ATOS DA PRESIDÊNCIA

INSTRUÇÕES NORMATIVAS

INSTRUÇÃO NORMATIVA TRE-RS P N. 103/2023

Dispõe sobre a instituição da Gestão de Vulnerabilidades no âmbito do Tribunal Regional Eleitoral do Rio Grande do Sul.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de apoiar a gestão de vulnerabilidades do Tribunal Regional Eleitoral do Rio Grande do Sul;

CONSIDERANDO a Resolução CNJ n. 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução TSE n. 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a Portaria DG/TSE n. 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 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 Rio Grande do Sul,
RESOLVE:
Art. 1º Instituir a Gestão de Vulnerabilidades como norma integrante da Política de Segurança de Informação da Justiça Eleitoral adotada pelo Tribunal Regional Eleitoral do Rio Grande do Sul.
CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES
Art. 2º 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 - ativos de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;
III - CVE: acrônimo de *Common Vulnerabilities and Exposures*, é um dicionário de vulnerabilidades com nomes padronizados para vulnerabilidades e outras informações de exposições de segurança;
IV - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
V - SCAP: acrônimo de *Security Content Automation Protocol*, é uma especificação estabelecida pelo NIST (*National Institute of Standards and Technology*) para expressar e manipular dados de segurança de forma padronizada;
VI - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
VII - vulnerabilidade de dia zero: falha na segurança de um software que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma Vulnerabilidade de Dia Zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um *patch* de segurança para essa falha, ela pode ser explorada por *hackers* em Explorações de Dia Zero. A correção de uma vulnerabilidade de dia zero geralmente é tarefa do fabricante do software, que precisará lançar um pacote de segurança para consertar a falha.
CAPÍTULO II
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 identificação, classificação e tratamento:
I - obtenção de informações para identificar vulnerabilidades técnicas em tempo hábil;
II - avaliação de exposição às vulnerabilidades técnicas;
III - adoção de medidas apropriadas e tempestivas para lidar com os riscos identificados.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 4° Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas, ficam definidas as seguintes responsabilidades e competências:

I - cabe à Assessoria de Segurança Cibernética:

a) manter monitoramento regular de sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção dos ativos em uso na infraestrutura do Tribunal;

b) acionar regularmente ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas na rede corporativa;

c) analisar e avaliar os riscos das vulnerabilidades técnicas detectadas;

d) acompanhar o tratamento das vulnerabilidades;

e) documentar as vulnerabilidades detectadas e as correções aplicadas;

f) documentar as justificativas para as correções não aplicadas;

g) realizar a análise crítica dos resultados da gestão de vulnerabilidades e propor melhorias nos processos;

h) reportar os resultados e propor melhorias ao Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSI).

II - cabe à unidade responsável pela gestão do ativo:

a) manter monitoramento regular de sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, para obter informações relacionadas às vulnerabilidades técnicas e medidas de correção dos ativos sob sua responsabilidade;

b) corrigir as vulnerabilidades técnicas ou aplicar controles para minimizar a probabilidade de exploração;

c) relatar à Assessoria de Segurança Cibernética as justificativas para as correções não aplicadas.

Art. 5° Os relatórios e registros gerados no processo de gestão de vulnerabilidades de ativos de processamento devem ser tratados e armazenados de forma segura, com acesso reservado às unidades envolvidas no processo.

CAPÍTULO IV
DO MONITORAMENTO DE BASES DE VULNERABILIDADES

Art. 6° A obtenção de informações relacionadas a vulnerabilidades técnicas e medidas de correção deverá ser feita através do monitoramento regular previsto no art. 4°, I, a e II, a, considerando os seguintes controles mínimos:

I - as fontes de consulta devem ser definidas pelos seguintes critérios:

a) qualidade das informações: verificar se as informações fornecidas pela fonte são precisas e atualizadas;

b) disponibilidade das informações: verificar a frequência de atualização das informações fornecidas pela fonte, dando preferência àquela com maior frequência;

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 - a obtenção de informações sobre vulnerabilidades técnicas e medidas de correção deve incluir:

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.

CAPÍTULO V

DA DESCOBERTA DE VULNERABILIDADES TÉCNICAS

Art. 7° A identificação de vulnerabilidades técnicas na rede corporativa deverá ser feita através de ferramentas automatizadas e rotinas de varreduras, considerando os seguintes controles mínimos:
I - emprego de ferramentas automatizadas de varredura e identificação de vulnerabilidades que possuam, no mínimo, as seguintes características:
a) utilização da fonte CVE como base para a verificação de vulnerabilidades nos ativos de processamento;
b) compatibilidade com SCAP ou outro protocolo de automatização da verificação de configurações de segurança.
II - deve ser assegurado que somente varreduras de vulnerabilidades autorizadas na lista de permissões (*whitelist*) possam ser executadas, local ou remotamente, e configuradas com direitos elevados nos ativos de processamento que estão sendo testados.

CAPÍTULO VI

DA AVALIAÇÃO DA EXPOSIÇÃO

Art. 8° Para analisar e avaliar os riscos de vulnerabilidades técnicas afetarem o ambiente da rede corporativa, os seguintes controles mínimos devem ser aplicados:
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 - avaliação quanto à necessidade de criar documentação de procedimentos para correção da vulnerabilidade técnica, contemplando 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 ao CSI sobre a impossibilidade de tratamento de vulnerabilidade técnica classificada como crítica.

CAPÍTULO VII

DO TRATAMENTO DE VULNERABILIDADES TÉCNICAS

Art. 9° A correção das vulnerabilidades técnicas e as ações para minimizar a probabilidade de exploração deverão considerar os seguintes controles mínimos:
I - adoção de testes e homologação da correção da vulnerabilidade técnica antes da sua instalação no ambiente da rede corporativa, considerando a viabilidade técnica e financeira;
II - execução dos procedimentos para correção da vulnerabilidade técnica, contemplando instalação, configuração, regras estabelecidas e procedimentos de restauração;

III - geração de registros de eventos (logs) das ações realizadas para correção das vulnerabilidades técnicas críticas, identificados de forma distinta.

Art. 10. Na impossibilidade de correção da vulnerabilidade, no prazo de 30 (trinta) dias, 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;

c) aumento da conscientização sobre a vulnerabilidade;

d) implementação de controles de segurança compensatórios.

Art. 11. As mudanças no ambiente da rede corporativa, motivadas pelas correções das vulnerabilidades técnicas, devem ser implantadas de acordo com o processo de Gerenciamento de Mudanças e Liberações vigente.

CAPÍTULO VIII

DA AVALIAÇÃO DE RESULTADOS

Art. 12. A análise crítica dos resultados da gestão de vulnerabilidades deverá considerar os seguintes controles:

I - comparação regular dos resultados dos tratamentos de vulnerabilidades técnicas consecutivas para verificar se foram corrigidas;

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 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 o CSI.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art.13. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvido o CSI.

Art.14. O descumprimento desta norma deve ser imediatamente registrado como incidente de segurança e comunicado ao CSI para apuração e consequente adoção das providências cabíveis.

Art.15. Esta Instrução Normativa entra em vigor na data de sua publicação.

DESEMBARGADOR FRANCISCO JOSÉ MOESCH,

PRESIDENTE.

PORTARIAS

PORTARIA TRE-RS P N. 1709, DE 19 DE ABRIL DE 2023.

INSTITUI O GRUPO DE PESQUISAS JUDICIÁRIAS (GPJ) NO ÂMBITO DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DO RIO GRANDE DO SUL E DÁ OUTRAS PROVIDÊNCIAS.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DO RIO GRANDE DO SUL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução CNJ nº 462/2022, que dispõe sobre a gestão de dados e estatística, cria a Rede de Pesquisas Judiciárias (RPJ) e os Grupos de Pesquisas Judiciárias (GPJ) no âmbito do Poder Judiciário e dá outras providências;

CONSIDERANDO a Resolução CNJ nº 76/2009, que dispõe sobre os princípios do Sistema de Estatística do Poder Judiciário, estabelece indicadores, fixa prazos, determina penalidades e dá outras providências;