Art. 1º DESIGNAR o servidor ALMIR LOPES DA SILVA, Secretário Judiciário, para exercer o cargo comissionado de Diretor-Geral deste Tribunal, nível CJ-4, no período de 18.06.2023 a 26.06.2023, em substituição a servidora MELISSA LAVAREDA RAMOS NOGUEIRA.
ART. 2º Esta Portaria entra em vigor na data de sua publicação.
Desembargador JORGE MANOEL LOPES LINS
Presidente do TRE/AM

PORTARIA Nº 558, DE 19 DE JUNHO DE 2023

O PRESIDENTE DO EGRÉGIO TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS, no uso das competências que lhe são conferidas pelo art. 18, incisos XII, do Regimento Interno e com fundamento no art. 35, inciso I, da Lei n. 8.112, de 11.12.1990, com redação dada pela Lei n. 9.527, de 10.12.1997,
CONSIDERANDO a Res. CNJ nº 370/2021, que institui a Estratégia Nacional Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a Res. CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a portaria DG/TSE nº 444/2021, que instituiu a norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;
CONSIDERANDO as boas práticas de segurança da informação e privacidade previstas nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;
CONSIDERANDO a necessidade de gerenciar os incidentes de segurança da informação que envolvam o tratamento de dados pessoais, de acordo com a lei 13.709/2018 (LGPD);
CONSIDERANDO, ainda, que a segurança da informação, a proteção e privacidade de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral Amazonas;
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a Norma Complementar de Gerenciamento de Vulnerabilidades do Tribunal Regional Eleitoral do Amazonas.
Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021.
CAPÍTULO II
DAS DEFINIÇÕES
Art. 3º Para efeitos desta norma 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; e
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. 4º 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:
a. Adoção de ações técnicas preventivas conforme norma de Configuração Segura de Ativos de TI vigente;
b. Obtenção de informações para identificar vulnerabilidades técnicas em tempo hábil;
c. Avaliação de exposição às vulnerabilidades técnicas; e
d. Adoção de medidas apropriadas e tempestivas para lidar com os riscos identificados.
CAPÍTULO IV
DO MONITORAMENTO DE BASES DE VULNERABILIDADES
Art. 5º 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
e. Notícias relacionadas a novas tecnologias e produtos.
CAPÍTULO V
DA DESCOBERTA DE VULNERABILIDADES TÉCNICAS
Art. 6º 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. 7º 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

DA AVALIAÇÃO DA EXPOSIÇÃO

Art. 8º 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. 9º 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 DOS RESULTADOS

Art. 10º Os resultados da gestão de vulnerabilidades serão analisados criticamente segundo os seguintes controles estabelecidos:

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 ao Comitê de Segurança da Informação e Gerenciamento de Crises Cibernéticas (CSIGCC), através de relatórios estatísticos, a respeito dos resultados de detecção e tratamento das vulnerabilidades no ambiente computacional; e

V. Proposição de melhorias nos processos da gestão de vulnerabilidades para a CSIGCC.

CAPÍTULO IX

DAS RESPONSABILIDADES

Art. 11º Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas, as responsabilidades e competências no âmbito da segurança da informação devem observar os seguintes parâmetros:

I. Ao Núcleo de Segurança da Informação 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 ao CSIGCC a análise crítica dos resultados da gestão de vulnerabilidades e proposição de melhorias nos processos.

II. À 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. 12º 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 VII

DISPOSIÇÕES FINAIS

Art. 13º Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas ou pelo Comitê Gestor de Proteção e Privacidade de Dados Pessoais, quando se tratar de tema relativo ao tratamento de dados pessoais.
Art. 14º Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 15º Esta norma complementar deverá ser revisada sempre que se fizer necessário ou conveniente à este Tribunal, nunca excedendo ao período máximo de 01 (um) ano, e encaminhada para nova apreciação do Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas.
Art. 16º Esta Política deve ser publicada no portal de intranet do Tribunal pelo Comitê de Segurança da Informação.
Art. 17º Esta Portaria entra em vigor na data de sua publicação.
Publique-se e cumpra-se.
Desembargador JORGE MANOEL LOPES LINS
Presidente do TRE - AM

PORTARIA Nº 564, DE 21 DE JUNHO DE 2023

Institui o Processos de Gerenciamento de Configuração e Ativo de Serviço de TIC, no âmbito do Tribunal Regional Eleitoral do Amazonas.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a implantação, pelo Tribunal, de práticas que favorecem a governança e a gestão da Tecnologia da Informação e Comunicação (TIC);
CONSIDERANDO a importância de definição e padronização dos processos relativos ao gerenciamento de serviços de TIC, a fim de prover e manter serviços e soluções de tecnologia da informação e comunicação que viabilizem e priorizem o cumprimento da função institucional da Justiça Eleitoral;
CONSIDERANDO que os processos de Gestão de TIC devem estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as atividades consideradas estratégicas, consoante dispõe o artigo 10 da Resolução n° 211/2015 do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO que cabe a cada órgão do Poder Judiciário definir, elaborar e aplicar os processos de trabalho da área de TIC, observando as boas práticas atinentes ao tema, criando um ambiente favorável à melhoria contínua, nos termos do artigo 12, §2°, da Resolução n° 211/2015 do Conselho Nacional de Justiça;
CONSIDERANDO a Portaria CNJ n° 211/2021, que dispor sobre o Índice de Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação do Poder Judiciário (iGovTIC-JUD), para o sexênio 2021-2026, no seu Anexo III, pergunta 21 do Manual IGovTIC-JUD 2023,
RESOLVE:
Art. 1º Instituir o Processo de Gerenciamento de Configuração e Ativo de Serviço de TIC, no âmbito do Tribunal Regional Eleitoral do Amazonas (TRE/AM).
Parágrafo único. O processo tem por fundamento as seguintes referências legais e normativas:
I. "*Control Objectives for Information and related Technology* 5 - COBIT 5", modelo de gestão de Governança em TI;
II. Resolução CNJ nº 211/2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);