viii A limpeza remota dos dados corporativos de dispositivos portáteis de usuário final de propriedade da Justiça Eleitoral para dispositivos perdidos ou roubados, ou quando do desligamento do usuário das funções exercidas na Justiça Eleitoral.
ix A implementação da segmentação dos espaços de trabalho corporativos que sejam utilizados nos dispositivos móveis de usuário final, onde houver suporte, para garantir a separação das aplicações e dados corporativos das aplicações e dados pessoais.
Capítulo VII
DISPOSIÇÕES FINAIS
Art. 8º Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI).
Art. 9º A revisão desta portaria ocorrerá a cada ano ou sempre que se fizer necessário ou conveniente para o TRE-MA.
Art. 10º 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. 11 Esta portaria entra em vigor na data de sua publicação e o plano de ação para sua implementação será apresentado no prazo de 60 dias a contar dessa data.
Cientifique-se. Publique-se. Cumpra-se.
Hebert Pinheiro Leite
Diretor-Gera

## INSTRUÇÃO NORMATIVA Nº 2/2023 INSTITUI NORMA DE GERENCIAMENTO DE VULNERABILIDADES NO ÂMBITO DO TRE-MA.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a Resolução CNJ nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a Resolução TSE nº 23.644, de 01 de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a Resolução TRE-MA nº 9888/2021, de 21 de outubro de 2021, que adota, no âmbito do Tribunal Regional Eleitoral do Maranhão, as diretrizes da Política de Segurança da Informação da Justiça Eleitoral,
RESOLVE:
Capítulo I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de Gerenciamento de Vulnerabilidades, em consonância com a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).
Capítulo II
DEFINIÇÕES
Art. 2º Para efeitos desta norma consideram-se as seguintes definições:
I - 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.
II - Ameaça - causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
III - Vulnerabilidade - fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
IV - Risco - potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo para o negócio da organização;
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, homologação e cópias de segurança antes da correção da vulnerabilidade técnica ser instalada no ambiente de produção 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) isolamento e 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 VIII

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 IX

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 unidade de Segurança Cibernética 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 adequada para cada tipo de ativo;

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 TIC 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 X

DISPOSIÇÕES FINAIS

Art. 12 Os casos omissos serão resolvidos pela CSI.

Art. 13 A revisão desta portaria ocorrerá a cada ano ou sempre que se fizer necessário ou conveniente para o TRE-MA.
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 entra em vigor na data de sua publicação e sua implementação se fará no prazo de 60 dias a contar dessa data.
Cientifique-se. Publique-se. Cumpra-se.
Hebert Pinheiro Leite
Diretor-Geral

## INSTRUÇÃO NORMATIVA Nº 3/2023 DISPÕE SOBRE AS REGRAS E OS PROCEDIMENTOS PARA A REALIZAÇÃO DA GESTÃO E MONITORAMENTO DE REGISTRO DE ATIVIDADES (LOGS) NO AMBIENTE COMPUTACIONAL DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a necessidade de apoiar a gestão do processo de tratamento e resposta a incidentes em redes computacionais no TRE-MA;
CONSIDERANDO a necessidade de definir processos para o gerenciamento e o monitoramento de logs (registro de eventos) em sistemas computacionais;
CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;
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 do Maranhão;
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a Instrução Normativa para Gestão e Monitoramento de Registro de Atividades (logs).
Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Res. TSE 23.644/2021.
CAPÍTULO II
DAS DEFINIÇÕES
Art. 3º Para efeitos desta norma consideram-se os termos e definições previstos na portaria DG /TSE 444/2021, além das seguintes:
I - Serviços de DHCP (Dynamic host configuration protocol) - servidores que fornecem endereços IP e outras configurações de forma dinâmica para o ambiente de rede de computadores.