Solicitação nº: 0111/2026; Favorecido: DENISE ARANHA SOUZA GODINHO; Cargo/Função: FC-06 CHEFE DE SEÇÃO; Deslocamento: GOIANIA a SILVANIA - SILVANIA a PIRACANJUBA - PIRACANJUBA a CALDAS NOVAS; Finalidade da viagem: Inspeções de Ciclo nos Cartórios das 7ª, 25ª e 31ª Zonas Eleitorais, sediadas em Caldas Novas, Piracanjuba e Silvânia, nos dias 11 e 12 de março de 2026.; Afastamento: 11/03/2026 a 12/03/2026; Nº de diárias: 1,5; Valor Unitário: 763,60; Total Bruto: 1.145,40; Total Líquido: 976,28

PORTARIAS

PORTARIA DG Nº 50, DE 18 DE MARÇO DE 2026

PUBLICAÇÃO EM : 20/03/2026

Portaria DG Nº 50, DE 18 DE março DE 2026.
O DIRETOR-GERAL EM SUBSTITUIÇÃO DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso da atribuição prevista no art. 46, inciso XVI, da Resolução TRE-GO nº 275, de 18 de dezembro de 2017 (Regulamento Interno), e considerando a instrução do procedimento SEI nº 25.0.000009284-6,
RESOLVE:
CAPÍTULO I
DAS DISPOSIÇÕES GERAIS
Art. 1º Fica instituída, no âmbito do Tribunal Regional Eleitoral de Goiás, a Norma de Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação - TI, a qual passa a integrar a Política de Segurança da Informação da Justiça Eleitoral - PSI, estabelecida pela Resolução TSE nº 23.644, de 1º de julho de 2021 e pela Resolução TRE-GO nº 355, de 10 de novembro de 2021.
CAPÍTULO II
DOS CONCEITOS E DAS DEFINIÇÕES
Art. 2º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG /TSE nº 444, de 8 de julho de 2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, regulamentado por meio da Portaria GSI/PR nº 93, de 18 de outubro de 2021.
Parágrafo único. Consideram-se, também, as seguintes definições:
I - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
II - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
III - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
IV - ativo de informação: todo dado ou informação gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, *software* ou recurso utilizado para seu processamento e/ou armazenamento.
CAPÍTULO III
DO ESCOPO E DO ÂMBITO DE APLICAÇÃO
Art. 3º A gestão de vulnerabilidades tem como objetivo refrear a exploração de vulnerabilidades técnicas na rede corporativa, por meio da aplicação sistemática das seguintes ações de prevenção, identificação, classificação e tratamento:
I - ações técnicas preventivas para reduzir o risco de exposição a ameaças;
II - obtenção de informações para identificar vulnerabilidades técnicas em tempo hábil;
III - avaliação de exposição às vulnerabilidades técnicas;

IV - adoção de medidas apropriadas e tempestivas para lidar com os riscos identificados;
V - remediação das vulnerabilidades encontradas;
VI - revisão das ações e atividades desempenhadas na mitigação das vulnerabilidades do ambiente.
Art. 4º Este normativo se aplica a todos(as) os(as) magistrados(as), servidores(as) em exercício na Justiça Eleitoral de Goiás, servidores(as) efetivos(as) deste Regional em exercício em outro órgão público, inativos(as), estagiários(as), prestadores(as) de serviço, colaboradores(as) e usuários(as) externos(as), outros órgãos públicos ou entidades privadas contratadas ou com parcerias celebradas, acordos de cooperação de qualquer tipo, convênios e termos congêneres, que fazem uso dos ativos de informação e de processamento desta Justiça especializada.
§ 1º Os contratos celebrados pelo Tribunal Regional Eleitoral de Goiás deverão atender aos requisitos desta portaria, bem como as normas referentes à proteção de dados pessoais.
§ 2º Os(as) usuários(as) relacionados(as) no *caput* são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos neste normativo.
§ 3º Os(as) usuários(as) de ativos de TI são responsáveis por:
a) manter o ambiente seguro, conforme os padrões estabelecidos nesta norma;
b) manter a confidencialidade das informações acessadas;
c) informar imediatamente qualquer risco identificado ou presumido à segurança da Instituição.
CAPÍTULO IV
DO MONITORAMENTO DE BASES DE VULNERABILIDADES
Art. 5º 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 e fontes de consulta pelos seguintes critérios:
a) qualidade das informações: verificar se as informações fornecidas pela fonte são precisas e atualizadas;
b) disponibilidades das informações: verificar a frequência de atualização das informações fornecidas pela fonte;
c) legitimidade da fonte: verificar se a fonte é representante autorizado do responsável pela informação 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 sem correções disponíveis (vulnerabilidade 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.
CAPÍTULO V
DA GESTÃO E DA ANÁLISE DE VULNERABILIDADES
Art. 6º O processo de gestão e análise de vulnerabilidades consiste em buscar, priorizar e corrigir vulnerabilidades em recursos, sistemas operacionais, infraestrutura, banco de dados, sistemas de informação, *softwares*, soluções e serviços de TI de forma a garantir que os ativos de TI tenham condições seguras de uso.

Parágrafo único. O processo de gestão de vulnerabilidades deve permitir a implementação de mecanismos para obtenção de informações sobre potenciais ameaças aos ativos de TI e adoção de salvaguardas apropriadas para lidar com os riscos associados.

Seção I

Da descoberta de vulnerabilidades técnicas

Art. 7º A descoberta de vulnerabilidades técnicas consiste na fase responsável por realizar o levantamento e a análise minuciosa dos sistemas, aplicativos, *softwares*, banco de dados, infraestrutura e processos para identificar possíveis falhas ou pontos fracos que possam ser explorados por ameaças, o que envolve a execução das seguintes atividades:

I - manter um inventário atualizado (marca, modelo, versão) de todos os ativos de TI, incluindo *hardware*, *software*, sistemas, bases de dados, equipamentos de TI, que forneçam ligação ao ambiente (*servers*, *switches*, roteadores, *access point*, impressoras, etc.);

II - realizar varredura de vulnerabilidades, sempre que possível e em intervalos planejados ou após alterações significativas no ambiente de TI, por equipe interna, terceiros, ferramentas automatizadas ou uma combinação de ambos;

III - preparar as ferramentas aplicadas nas varreduras de vulnerabilidades e verificar sua integridade de forma a evitar erros no mapeamento de brechas de segurança;

IV - realizar teste de vulnerabilidades, sempre que possível, por meio de *scanners* de ambiente, testes de penetração (*pentest*) e acompanhamento de alertas de segurança.

Art. 8º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para rotinas de identificação de vulnerabilidades técnicas na rede corporativa, utilizando-se, regularmente, de ferramentas automatizadas:

I - empregar ferramenta atualizada de varredura de vulnerabilidades para investigar automaticamente os ativos e identificar vulnerabilidades na rede corporativa, considerando pelo menos as seguintes características:

a) utilização da fonte "*Common Vulnerabilities and Exposures - CVE*" (Vulnerabilidades e Esposições Comuns) 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) classificação de severidade das vulnerabilidades identificadas, atribuindo, no mínimo, os critérios de padronização *Common Vulnerability Scoring System - CVSS* estático ou padrões dinâmicos aprimorados.

II - 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;

III - usar conta de serviço dedicada para varreduras de vulnerabilidades, que não deve ser utilizada para outras atividades administrativas e deve estar vinculada aos equipamentos específicos em endereços de *Internet Protocol - IP* específicos.

Seção II

Da avaliação da exposição

Art. 9º A avaliação da exposição é a fase responsável por compreender o impacto e a criticidade das vulnerabilidades de TI identificadas, priorizando as ações necessárias para mitigá-las, o que envolve a execução das seguintes atividades:

I - coletar e analisar as informações disponíveis sobre vulnerabilidades, incluindo *logs* e outros registros gerados pelos recursos, sistemas e serviços de TI;

II - realizar varreduras automatizadas (autenticadas e não autenticadas) de vulnerabilidades nos ativos de TI, sob responsabilidade da Secretaria de Tecnologia da Informação - STI, com periodicidade planejada:

a) ativos críticos (infraestrutura de rede e lógica, sistemas administrativos e eleitorais, ambiente de produção, etc): no mínimo, bimestralmente;

b) demais ativos: no mínimo, semestralmente;

c) ou a qualquer tempo, quando necessário para avaliação do ambiente e exposição de riscos e ameaças desconhecidas.

III - avaliar a integridade dos resultados obtidos na detecção das vulnerabilidades;

IV - identificar a existência de outros eventos e alertas relacionados com as vulnerabilidades em questão;

V - verificar que tipos de informações e processos podem ser afetados com as vulnerabilidades identificadas;

VI - avaliar a relevância e o impacto das vulnerabilidades a fim de definir quais medidas devem ser tomadas para a remediação;

VII - manter, dentro do possível, um banco de dados de vulnerabilidades coletadas de várias fontes, como *sites* de segurança da informação, boletins de segurança ou publicações de fornecedores de *softwares* que precisam ser aplicadas aos ativos da STI;

VIII - analisar, regularmente, as informações coletadas e mantidas no banco de dados de vulnerabilidades objetivando identificar tendências e padrões visando a tomada de medidas proativas para evitar fragilidades futuras;

IX - classificar/categorizar a severidade das vulnerabilidades identificadas e atribuir a elas um nível de prioridade de acordo com a gravidade e o risco real.

Art. 10. 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, 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 Comitê Gestor de Segurança da Informação - CGSI sobre a impossibilidade de tratamento de vulnerabilidade técnica classificada como crítica;

VII - geração de registro do incidente.

Seção III

Do tratamento de vulnerabilidades técnicas

Art. 11. O tratamento de vulnerabilidades técnicas é a fase responsável por corrigir ou remediar as vulnerabilidades identificadas e avaliadas com base na aplicação de correções, *patches* de segurança, atualizações de *softwares* ou implementação de contramedidas, o que envolve a execução das seguintes atividades:

I - estabelecer e manter uma estrutura de remediação documentada e com revisões frequentes;

II - executar atualizações de aplicativos e sistemas operacionais por meio do gerenciamento automatizado de *patches* de segurança com maior frequência;

III - tratar vulnerabilidades com base na priorização realizada a partir da classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo impactado tem para o negócio;

IV - corrigir as vulnerabilidades detectadas por meio de processos e ferramentas em intervalos planejados;

V - implantar em produção, somente as correções de vulnerabilidades que foram efetivamente testadas e aprovadas de forma que os controles apropriados em relação aos testes, avaliação de riscos e reparação sejam aplicados.

Art. 12. Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados para corrigir as vulnerabilidades técnicas ou minimizar a probabilidade de exploração:

I - observância da norma de Tratamento e Resposta a Incidentes em Redes de Computadores vigente;

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, contemplando 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;

V - quando não existir a possibilidade de correção da vulnerabilidade - 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 reais;

c) aumento da conscientização sobre a vulnerabilidade;

d) implementação de controles de segurança compensatórios.

Art. 13. 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.

Seção IV

Da avaliação dos resultados

Art. 14. A avaliação dos resultados é fase responsável por avaliar se as medidas de remediação tomadas e as ações realizadas foram efetivas ao ambiente do Tribunal, o que envolve a execução das seguintes atividades:

I - confirmar o restabelecimento da normalidade dos recursos computacionais após tratamento das vulnerabilidades;

II - registrar as ações realizadas durante o processo de remediação, incluindo as vulnerabilidades identificadas, as soluções aplicadas e os resultados dos testes;

III - preparar relatórios detalhados sobre vulnerabilidades encontradas, análises de risco, ações tomadas e recomendações;

IV - registrar lições aprendidas e *feedback* com os(as) usuários(as) envolvidos;

V - atualizar periodicamente políticas e procedimentos e controles internos com base nas evidências obtidas durante a gestão de vulnerabilidades;
VI - organizar e manter repositório com registros e relatórios utilizados como base para avaliação e aprimoramento do processo.
Art. 15. Os controles estabelecidos nos incisos deste artigo devem ser aplicados para analisar criticamente os resultados da gestão de vulnerabilidades e promover a melhoria contínua do processo:
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 periódica ao CGSI, por meio de relatórios estatísticos, sobre os resultados de detecção e tratamento das vulnerabilidades no ambiente computacional;
V - proposição de melhorias nos processos da gestão de vulnerabilidades para o CGSI, com base em relatórios técnicos, métricas, registros de incidentes, lições aprendidas e *feedback* obtidos nas fases de avaliação e tratamento.
Seção V
Das responsabilidades
Art. 16. Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas, as responsabilidades e competências no âmbito da segurança da informação devem observar os seguintes parâmetros:
I - à Unidade de Segurança Cibernética caberá:
a) 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;
b) monitorar ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas no ativo, assegurando a execução de verificações na periodicidade mínima definida para cada tipo de ativo;
c) analisar e avaliar os riscos das vulnerabilidades técnicas detectadas, emitindo os relatórios técnicos correspondentes;
d) comunicar-se com as áreas da Secretaria de TI responsáveis pelos ativos, a fim de informar e obter informações acerca de vulnerabilidades existentes;
e) acompanhar a detecção e o tratamento das vulnerabilidades através de ferramenta automatizada específica e documentação produzida pelas unidades;
f) avaliar projetos de atualização ou correção, que se façam necessários para mitigar riscos críticos, apoiando no embasamento técnico para a tomada de decisão corretiva;
g) reportar à STI a análise crítica dos resultados da gestão de vulnerabilidades e proposição de melhorias nos processos;
h) manter documentação do ciclo de vida da gestão de vulnerabilidades, incluindo os planos de ação, os relatórios de análise, as justificativas para não aplicação de correções e os resultados informados pelas equipes executoras.
II - à unidade responsável pela administração do ativo deverá:
a) identificar, avaliar, classificar, sempre que possível, por meio de ferramenta automatizada, as vulnerabilidades de TI dos ativos sob responsabilidade da unidade, assegurando a execução de verificações na periodicidade mínima definida no art. 9º desta portaria;

b) elaborar plano de ação para o tratamento das vulnerabilidades, em conjunto com as demais unidades da STI, definindo a ordem de prioridade para as correções e os prazos para execução, com base na análise de risco, considerando sempre que possível, o processo de Gestão de Mudanças estabelecido;
c) planejar e executar ações de correção das vulnerabilidades de TI ou, ao menos, minimizar a probabilidade de exploração, conforme plano de ação definido;
d) emitir relatório técnico das vulnerabilidades, encontradas, tratadas e não tratadas, reportando, no mínimo, identificação do ativo, *status* da correção, ações contempladas ou não contempladas na correção, responsável(is) técnico(s), técnica utilizada para mitigação, entre outras informações completivas.
CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS
Art. 17. Deverão ser realizadas práticas de conscientização e treinamento sobre vulnerabilidades de segurança de TI aos servidores e colaboradores, relativos às melhores práticas para uso de *software* e *hardwares*, visando a proteção contra ameaças cibernéticas.
Art. 18. Esta norma complementar deverá ser revisada a cada 24 meses, ou a qualquer tempo conforme necessidade, e encaminhada para nova apreciação do CGSI.
Art. 19. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação do TRE-GO.
Art. 20. Esta portaria entra em vigor na data de sua publicação.
HUMBERTO VILANI
Diretor-Geral em substituição

ATOS DA PRESIDÊNCIA

DECISÕES

EXTRATO CONCESSÃO DE DIÁRIAS - 0122/2026

PUBLICAÇÃO EM : 20/03/2026

Solicitação nº: 0122/2026; Favorecido: NELSON GARCIA PEREIRA JUNIOR; Cargo/Função: JUIZ ELEITORAL; Deslocamento: ALVORADA DO NORTE a GOIANIA; Finalidade da viagem: Deslocamento do MM. Juiz da 123ª Zona Eleitoral - Alvorada do Norte, Dr. Nelson Garcia Pereira Júnior, em razão de sua participação no Encontro de Magistrados da Justiça Eleitoral de Goiás.; Afastamento: 25/03/2026 a 28/03/2026; Nº de diárias: 3,5; Valor Unitário: 1.153,37; Total Bruto: 4.036,79; Total Líquido: 3.743,57

EDITAIS

TERMO DE HOMOLOGAÇÃO - CONCURSO DE REMOÇÃO Nº 1/2026

PUBLICAÇÃO EM : 20/03/2026

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, Desembargador Luiz Claúdio Veiga Braga, no uso de suas atribuições legais, nos termos das Resoluções TRE-GO nº 276/2018, de 29 de janeiro de 2018, e nº 307/2019, de 28 de junho de 2019 (alterada pela Resolução TRE-GO nº 390, de 20 de setembro de 2023), observadas as prescrições contidas na Resolução TSE nº 23.701, de 31 de maio de 2022, considerando o contido no processo SEI n° 26.0.000002708-0, HOMOLOGA o resultado final do Concurso de Remoção nº 1/2026, conforme