Tribunal Regional Eleitoral - RJ
Diretoria Geral
Secretaria de Administração
Coordenadoria de Gestão Documental, Informação e Memória

INSTRUÇÃO NORMATIVA DG TRE-RJ Nº 02, DE 16 DE JANEIRO DE 2023.

Dispõe sobre a gestão de vulnerabilidades em sistemas de informação no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das suas atribuições regulamentares,

CONSIDERANDO a **Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) (https://atos.cnj.jus.br/atos/detalhar/3975)**;

CONSIDERANDO a **Resolução TSE nº 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e 27002;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a **Lei 13.709, de 14 de agosto de 2018 (LGPD) (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)**;

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 de Janeiro; e

CONSIDERANDO, ainda, o disposto no processo SEI n.º 2022.0.000055701-4,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a norma de Gestão de Vulnerabilidades no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela **Res. TSE 23.644/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**.

Art. 3º Para os efeitos desta norma, aplicam-se os termos e definições conceituados na **Portaria TSE nº 444, de 8 de julho de 2021 (https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-444-de-08-de-julho-de-2021)**.

CAPÍTULO II

DOS OBJETIVOS

Art. 4° A gestão de vulnerabilidades tem como objetivo prevenir a exploração de vulnerabilidades técnicas na rede corporativa, por meio da aplicação sistemática das seguintes ações:

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

II - avaliação de exposição às vulnerabilidades técnicas identificadas;

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

CAPÍTULO III

DA IDENTIFICAÇÃO DE VULNERABILIDADES TÉCNICAS

Art. 5º Informações sobre vulnerabilidades tecnicas relacionadas aos ativos de processamento em uso na rede corporativa devem ser pesquisadas periodicamente por meio das seguintes ações:

I - monitoramento de vulnerabilidades tecnicas;

II - procedimento interno de verificação de existência de vulnerabilidades tecnicas.

CAPÍTULO IV

DO MONITORAMENTO DE BASES DE VULNERABILIDADES

Art. 6º O monitoramento de vulnerabilidades técnicas deve ser realizado diariamente através de pesquisas em sítios de fabricantes, fóruns especializados, listas de e-mails, grupos especiais e outras fontes de consulta consideradas relevantes.

Art. 7º As fontes de consulta devem ser definidas segundo critérios de:

I - qualidade das informações - informações precisas e atualizadas;

II - disponibilidade das informações - frequência de atualização das informações;

III - legitimidade da fonte - verificar se a fonte é representante autorizada do responsável pela informação ou reconhecida como confiável pela comunidade de segurança da informação.

Art. 8º As pesquisas devem abranger, dentre outras:

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

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

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

IV - dados sobre segurança da informação de consultorias especializadas, empresas desenvolvedoras de soluções de segurança, polícia, agências de segurança do governo ou congêneres;

V - notícias relacionadas a novas tecnologias e produtos.

CAPÍTULO V

DA DESCOBERTA DE VULNERABILIDADES TÉCNICAS

Art. 9º Devem ser realizadas varreduras e testes periódicos, de forma automatizada, em todos os ativos de processamento conectados à rede do TRE-RJ, a fim de identificar vulnerabilidades técnicas observando-se os seguintes requisitos:

I - empregar pelo menos uma ferramenta atualizada de varredura de vulnerabilidades, compatível com SCAP, de acordo com a disponibilidade de recursos e a necessidade;

II - assegurar o planejamento prévio das varreduras e testes, juntamente com as equipes responsáveis pelos ativos envolvidos, contemplando o escopo da análise e a definição de procedimentos de contingência;

III - 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;

IV - 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.

Art. 10. As varreduras devem ser realizadas a cada três meses ou com frequência maior para os ativos corporativos internos e mensalmente ou com frequência maior para os ativos corporativos expostos externamente, bem como sob demanda, mediante notificação prévia dos envolvidos, em datas previamente acordadas com estes.

CAPÍTULO VI

DA AVALIAÇÃO DA EXPOSIÇÃO

Art. 11. As vulnerabilidades técnicas encontradas devem ser inicialmente avaliadas quanto a:

I - pertinência - verificar se a vulnerabilidade atinge de fato algum ativo da instituição;

II - aplicabilidade - verificar se a vulnerabilidade existe de fato no ambiente computacional da instituição, considerando, dentre outros: configurações específicas do ativo, versões de sistemas, presença ou não de recursos relacionados à vulnerabilidade.

Art. 12. As vulnerabilidades técnicas identificadas como potenciais devem ser classificadas conforme os riscos a elas associados: facilidade de exploração, impacto dos danos potenciais, criticidade do ativo afetado para as atividades do órgão, dentre outros.

Art. 13. Cada nível de criticidade definido para a classificação das vulnerabilidades técnicas deve prever um prazo de resposta acerca dos procedimentos adotados para tratamento da respectiva vulnerabilidade.

Art. 14. O Núcleo de Defesa Cibernética deve notificar as unidades responsáveis pelos ativos onde as vulnerabilidades potenciais foram encontradas.

CAPÍTULO VII

DO TRATAMENTO DE VULNERABILIDADES TÉCNICAS

Art. 15. As unidades notificadas acerca de vulnerabilidades existentes nos ativos sob sua responsabilidade devem identificar a melhor forma de tratar os problemas reportados e atuar para corrigir as vulnerabilidades ou para minimizar a probabilidade de sua exploração.

Art. 16. Todos os procedimentos adotados para tratamento das vulnerabilidades devem ser registrados.

Art. 17. A impossibilidade de tratamento de uma vulnerabilidade deve ser registrada e comunicada à Assessoria de Segurança da Informação e à Comissão de Segurança da Informação.

Art. 18. Finalizado o tratamento das vulnerabilidades, as correções aplicadas devem ser validadas e a mitigação dos riscos, confirmada.

CAPÍTULO VIII

DAS RESPONSABILIDADES

Art. 19. Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas, as responsabilidades e competências no âmbito da segurança da informação devem ser segregadas, observados os seguintes parâmetros:

I - o Núcleo de Defesa Cibernética e a unidade responsável pela administração do ativo de processamento devem 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;

II - o Núcleo de Defesa Cibernética é responsável por:

a) monitorar, identificar, avaliar, classificar e registrar as vulnerabilidades técnicas;

b) notificar a unidade responsável pelo tratamento da vulnerabilidade, quando for o caso;

c) acompanhar o tratamento das vulnerabilidades técnicas e apoiar as unidades responsáveis pelo seu tratamento;

d) gerar relatórios e estatísticas para acompanhamento pelas equipes técnicas envolvidas, pela alta gestão ou pelos órgãos de controle;

e) propor, monitorar e avaliar regularmente o processo de gestão de vulnerabilidades técnicas.

III - a unidade responsável pela administração do ativo de processamento é responsável por investigar e tratar as vulnerabilidades reportadas pelo Núcleo de Defesa Cibernética, executando ações de contenção, correção e resposta ou aplicando controles para minimizar a probabilidade de sua exploração.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 20. 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.

Art. 21. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida, se necessário, a Comissão de Segurança da Informação.

Art. 22. Esta norma deve ser revisada a cada 3 (três) anos, ou antes, se necessário, pela Assessoria de Segurança da Informação com participação da Secretaria de Tecnologia da Informação e posterior encaminhamento para apreciação pela Comissão de Segurança da Informação.

Art. 23. Esta norma entra em vigor na data de sua publicação e sua implementação se fará no prazo de um ano a contar dessa data.

ELINE IRIS RABELLO GARCIA DA SILVA
Diretor(a)-Geral

Este texto não substitui o publicado no **DJE TRE-RJ nº 16, de 18/01/2023, p. 3 (https://dje.tse.jus.br/dje/pdf/v1/edicao/101548#page=3)**