18.	13/12/2021	Encaminhamento a CEOFI da folha de pagamento de dezembro/2021 e demais folhas suplementares.
19.	16/12/2021	Publicaça o de termo aditivo de prorrogaça o dos contratos cuja vige ncia encerrara entre 19/12 e 31/12/2019.
20.	16/12/2021	Reclassificaça o da despesa orçamenta ria (CEOFI e COMAP) relativa a suprimento de fundos e baixa da respectiva responsabilidade.
21.	16/12/2021	Ajustes dos saldos dos empenhos a liquidar (reforço/anulaça o).
22.	16/12/2021	Anulaça o dos saldos remanescentes de empenhos referentes a despesas com dia rias, ajuda de custo e suprimento de fundos.
23.	16/12/2021	Providenciar o cancelamento de restos a pagar inscritos ou reinscritos que na o sa o devidos.
24.	16/12/2021	Devoluça o ao respectivo o rga o repassador dos saldos orçamenta rios e financeiros na o utilizados, recebidos por descentralizaça o de cre dito.
25.	16/12/2021	Emissa o de ordem de pagamento, de GRU e Documento de Arrecadaça o de tributos e contribuiço es (DARF, DAR e GPS).
26.	16/12/2021	Assinatura das Ordens de Pagamento pelo Ordenador de Despesas e pelo Gestor Financeiro.
27.	16/12/2021	Registrar no SIAFI os contratos celebrados pelo TSE no referido exercício.
28.	16/12/2021	Regularizaça o de contas conta beis (impactadas pela execução orçamentária e financeira).
29.	17/12/2021	Conformidade de Registros de Gesta o.
30.	17/12/2021	Indicaça o pelo Ordenador de Despesa ou por quem estiver delegado formalmente no SIAFI, na tabela de UG, dos empenhos a serem inscritos em restos a pagar na o processados a liquidar e em liquidaça o.

PORTARIA TSE Nº 460 DE 13 DE JULHO DE 2021.

Institui norma de gerenciamento de vulnerabilidades, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, 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), e a Resolução-TSE nº 23.501, de 19 de dezembro de 2016, que institui a Política de Segurança da Informação (PSI) no âmbito 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 do Tribunal Superior Eleitoral (TSE).

Art. 2º Para os efeitos da Política de Segurança da Informação do TSE, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 8 de julho de 2021.

Capítulo II

DOS OBJETIVOS E RESPONSABILIDADES

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.

Art. 4º 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 - Equipe de Gestão da Segurança de Tecnologia da Informação (TI) e unidade responsável pela administração do ativo de processamento - responsáveis pelo 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;

II - Seção de Sistemas Operacionais - responsável pelo acionamento regular de ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas na rede corporativa;

III - Equipe de Gestão da Segurança de TI - responsável pela análise e avaliação dos riscos das vulnerabilidades técnicas no ambiente da rede corporativa;

IV - Equipe de Gestão da Segurança de TI - responsável pelo acompanhamento do tratamento das vulnerabilidades;

V - unidade responsável pela administração do ativo de processamento - responsável pela correção das vulnerabilidades técnicas ou aplicação de controles para minimizar a probabilidade de exploração;

VI - Equipe de Gestão da Segurança de TI - responsável pela análise crítica dos resultados da gestão de vulnerabilidades e proposição de melhorias nos processos.

Art. 5º 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 III

DA IDENTIFICAÇÃO DE VULNERABILIDADES TÉCNICAS

Art. 6º Informações sobre vulnerabilidades técnicas relacionadas com ativos de processamento em uso na rede corporativa devem ser pesquisadas periodicamente para dirimir os riscos associados, por meio da implantação de medidas de segurança apropriadas, considerando, no mínimo, as seguintes:

I - monitoramento de vulnerabilidades técnicas utilizando as fontes relacionadas em procedimento especifico, a ser definido pela área responsável em conjunto com a Equipe de Gestão da Segurança de TI;

II - verificação de vulnerabilidades técnicas, mediante:

a) utilização de procedimento específico, a ser definido pela área responsável em conjunto com a Equipe de Gestão da Segurança de TI;

b) teste de invasão, teste de quebra de senhas, teste de quebra de cifração, teste com técnicas de invasão/defesa, entre outros;

c) contratação de serviço externo para tentativa contínua de detecção de falhas de segurança na rede corporativa.

Seção I

MONITORAMENTO DE VULNERABILIDADES TÉCNICAS

Art. 7º 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.

Seção II

VERIFICAÇÃO DE VULNERABILIDADES TÉCNICAS

Art. 8º 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 todos os ativos de processamento e identificar todas as 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;

c) disponibilidade de:

1. console de administração centralizada com possibilidade de instalação remota;
2. atualização automática e programável;
3. configuração de perfis de acesso;
4. bloqueio de alteração das configurações por meio de senha;
5. serviço de suporte do fabricante no idioma português;
6. serviço de atualização do fabricante;
7. mecanismo de varredura em tempo real;
8. mecanismo de controle estatístico e emissão de relatórios.

II - assegurar 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;

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 IV

DA AVALIAÇÃO DA EXPOSIÇÃO

Art. 9º 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 processo de classificação de risco para priorizar a correção da vulnerabilidade técnica, conforme procedimento definido pela Equipe de Gestão da Segurança de TI;

VI - comunicação imediata à Comissão Técnica de Tecnologia da Informação (CTTI) de impossibilidade de tratamento de vulnerabilidade técnica classificada como crítica;

VII - geração de registro do incidente.

Capítulo V

DO TRATAMENTO DE VULNERABILIDADES TÉCNICAS

Art. 10. Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para corrigir as vulnerabilidades técnicas ou minimizar a probabilidade de exploração:

I - observância do Processo de Tratamento e Resposta a Incidentes em Redes de Computadores;

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.

Art. 11. 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.

Art. 12. 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 à Comissão de Segurança da Informação (CSI) a respeito da evolução, dos riscos e dos achados dos testes e das varreduras;
V - proposição de melhorias nos processos da gestão de vulnerabilidades para a CSI.
Capítulo VI
DISPOSIÇÕES FINAIS
Art. 13. Os casos omissos serão resolvidos pela CSI.
Art. 14. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TSE.
Art. 16. 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. 17. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data.
RUI MOREIRA DE OLIVEIRA
Documento assinado eletronicamente em 20/07/2021, às 14:34, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1706383&crc=69D9C719, informando, caso não preenchido, o código verificador 1706383 e o código CRC 69D9C719.
2020.00.000004513-0

PORTARIA TSE Nº 457 DE 13 DE JULHO DE 2021.

Institui norma de gerenciamento de *backup* e restauração de dados relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, 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), e a Resolução-TSE nº 23.501, de 19 de dezembro de 2016, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral,
RESOLVE:
Capítulo I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de gerenciamento de *backup* e restauração de dados, em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral (TSE).
Art. 2º Para os efeitos da Política de Segurança da Informação do TSE, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 8 de julho de 2021.
Capítulo II
DO PLANEJAMENTO DA CÓPIA DE SEGURANÇA (*BACKUP*)
Art. 3º As informações do TSE, incluindo dados pessoais, biográficos, biométricos e corporativos, devem ser protegidas por meio de rotinas sistemáticas de cópia de segurança.
Art. 4º A unidade responsável pelo gerenciamento de cópia de segurança, juntamente com os respectivos proprietários dos ativos de informação, deve definir os prazos de realização, retenção e descarte das informações armazenadas na cópia de segurança, respeitando os níveis de classificação atribuídos, de acordo com a necessidade de cada serviço e com as leis que os regulamentem.