III - propor soluções de backup das informações produzidas ou custodiadas pelo Tribunal;
IV - providenciar a criação e manutenção dos backups;
V - configurar as soluções de backup;
VI - manter as unidades de armazenamento de backups funcionais, preservadas e seguras;
VII - verificar periodicamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;
VIII - gerenciar mensagens e registros de auditoria (logs) dos backups;
IX - tomar medidas preventivas para evitar falhas;
X - reportar imediatamente os incidentes ou erros que causem indisponibilidade ou que impossibilitem a restauração dos backups;
XI - providenciar a execução dos testes de restauração;
XII - restaurar ou recuperar os backups em caso de necessidade.
CAPÍTULO V
DAS DISPOSIÇÕES FINAIS
Art. 32. Esta norma complementar deverá ser revisada a cada 12 meses.
Art. 33. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão de Segurança da Informação deste Tribunal.
Art. 34. Esta Portaria entrará em vigor na data de sua publicação.
Cuiabá, 8 de novembro de 2022.
Desembargador **CARLOS ALBERTO ALVES DA ROCHA**
Presidente do TRE-MT

PORTARIA Nº 427/2022

Institui norma de gerenciamento de vulnerabilidades no âmbito do Tribunal Regional Eleitoral de Mato Grosso.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO, no uso das atribuições que lhe confere art. 19, XI, do Regimento Interno deste Tribunal,
CONSIDERANDO a Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução TSE nº 23.644/2021, que instituiu a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO o que consta no Processo SEI nº 8303.2022-9,
RESOLVE
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de Gerenciamento de Vulnerabilidades, em consonância com a Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral de Mato Grosso.
CAPÍTULO II
DEFINIÇÕES
Art. 2º Para efeitos desta Portaria consideram-se as seguintes definições:
I - Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
II - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
III - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

IV - Ativo de informação: todo dado ou informação gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento.

CAPÍTULO III

DOS OBJETIVOS

Art. 3º A gestão de vulnerabilidades tem como objetivo prevenir a exploração de vulnerabilidades técnicas na rede corporativa, por meio da aplicação sistemática das seguintes ações de prevenção, identificação, classificação e tratamento:

I - adoção de ações técnicas preventivas conforme norma de Configuração Segura de Ativos de TI vigente;

II - obtenção de informações para identificar vulnerabilidades técnicas em tempo hábil;

III - avaliação de exposição às vulnerabilidades técnicas;

IV - adoção de medidas apropriadas e tempestivas para lidar com os riscos identificados.

CAPÍTULO IV

DO MONITORAMENTO DE BASES DE VULNERABILIDADES

Art. 4º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção:

I. definir a relação de fontes de consulta pelos seguintes critérios:

a) qualidade das informações: verificar se as informações fornecidas pela fonte são precisas e atualizadas (algumas apenas repassam notícias ou informações de outras fontes);

b) disponibilidade das informações: verificar a frequência de atualização das informações fornecidas pela fonte (a vulnerabilidade técnica pode ser explorada por um período mais longo se a fonte demorar muito para atualizar suas informações);

c) legitimidade da fonte: verificar se a fonte é representante autorizado do responsável pela informação (como fóruns específicos de fabricantes para comunicação com seus clientes ou fornecimento de patches) ou reconhecida como confiável pela comunidade de segurança da informação.

II. obter informações sobre vulnerabilidades técnicas e medidas de correção, incluindo:

a) notícias e alertas sobre ameaças, vulnerabilidades, ataques e patches, com especial atenção às vulnerabilidades de dia zero;

b) melhores práticas de segurança da informação adotadas pelo mercado: políticas, procedimentos, diretrizes e listas de verificação;

c) tendências do mercado de segurança da informação relacionadas ao setor: leis e regulamentos, requisitos de clientes e soluções de fornecedores;

d) dados sobre segurança da informação de consultorias especializadas, outras organizações, polícia, agências de segurança do governo ou congêneres;

e) notícias relacionadas a novas tecnologias e produtos.

CAPÍTULO V

DA DESCOBERTA DE VULNERABILIDADES TÉCNICAS

Art. 5º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para utilizar regularmente ferramentas automatizadas e rotinas para a identificação de vulnerabilidades técnicas na rede corporativa:

I - empregar ferramenta atualizada de varredura de vulnerabilidades para investigar automaticamente os ativos e identificar vulnerabilidades na rede corporativa, considerando pelo menos as seguintes características:

a) utilização da fonte Common Vulnerabilities and Exposures (CVE) como base para a verificação de vulnerabilidades nos ativos de processamento;
b) compatibilidade com Security Content Automation Protocol (SCAP) ou outro protocolo de automatização da verificação de configurações de segurança;
II - assegurar que somente varreduras de vulnerabilidades autorizadas possam ser executadas, local ou remotamente, e configuradas com direitos elevados nos ativos de processamento que estão sendo testados;
III - usar credencial (ou conta de acesso) dedicada para varreduras de vulnerabilidades, que não deve ser usada para outras atividades administrativas e deve estar vinculada aos equipamentos específicos em endereços de Internet Protocol (IP) específicos.

CAPÍTULO VI

DA AVALIAÇÃO DA EXPOSIÇÃO

Art. 6º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para analisar e avaliar os riscos de as vulnerabilidades técnicas afetarem o ambiente da rede corporativa:
I - consulta de inventário de ativos para identificar quais ativos de processamento serão afetados pela vulnerabilidade técnica, o valor dos ativos para a organização, os requisitos de segurança da informação e a classificação de segurança;
II - verificação de como a vulnerabilidade técnica pode afetar o ambiente da rede corporativa, considerando interfaces e interdependências internas e externas, requisitos de segurança da informação implementados e classificação de segurança dos ativos de processamento considerados críticos;
III - avaliação quanto à necessidade de criar ambiente de teste, realizar provas de conceito (Proofs of Concept ou PoCs), desativar serviços/funcionalidades ou aplicar patches de correção;
IV - documentação de procedimentos para correção da vulnerabilidade técnica, contemplado instalação, configuração, regras estabelecidas e procedimentos de restauração (caso a correção introduza comportamento instável na rede corporativa);
V - utilização de classificação de risco para priorizar a correção da vulnerabilidade técnica, conforme nível de criticidade, potencial de dano, facilidade de exploração da ameaça e nível de sigilo das informações acessadas pelo ativo;
VI - comunicação imediata à Comissão de Segurança da Informação sobre a impossibilidade de tratamento de vulnerabilidade técnica classificada como crítica;
VII - geração de registro do incidente.

CAPÍTULO VII

DO TRATAMENTO DE VULNERABILIDADES TÉCNICAS

Art. 7º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para corrigir as vulnerabilidades técnicas ou minimizar a probabilidade de exploração:
I - observância da norma de Tratamento e Resposta a Incidentes em Redes de Computadores vigente;
II - adoção de testes e homologação da correção da vulnerabilidade técnica antes de ser instalada no ambiente da rede corporativa;
III - atualização dos procedimentos para correção da vulnerabilidade técnica, contemplado instalação, configuração, regras estabelecidas e procedimentos de restauração, quando for o caso;
IV - geração de registros de eventos (logs) das ações realizadas para correção da vulnerabilidade técnica, identificados de forma distinta;
V - quando não existir a possibilidade de correção da vulnerabilidade - seja por impossibilidade de atualização de software ou alteração de configuração - desde que devidamente justificado, deverá ser considerado o uso de outros controles, tais como:

a) desativação de serviços relacionados à vulnerabilidade;
b) aumento do monitoramento relacionado ao ativo para detectar ou prevenir ataques reais;
c) aumento da conscientização sobre a vulnerabilidade;
d) implementação de controles de segurança compensatórios.
Art. 8º As mudanças no ambiente da rede corporativa motivadas pelas correções das vulnerabilidades técnicas devem ser implantadas de acordo com o processo de Gerência de Mudanças vigente.
CAPÍTULO VI
DA AVALIAÇÃO DE RESULTADOS
Art. 9º Os controles estabelecidos nos incisos deste artigo devem ser aplicados para analisar criticamente os resultados da gestão de vulnerabilidades:
I - comparação regular dos resultados dos tratamentos de vulnerabilidades técnicas consecutivas para verificar se foram corrigidas em tempo hábil;
II - acompanhamento regular do nível de exposição dos principais ativos de processamento;
III - acompanhamento regular da evolução das vulnerabilidades técnicas no ambiente da rede corporativa;
IV - comunicação periódica à Comissão de Segurança da Informação (CSI), através de relatórios estatísticos, a respeito dos resultados de detecção e tratamento das vulnerabilidades no ambiente computacional;
V - proposição de melhorias nos processos da gestão de vulnerabilidades para a CSI.
CAPÍTULO VII
DAS RESPONSABILIDADES
Art. 10. Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas, as responsabilidades e competências no âmbito da segurança da informação devem observar os seguintes parâmetros:
I. à Seção de Gerencia de Redes caberá:
a) monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção;
b) acionar ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas no ativo, assegurando a execução de verificações na periodicidade mínima definida para cada tipo de ativo no procedimento vigente de Gestão de Ativos;
c) analisar e avaliar os riscos das vulnerabilidades técnicas detectadas;
d) comunicar-se com a ETIR (Equipe Técnica de Resposta a Incidentes de Redes Computacionais) e com as áreas da Secretaria de TI responsáveis pelos ativos, a fim de informar e obter informações acerca de vulnerabilidades existentes;
e) acompanhar a detecção e o tratamento das vulnerabilidades através de ferramenta automatizada específica e documentação produzida pelas unidades;
f) reportar à CSI a análise crítica dos resultados da gestão de vulnerabilidades e proposição de melhorias nos processos.
II. a unidade responsável pela administração do ativo deverá:
a) planejar e corrigir as vulnerabilidades técnicas encontradas ou aplicar controles para minimizar a probabilidade de exploração enquanto não for possível a correção definitiva;
b) documentar vulnerabilidades detectadas e correções aplicadas;
c) documentar justificativa para correções não aplicadas.
Art. 11. Os relatórios e registros gerados no processo de gestão de vulnerabilidades de ativos de TI devem ser tratados e armazenados de forma segura e com acesso reservado às unidades envolvidas no processo.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS
Art. 12. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.
Art. 13. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o Tribunal.
Art. 14. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 15. Esta portaria entrará em vigor na data de sua publicação.
Cuiabá, 8 de novembro de 2022.
Desembargador **CARLOS ALBERTO ALVES DA ROCHA**
Presidente do TRE-MT

PORTARIA Nº 448/2022

Estabelece cronograma de encerramento do exercício financeiro de 2022 e fixa prazo para atendimento das demandas internas de materiais.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO, usando das atribuições legais que lhe confere o artigo 19, inciso XI do Regimento Interno deste Tribunal (Resolução nº 1.152, de 7 de agosto de 2012),
CONSIDERANDO os dispositivos da Lei nº 4.320, de 17 de março de 1964, da Lei Complementar nº 101, de 04 de maio de 2000, do Decreto nº 93.872, de 23 de dezembro de 1986, e da Emenda Constitucional nº 95, de 15 de dezembro de 2016;
CONSIDERANDO os dispositivos da Instrução Normativa TSE nº 11, de 27 de julho de 2017, que dispõe sobre os procedimentos a serem adotados para a inscrição de créditos em Restos a Pagar no âmbito do Tribunal Superior Eleitoral;
CONSIDERANDO os prazos estabelecidos no Cronograma e Procedimentos de Solicitação de Liberação de Recursos e das Fases de Créditos de Despesas Obrigatórias, divulgado na Orientação SOF/TSE nº 13, atualizada em janeiro/2022;
CONSIDERANDO o que consta do Processo SEI nº 09650.2-22-3,
RESOLVE:
Art. 1º Definir o cronograma de encerramento do exercício financeiro de 2022, que deverá ser observado por todas as unidades administrativas deste Tribunal:

ITEM	DATA LIMITE	PROCEDIMENTO
1	04/11/2022	Envio à SAO, pelas áreas demandantes, de pedidos de ARP´s vigentes.
2	15/11/2022	Recolhimento das devoluções dos PIX recebidos indevidamente pelos mesários e demais convocados nas eleições 2022.
3	18/11/2022	Utilização do Cartão de Pagamento do Poder Judiciário (Suprimento de Fundos).
4	28/11/2022	Encaminhamento das prestações de contas relativas a suprimentos de fundos não atinentes as eleições 2022.
5	30/11/2022	Solicitações de ressarcimentos de despesas.
6	30/11/2022	Encaminhamento à CED/SGP de propostas de concessões de diárias e de requisições de passagens.