restauração.

CAPÍTULO VIII

DA DOCUMENTAÇÃO E CONFIGURAÇÃO DAS IMAGENS

Art. 13. A instalação e as alterações na configuração dos serviços ou sistemas de informação e de seus componentes devem ser documentadas para registrar quais passos exatos foram seguidos para alcançar pleno êxito, de forma que seja possível reconstituir, a partir dessas informações, a última configuração antes de uma falha, sem a necessidade de recorrer a cópias de segurança (backup).

Art. 14. Os registros de configuração da imagem devem conter informações mínimas e relevantes, especialmente:

I - data da modificação;

II - responsável pela modificação;

III - justificativa para a modificação;

IV - descrição da modificação;

V - sistema operacional utilizado;

VI - descrição de como o serviço ou sistema de informação foi instalado, quais componentes e pacotes foram implementados e quais funcionalidades foram desativadas e bloqueadas;

VII - configuração de segurança implementada;

VIII - indicação de como foi feito o particionamento;

IX - local onde pode ser encontrada a lista de pacotes instalados;

X - descrição de quais portas ficaram ativas após a instalação; e

XI - indicação de quais os usuários criados com seus respectivos UIDs (identificador de usuário) e GIDs (gestor de identidade).

Art. 15. Os registros de configuração da imagem devem ser armazenados em local seguro e com acesso restrito aos administradores dos ativos de informação e de processamento, pois contêm informações que podem ser utilizadas para comprometer mais facilmente a segurança do ambiente da rede corporativa.

CAPÍTULO IX

DA INSTALAÇÃO DE CORREÇÕES

Art. 16. Deverá ser implantado processo de gerenciamento de correções de sistemas operacionais e de softwares de terceiros, para assegurar que estejam executando as atualizações de segurança mais recentes disponibilizadas pelos fabricantes.

Art. 17. Os controles mínimos estabelecidos nos incisos deste artigo devem ser implementados para assegurar que as configurações estabelecidas não foram alteradas durante o processo de instalação de correções (patches, fixes, service packs) para vulnerabilidades conhecidas nos serviços ou sistemas de informação:

I - aplicação somente daquelas que corrigem problemas em componentes que estejam efetivamente instalados, pois a instalação indiscriminada de atualizações pode enfraquecer a segurança do ambiente da rede corporativa ao invés de fortalecê-la;

II - revisão da configuração dos serviços ou sistemas de informação após instalar uma correção, para certificar-se de que a instalação não tenha revertido eventuais modificações realizadas (especialmente aquelas destinadas a desativar componentes e funcionalidades);

III - estabelecer o escalonamento da implantação de correções por grupos de computadores ou unidades organizacionais, e agendamento em horários adequados, visando diminuir o impacto das atualizações no tráfego de rede e funcionamento de serviços essenciais; e

VI - estabelecer o processo de atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com maior frequência.

Art. 18. Os registros de configuração da imagem devem ser atualizados com as ações realizadas durante o processo de instalação de correções.

Art. 19. Estações de trabalho e notebooks com Sistemas Operacionais sem suporte do fabricante para novas atualizações de segurança devem ser imediatamente substituídos por outro equipamento com Sistema Operacional atualizado e estável.

Parágrafo único. No caso de Servidores de Rede em produção, será feito planejamento para atualização do Sistema Operacional e migração de sistemas hospedados, visando diminuir a possibilidade de indisponibilidade dos serviços de TIC.

CAPÍTULO X

DAS FERRAMENTAS DE GERENCIAMENTO DE CONFIGURAÇÃO

Art. 20. Os controles mínimos estabelecidos nos incisos deste artigo devem ser implementados para assegurar que as configurações estabelecidas não sejam alteradas acidental ou intencionalmente durante o uso dos serviços ou sistemas de informação:

I - utilização de ferramenta de gerenciamento de configuração que automaticamente impõe as configurações estabelecidas de serviços ou sistemas de informação em intervalos agendados regularmente; e

II - utilização de sistema de monitoramento de configuração para verificar se a configuração corrente permanece idêntica à configuração aprovada, catalogar exceções aprovadas e alertar quando ocorrerem alterações não autorizadas.

CAPÍTULO X

DO SUPORTE DOS FABRICANTES E COMUNIDADES

Art. 21. Todos os ambientes computacionais deverão ser mantidos em versões suportadas pelos respectivos fabricantes ou comunidades desenvolvedoras, de forma a garantir a existência de correções para os problemas de segurança identificados, bem como viabilizar a prestação de suporte técnico pelo fabricante.

§ 1º Para soluções baseadas em código aberto ou software gratuito, deve ser assegurado que seus projetos estejam ativos e suportados pelas respectivas comunidades.

§ 2º Caso algum ambiente se mantenha operacional em versão não suportada pelo fabricante ou pela comunidade, deverão ser analisadas medidas adicionais de segurança que assegurem a proteção do ativo de processamento e do respectivo ambiente.

CAPÍTULO XII

DISPOSIÇÕES FINAIS

Art. 22. Os casos omissos serão resolvidos pela Diretoria-Geral, subsidiada pela Comissão de Segurança da Informação deste Tribunal.

Art. 23. A revisão desta portaria ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 18 (dezoito) meses.

Art. 24. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à Comissão de Segurança da Informação para apuração e consequente adoção das providências cabíveis.

Art. 25. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 8 (oito) meses a contar desta data.

Campo Grande, na data da assinatura eletrônica.

Desembargador CARLOS EDUARDO CONTAR

Presidente

PORTARIA PRESIDÊNCIA Nº 85/2025 TRE/PRE/GABPRE

Aprova o Plano de Gestão de Riscos de TIC no âmbito do Tribunal Regional Eleitoral de Mato Grosso do Sul.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE MATO GROSSO DO SUL, DESEMBARGADOR CARLOS EDUARDO CONTAR, em exercício, no uso de suas atribuições que lhe são conferidas pelo art. 43, XI e XXI, do Regimento Interno do Tribunal (Resolução TRE-MS n.º 801/2022),

Considerando as diretrizes estabelecidas na Política de Gestão de Riscos, aprovada pela Resolução TRE/MS n.º 657/2019;

Considerando os termos do art. 37, da Resolução CNJ nº 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

RESOLVE:

Art. 1º Aprovar o Plano de Gestão de Riscos de TIC (PGR TIC 2025), com foco na continuidade de negócios, manutenção dos serviços e alinhamento ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas e atuar de forma preditiva e preventiva às possíveis incertezas, registrado sob evento SEI de ID 1857625.

Art. 2º O processo de gestão de riscos de TIC deverá observar como metodologia o Manual de Gestão de Riscos do TRE/MS, segunda edição, instituído pela Portaria PRE nº 2/2025 e seu Anexo , e as disposições contidas na Resolução TRE/MS n. 657/2019, que instituiu a Política de Gestão de Riscos do TRE/MS.

Art. 3º Revoga-se a Portaria PRE n.º 202/2023, de 31 de julho de 2023.

Art. 4º Esta Portaria entrará em vigor na data de sua assinatura.

Campo Grande/MS, na data da assinatura eletrônica.

Desembargador CARLOS EDUARDO CONTAR