ATOS DA PRESIDÊNCIA

INSTRUÇÕES NORMATIVAS

INSTRUÇÃO NORMATIVA Nº 61, DE 19 DE NOVEMBRO DE 2021

Regulamenta o Processo de Gestão de Vulnerabilidades em sistemas de informação no âmbito do Tribunal Regional Eleitoral de Pernambuco (TRE-PE).

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais,

CONSIDERANDO a Lei nº 13.709, de 14/8/2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral (TSE), que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral; e

CONSIDERANDO a Instrução Normativa nº 15, de 30 de março de 2017, deste Tribunal, que estabelece normas gerais para garantir o gerenciamento das operações e comunicações dos recursos de processamento da informação da Justiça Eleitoral de Pernambuco,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Instrução Normativa regulamenta o Processo de Gestão de Vulnerabilidades em sistemas de informação no âmbito do Tribunal Regional Eleitoral de Pernambuco (TRE-PE).

Parágrafo único. As diretrizes para a identificação, análise e tratamento das vulnerabilidades em sistemas de informação do TRE-PE estão estabelecidas nesta norma.

Art. 2º Para efeito desta Instrução Normativa consideram-se:

I - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou para o Tribunal;

II - ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pelo TRE-PE;

III - internet of things (IOT): a internet das coisas, que se refere a grupos de dispositivos digitais que coletam e/ou transmitem dados pela internet;

IV - risco: probabilidade de uma fonte de ameaça explorar uma vulnerabilidade de um sistema de informação; e

V - vulnerabilidade: fragilidade ou falha de um ativo, grupo de ativos ou dispositivos digitais, que pode ser explorada por uma ou mais ameaças.

Art. 3º Compete à Seção da Segurança da Informação (SESIN) acompanhar, controlar e aperfeiçoar o processo de gestão de vulnerabilidades em sistemas de informação, visando a minimizar a sua ocorrência e a proteger as informações pessoais e/ou sensíveis.

CAPÍTULO II

DOS PROCEDIMENTOS PREVENTIVOS

Art. 4º Os procedimentos preventivos observarão as seguintes diretrizes:

I - manter atualizados os seguintes ativos de tecnologia da informação e comunicação (TIC):

a) sistemas operacionais e aplicativos instalados em estações de trabalho e notebooks;

b) sistemas operacionais de equipamentos servidores físicos ou virtuais;

c) servidores de aplicação (middleware);
d) sistemas de gestão de banco de dados;
e) infraestrutura de virtualização;
f) sistemas de comunicação de TIC;
g) sistemas e aplicações Web*;*
h) sistemas de IOT;
i) ativos de videomonitoramento; e
j) sistemas operacionais e aplicativos instalados em aparelhos celulares, tablets ou outros dispositivos móveis institucionais; e
II - testar novos sistemas de informação quanto à existência de vulnerabilidades antes de sua entrada em produção.
§ 1º Os procedimentos indicados nos incisos I e II deste artigo serão executados conforme a competência descrita a seguir:
a) procedimentos contidos nas alíneas "a", "b", "c", "d", "e" e "f" do inciso I - pelas unidades da Coordenadoria de Infraestrutura (COINF), da STIC, conforme suas competências regulamentares;
b) procedimentos contidos nas alíneas "g" e "h" do inciso I, e no inciso II - pelas unidades da Coordenadoria de Sistemas (COSIS) e da Coordenadoria de Serviços (COSERV), ambas da STIC, conforme suas competências regulamentares;
c) procedimento contido na alínea "i" do inciso I - pela Assessoria de Segurança (ASSEG); e
d) procedimento contido na alínea "j" do inciso I - pelos(as) usuários(as) autorizados(as) a utilizar aparelhos celulares, tablets ou outros dispositivos móveis institucionais.
§ 2º Toda atualização dos sistemas de informação utilizados pelo TRE-PE deverá ser precedida de análise de compatibilidade e, se aplicável, de testes em ambiente de homologação com o intuito de garantir a disponibilidade e integridade dos sistemas e minimizar o risco de incompatibilidades que possam produzir incidentes no ambiente de TIC.
§ 3º Quando não for possível realizar quaisquer dos procedimentos preventivos estabelecidos neste artigo, a unidade técnica competente indicada no § 1º comunicará, justificadamente, à SESIN, para análise e elaboração de relatório quanto aos riscos envolvidos.
§ 4º O relatório produzido pela SESIN será submetido à apreciação e deliberação do Comitê Executivo de Tecnologia da Informação e Comunicação (CETIC).
Art. 5º Para novos sistemas de informação desenvolvidos integralmente no TRE-PE, a gestão de vulnerabilidades e a proteção a dados pessoais deverão ser consideradas como prioritárias, desde a fase de concepção até a fase de execução.
Art. 6º Deverão ser realizadas varreduras e testes de segurança periódicos em todos os ativos de informação conectados à rede do TRE-PE em busca de vulnerabilidades.
Parágrafo único. A varredura prevista no caput deste artigo poderá ser de dois tipos:
I - ampla: composta por testes para diversas vulnerabilidades de aplicativos, sistemas operacionais e redes; e
II - restrita: composta por testes de vulnerabilidades específicos em ambiente limitado.
Art. 7º As atividades de varreduras e os testes de segurança poderão ser realizados de forma automatizada e rotineira ou sob demanda, de acordo com a necessidade e a disponibilidade de recursos.
§ 1º As diretrizes para as varreduras automatizadas serão definidas pela SESIN, com o apoio das unidades da Coordenadoria de Infraestrutura, conforme suas competências regulamentares.
§ 2º As rotinas automatizadas serão executadas pelas unidades da COINF, conforme suas competências regulamentares, devendo os relatórios produzidos serem enviados à SESIN para análise e providências, se for o caso.

§ 3º As varreduras sob demanda poderão ser realizadas por iniciativa da SESIN, das unidades da COINF ou de outras unidades, devendo, neste último caso, serem precedidas de autorização do(a) titular da Secretaria de Tecnologia da Informação e Comunicação (STIC).

§ 4º As varreduras e os testes de segurança serão inicialmente aplicados aos ativos definidos como essenciais pelo Comitê de Gestão Estratégica (COGEST), devendo serem ampliados para os demais ativos, de acordo com a disponibilidade de recursos ou quando houver uma demanda específica.

CAPÍTULO III

DOS PROCEDIMENTOS CORRETIVOS

Art. 8º As vulnerabilidades identificadas serão analisadas e classificadas quanto ao seu risco, conforme diretrizes estabelecidas na Resolução nº 277, de 12 de dezembro de 2016, deste Tribunal, e de acordo com as orientações a seguir:

I - de impacto: considerar o potencial de dano, a facilidade de exploração por uma ameaça, a importância do ativo para a atividade do TRE-PE e o nível de privacidade e sigilo das informações acessadas pelo ativo;

II - de probabilidade: considerar a possibilidade de concretização da ameaça; e

III - de significância: considerar o resultado da multiplicação da probabilidade pelo impacto.

Art. 9º A matriz de risco das vulnerabilidades identificadas deverá ser elaborada pela SESIN, que demandará, quando necessário, o apoio de outras unidades visando ao correto e adequado enquadramento do impacto e/ou probabilidade.

Parágrafo único. A matriz de risco será elaborada com base nas Tabelas 1, 2 e 3, constantes do Anexo desta Instrução Normativa.

Art. 10. A matriz de risco das vulnerabilidades identificadas deverá ser apresentada pelo(a) Coordenador(a) de Governança, Gestão e Segurança da Informação (COGGI) ao(à) Secretário(a) de TIC, que deliberará e coordenará, com as unidades envolvidas, a adoção das providências necessárias, de acordo com a seguinte classificação das vulnerabilidades:

I - vulnerabilidades classificadas como "altas": deverão ser adotadas, de imediato, medidas para mitigar e/ou corrigir a falha;

II - vulnerabilidades classificadas como "médias": deverão ser programadas medidas para mitigar e /ou corrigir a falha; e

III - vulnerabilidades classificadas como "baixas": serão aceitas e monitoradas, podendo ter sua classificação quanto ao risco alterada, caso haja mudança de cenário.

§ 1º Caberá à SESIN realizar o monitoramento dos procedimentos corretivos aprovados, reportando ao(à) Coordenador(a) da COGGI eventual descumprimento, visando às gestões necessárias junto à unidade responsável.

§ 2º A conclusão dos procedimentos corretivos deverá ser comunicada ao(à) Coordenador(a) da COGGI pela SESIN.

Art. 11. Caso a vulnerabilidade identificada envolva um ativo de informação desenvolvido ou mantido por outro órgão público, este deverá ser comunicado.

Parágrafo único. A comunicação prevista no caput deste artigo será realizada pelo gabinete da STIC de acordo com as informações apresentadas pela COGGI.

Art. 12. Deverá ser elaborado, pela SESIN, relatório contendo as vulnerabilidades identificadas, a matriz de risco e as providências adotadas, o qual será encaminhado quadrimestralmente ao Comitê de Governança e Segurança da Informação (CGSI), ao(à) Secretário(a) de TIC e ao(à) Gestor(a) de Segurança da Informação.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 13. A SESIN deverá elaborar o mapa do processo de gestão de vulnerabilidades dos sistemas de informação definidos como essenciais em até 60 (sessenta) dias, a partir da publicação desta norma.
Art. 14. Os casos omissos e eventuais dúvidas quanto à aplicação desta Instrução Normativa serão dirimidos pelo CETIC, ouvido o Comitê de Governança e Segurança da Informação, quando necessário.
Art. 15. Esta Instrução Normativa entra em vigor na data de sua publicação.
Recife, 19 de novembro de 2021.
CARLOS FREDERICO GONÇALVES DE MORAES
Presidente
Anexo-IN-61-2021-gestão-vulnerabilidades.pdf

SECRETARIA DE GESTÃO DE PESSOAS

PORTARIAS

PORTARIA Nº 793/2021

O SECRETÁRIO DE GESTÃO DE PESSOAS DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais conferidas pela Portaria n.º 398, de 07.06.2021, e considerando o disposto no Processo SEI nº 0021740-58.2021.6.17.8000,
RESOLVE
interromper, a contar de 04.11.2021, com fundamento no art. 80 da Lei n.º 8.112/90, a primeira parcela de férias de 2021 de EUDA CRYSTHINA FERREIRA DE CASTRO, tendo em vista a necessidade do serviço.
Recife, 09 de novembro de 2021.
ANTÔNIO JOSÉ DO NASCIMENTO
SECRETÁRIO

PORTARIA Nº 789/2021

O SECRETÁRIO DE GESTÃO DE PESSOAS DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais conferidas pela Portaria n.º 398, de 07.06.2021, e considerando o disposto no Processo SEI nº 0021608-53.2021.6.17.8500,
RESOLVE
interromper, a contar de 04.11.2021, com fundamento no art. 80 da Lei n.º 8.112/90, a terceira parcela de férias de 2021 de FLÁVIA SIMONE DA SILVA, tendo em vista a necessidade do serviço.
Recife, 05 de novembro de 2021.
ANTÔNIO JOSÉ DO NASCIMENTO
SECRETÁRIO

PORTARIA Nº 775/2021

O SECRETÁRIO DE GESTÃO DE PESSOAS DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais conferidas pela Portaria n.º 398, de 07.06.2021, e considerando o disposto no Processo SEI nº 0002096-32.2021.6.17.8000,
RESOLVE
interromper, a contar de 28.01.2021, com fundamento no art. 80 da Lei n.º 8.112/90, a terceira parcela de férias de 2020 de MICHELLE MANZI CASTELO BRANCO tendo em vista a necessidade do serviço.
Recife, 25 de outubro de 2021.
ANTÔNIO JOSÉ DO NASCIMENTO