PORTARIA DG Nº 441/2026

PUBLICAÇÃO EM : 04/09/2026

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, usando das atribuições que lhe são conferidas pelo artigo 35, inciso VIII do Regulamento da Secretaria deste Tribunal e considerando o contido no SEI nº 0016196-43.2026.6.16.8000,
RESOLVE
Art. 1º LOTAR o servidor MARCOS ARMENIO MILITÃO, ocupante do cargo de Técnico Judiciário - Apoio Especializado - Polícia Judicial, do Quadro de Pessoal deste Tribunal, no Gabinete da Presidência.
Art. 2º Esta Portaria entra em vigor na data de sua publicação, com efeitos a partir de 01/09/2026.
Curitiba, 02 de setembro de 2026.
VALCIR MOMBACH
Diretor- Geral

PORTARIA DG Nº 442/2026

PUBLICAÇÃO EM : 04/09/2026

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, usando das atribuições que lhe são conferidas pelo artigo 35, inciso VIII do Regulamento da Secretaria deste Tribunal e considerando o contido no SEI nº 0016129-78.2026.6.16.8000,
RESOLVE
Art. 1º LOTAR a servidora VIVIAN WOLFF DE LIZ, ocupante do cargo de Técnico Judiciário Área Administrativa, do Quadro de Pessoal deste Tribunal, na Seção de Logística de Eleições - SLE .
Art. 2º Esta Portaria entra em vigor na data de sua publicação, com efeitos a partir de 01/09/2026.
Curitiba, 02 de setembro de 2026.
VALCIR MOMBACH
Diretor Geral

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

NORMA TÉCNICA

NORMA TÉCNICA Nº 06, DE 28 DE AGOSTO DE 2026

PUBLICAÇÃO EM : 04/09/2026

Estabelece os procedimentos e as responsabilidades para a realização de Testes de Penetração (Pentest) no âmbito da Justiça Eleitoral do Paraná.
O SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO, no uso de suas atribuições legais e regimentais;
CONSIDERANDO a necessidade de definir processos para a realização de testes de penetração como ferramenta de validação da eficácia dos controles de segurança;
CONSIDERANDO a Resolução CNJ nº 396, de 07/06/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução TSE n° 23.763, de 9/06/2026, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-PR nº 974, de 15 de abril de 2026, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral do Paraná;
CONSIDERANDO as boas práticas em gestão de riscos e segurança da informação previstas nas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8, especialmente o Controle 18 (*Penetration Testing*);
CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a Lei nº 13.709, de 14/08/2018 (LGPD);
CONSIDERANDO a necessidade de integrar a realização de Testes de Penetração ao processo de Gestão de Riscos e Gestão de Vulnerabilidades do Tribunal;
CONSIDERANDO o contido no Processo SEI nº 0013648-45.2026.6.16.8000;
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º A presente Norma Técnica estabelece os procedimentos e define as responsabilidades para a solicitação, autorização, execução e gestão dos resultados dos Testes de Penetração (Pentest) realizados no âmbito da Justiça Eleitoral do Paraná.
Art. 2º Esta norma observa a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.763/2026 e Resolução 974/2026 que instituiu a Política de Segurança da Informação, no âmbito da Justiça Eleitoral do Paraná, e complementa os protocolos instituídos pela Portaria CNJ nº 162/2021, em especial o ANEXO V, que dispõe sobre as *Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e /ou criação de rotina de auditorias cruzadas.*
CAPÍTULO II
DAS DEFINIÇÕES E OBJETIVOS
Art. 3º Para efeitos desta norma consideram-se os termos e definições previstos na Portaria DG /TSE nº 444/2021, acrescidos de:
I - Teste de Penetração (Pentest): Processo controlado e autorizado que simula ataques cibernéticos contra ativos de tecnologia da informação para identificar e explorar vulnerabilidades, avaliando a eficácia dos controles de segurança.
II - Regras de Engajamento (RoE): Documento que define os limites, técnicas permitidas e proibidas, janelas de teste, escopo e canais de comunicação para um Teste de Penetração.
III - Gestor do Ativo: Servidor ou unidade responsável por um sistema, informação ou componente de infraestrutura (o "proprietário" do ativo).
Art. 4º Os Testes de Penetração têm por objetivo:
I - Identificar e validar vulnerabilidades técnicas em infraestrutura, sistemas e aplicações;
II - Avaliar o impacto potencial de uma exploração bem-sucedida de vulnerabilidades;
III - Testar a eficácia dos controles de segurança (preventivos, detectivos e de resposta);
IV - Fornecer subsídios para o processo de Gestão de Riscos e de Vulnerabilidades;
V - Assegurar a conformidade com requisitos legais e regulatórios.
CAPÍTULO III
DA AUTORIZAÇÃO E ESCOPO
Art. 5º Nenhum Teste de Penetração, interno ou externo, poderá ser iniciado sem autorização formal e por escrito, consubstanciado em "Termo de Autorização e Regras de Engajamento".
Art. 6º O Termo de Autorização e Regras de Engajamento deve ser elaborado pela Coordenadoria de Segurança da Informação e aprovado pela Secretaria de Tecnologia da Informação (SECTI).
Art. 7º O Termo de que trata o art. 6º deve conter, no mínimo:

I - O escopo detalhado dos ativos (IPs, URLs, sistemas, aplicações);
II - Os ativos e técnicas expressamente excluídos (fora do escopo);
III - A metodologia (ex: Black Box, Grey Box, White Box);
IV - A identificação da equipe de teste (Pentesters);
V - O cronograma, incluindo datas, horários (janelas de teste) e duração;
VI - Os pontos de contato de emergência (equipe de teste e SECTI);
VII - As regras para o manuseio de dados sensíveis ou pessoais encontrados, em conformidade com a LGPD;
VIII - A comprovação de autorização prévia junto a provedores de serviços em nuvem ou terceiros, quando os ativos testados estiverem sob infraestrutura de terceirizados.
Art. 8º A frequência dos testes será definida pelo GSI, com base na análise de riscos e criticidade dos ativos, observando-se:
I - A obrigatoriedade de testes em aplicações críticas expostas à Internet;
II - A realização de testes antes da entrada em produção de novos sistemas judiciais ou administrativos relevantes;
III - A realização de testes após mudanças significativas na arquitetura de segurança.
CAPÍTULO IV
DAS REGRAS DE EXECUÇÃO E CONDUTA
Art. 9º São expressamente proibidas durante os testes, salvo autorização excepcional e justificada no Termo de Autorização:
I - Ações que visem causar Negação de Serviço (DoS/DDoS) ou indisponibilidade dos ambientes de produção;
II - A exfiltração, alteração, ou destruição de dados reais, em especial dados pessoais ou protegidos por sigilo legal;
III - O acesso ou tentativa de acesso a sistemas de terceiros ou fora do escopo definido;
IV - Testes de engenharia social que não tenham sido previamente alinhados com a Administração Superior.
Art. 10 A equipe de teste deve interromper imediatamente qualquer ação que, de forma não intencional, cause instabilidade, degradação de serviço ou corrupção de dados, comunicando o fato imediatamente ao ponto de contato de emergência da SECTI.
Art. 11 Todos os relatórios, dados brutos e informações coletadas durante o teste são classificados como [RESTRITO] ou [SECRETO], conforme a Política de Classificação da Informação do Tribunal, e devem ser armazenados e transmitidos por meios criptografados.
Art. 12 Se o teste for realizado por entidade externa, é obrigatória a assinatura de Acordo de Confidencialidade (NDA) e a comprovação de qualificação técnica da equipe executora.
CAPÍTULO V
DAS RESPONSABILIDADES
Art. 13 Cabe à SECTI, por meio de suas áreas técnicas:
I - Elaborar o plano anual de Testes de Penetração, com base na análise de riscos;
II - Gerenciar o processo de contratação de serviços de Pentest, quando aplicável;
III - Elaborar o Termo de Autorização e Regras de Engajamento em conjunto com os Gestores de Ativos;
IV - Supervisionar a execução dos testes e servir como ponto de contato técnico e de emergência;
V - Receber e validar tecnicamente os relatórios de vulnerabilidades entregues pela equipe de teste.
Art. 14 Cabe aos Gestores dos Ativos de Informação (Proprietários dos Sistemas):
I - Aprovar formalmente o Termo de Autorização para a realização dos testes em seus ativos;

II - Disponibilizar informações (ex: contas de usuário, documentação), caso a metodologia (ex: Grey Box) exija;
III - Receber o relatório de vulnerabilidades e elaborar o Plano de Ação para remediação;
IV - Assegurar a implementação das correções nos prazos definidos.
Art. 15 Cabe à Equipe de Teste (*Pentesters*):
I - Ater-se estritamente ao escopo, metodologia e regras de engajamento autorizadas;
II - Manter sigilo absoluto sobre as informações e vulnerabilidades encontradas;
III - Reportar imediatamente falhas críticas ou instabilidades, conforme art. 10;
IV - Elaborar o relatório técnico final, contendo a classificação de risco (ex: CVSS), descrição das falhas, evidências (provas de conceito) e recomendações de correção.
CAPÍTULO VI
DA GESTÃO DE VULNERABILIDADES E RE-TESTE
Art. 16 As vulnerabilidades identificadas no relatório final deverão ser registradas e tratadas conforme o processo de Gestão de Riscos e Vulnerabilidades do Tribunal.
§ 1º A priorização da remediação e os prazos máximos para correção serão estabelecidos de acordo com a pontuação CVSS (*Common Vulnerability Scoring System*), conforme a seguinte escala:

Criticidade	Pontuação CVSS	Prazo para Remediação	Ação Requerida
Crítica	9.0 - 10.0	Até 5 dias úteis	Correção imediata ou aplicação de controle compensatório urgente.
Alta	7.0 - 8.9	Até 20 dias úteis	Inclusão prioritária no ciclo de manutenção /desenvolvimento.
Média	4.0 - 6.9	Até 60 dias úteis	Planejamento conforme cronograma da área técnica.
Baixa	0.1 - 3.9	Conforme conveniência	Monitoramento ou correção em atualizações futuras de rotina.

§ 2º Os prazos previstos no § 1º poderão ser prorrogados mediante justificativa técnica fundamentada do Gestor do Ativo, com anuência do Gestor de Segurança da Informação (GSI).
§ 3º Os prazos para remediação, citados no §1º serão definidos em comum acordo entre GSIPDP e Gestor do Ativo de Informação, observando-se a severidade: Crítica, Alta, Média e Baixa (conforme escala).
Art. 17 Após a aplicação das correções, a SECTI deverá providenciar a validação (re-teste) para confirmar a eficácia da remediação.
Art. 18 Caso uma vulnerabilidade não possa ser corrigida por limitações técnicas ou operacionais, o risco residual deverá ser formalmente documentado e submetido à apreciação do Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais (CGSIPDP) para aceitação formal.
CAPÍTULO VII
DISPOSIÇÕES FINAIS
Art. 19 Os casos omissos serão resolvidos pelo CGSIPDP.
Art. 20 Esta norma será revisada sempre que se fizer necessário, mediante aprovação do CGSIPDP.
Art. 21 Esta Norma Técnica entrará em vigor na data de sua publicação.
Curitiba, 28 de agosto de 2026.
GILMAR JOSÉ FERNANDES DE DEUS
Secretário de Tecnologia da Informação

0013648-45.2026.6.16.8000	0435168v2