TRIBUNAL REGIONAL ELEITORAL DE GOIÁS
PRAÇA CÍVICA, 300 - Bairro CENTRO - CEP 74003-010 - Goiânia - GO - www.tre-go.jus.br

PORTARIA DG Nº 333, DE 03 DE NOVEMBRO DE 2025.

O **DIRETOR-GERAL 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 25.0.000006720-5,

RESOLVE:

CAPÍTULO I

DAS DISPOSÇÕES GERAIS

Art. 1º Fica instituída a Norma de Uso Aceitável de Ativos de TI relativa à segurança da informação e comunicação no âmbito do Tribunal Regional Eleitoral de Goiás, a qual passa a integrar a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.644/2021.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeitos desta norma, aplicam-se os termos e definições previstos na Portaria DG/TSE nº 444/2021, 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.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 3º Esta norma tem como princípios norteadores:

I – garantia da segurança institucional;

II – assegurar a integridade, confidencialidade, autenticidade e disponibilidade dos ativos de informação e comunicação.

CAPÍTULO IV

DO ESCOPO E DO ÂMBITO DE APLICAÇÃO

Art. 4º São objetivos desta norma:

I – estabelecer diretrizes para o uso dos recursos de tecnologia da informação e comunicação; e

II – preservar os recursos sob a responsabilidade do Tribunal.

Art. 5º 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, 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 Especializada.

§ 1º Os contratos celebrados pelo Tribunal deverão atender aos requisitos desta portaria, bem como as normas referentes à proteção de dados pessoais.

§ 2º Os(as) usuários(as) relacionados 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, incluindo criação de senhas seguras, 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 V

DO USO DOS ATIVOS DE TI

Seção I

Das estações de trabalho

Art. 6º O uso dos ativos de TI da rede corporativa está restrito aos(as) usuários(as) autorizados(as), conforme os acordos de segurança por eles(as) assinados, e deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades.

Parágrafo único. Todo(a) servidor(a) e colaborador(a) da Justiça Eleitoral terá, em seu posto de trabalho, acesso a uma estação de trabalho destinada à execução de atividades da Justiça Eleitoral ou a elas diretamente correlatas.

Art. 7º A utilização dos ativos de TI, próprios ou de terceiros, ou sua conexão à rede corporativa, requer prévia aprovação da Secretaria de Tecnologia da Informação (STI) ou deliberação do Comitê Gestor de Segurança da Informação (CGSI), conforme o caso.

Art. 8º As estações de trabalho possuirão configurações de *hardware* e *software* padronizadas pela STI, sempre que possível, de forma automatizada, por meio da aplicação de Políticas de Grupo (GPOs), de acordo com a necessidade de utilização dos(as) usuários(as) e deverão atender, no mínimo, aos seguintes requisitos de segurança:

I – o sistema operacional deve possuir suporte ativo para recebimento de atualizações de segurança homologadas pela STI;

II – deverão possuir *software antimalware* (que previna *software* malicioso) instalado, ativado, permanentemente atualizado e configurado para realizar verificação automática das mídias removíveis;

III – todos os *softwares* instalados deverão ser configurados para receber atualização de forma controlada, exceto quando a atualização for tecnicamente inviável;

IV – a reprodução automática de mídias removíveis, nas estações de trabalho, deve estar desativada, preferencialmente via GPO;

V – as configurações de segurança das estações de trabalho dos(as) usuários(as) serão definidas e configuradas pela STI.

Art. 9º As estações de trabalho receberão *softwares* homologados e licenciados pela STI, conforme a necessidade de cada usuário(a) e a disponibilidade de licenças.

Art. 10. A critério da STI, poderão ser desabilitados dispositivos de *hardware* e *software* nativos dos equipamentos, a fim de preservar a segurança e a integridade da rede de comunicação de dados.

Art. 11. Não é permitido o compartilhamento de pastas de arquivos locais na rede sem a anuência da STI.

Art. 12. É dever do(a) usuário(a) bloquear a sua estação de trabalho sempre que se ausentar do seu posto de trabalho.

Parágrafo único. As estações de trabalho devem ser configuradas para ter bloqueio automático de tela em casos de período de inatividade e, para restaurar a sessão, o(a) usuário(a) deverá ser obrigado a fornecer novamente suas credenciais de acesso.

Art. 13. Compete ao(à) usuário(a) zelar pela integridade e conservação dos ativos de TI:

§ 1º É vedada a abertura das estações de trabalho por pessoal não autorizado pela Secretaria de Tecnologia da Informação.

§ 2º O(a) usuário(a) deve informar, imediatamente à STI, quando identificar violação da integridade física do equipamento por ele utilizado.

§ 3º Será considerado uso indevido, por parte dos(as) usuários(as), permitir que pessoas estranhas aos quadros da Justiça Eleitoral tenham acesso aos equipamentos e/ou recursos de TI do Tribunal.

Art. 14. É vedado aos(às) usuários(as):

I – instalar, por conta própria, quaisquer tipos de *software* nas estações de trabalho que não estejam disponibilizados em área específica de *softwares* homologados (Central do *Software*), sendo facultada à STI a verificação, de forma presencial ou remota, e a desinstalação, sem necessidade de comunicação prévia;

II – alterar quaisquer configurações de *hardware* ou *software* nas estações de trabalho sem a autorização e orientação da STI.

Art. 15. É vedado à STI conceder aos(as) usuários(as) finais privilégios de administrador local nas estações de trabalho.

Parágrafo único. Havendo necessidade de o(a) usuário(a) final possuir acesso privilegiado, a chefia imediata deverá solicitar de forma justificada à STI, conforme previsto na Norma de Gestão de Identidades e Controle de Acesso Físico e Lógico, complementar à Política de Segurança da Informação do TRE-GO.

Art. 16. A instalação de novo serviço ou *software*, deverá ser solicitada à STI, no canal de atendimento de requisições de serviços, condicionado o atendimento do pedido à disponibilidade de licença.

Parágrafo único. Quando um *software* ou serviço não for mais útil para o desempenho das atividades institucionais, o(a) usuário(a) deverá solicitar à STI a sua desinstalação.

Art. 17. As unidades do Tribunal devem, obrigatoriamente, submeter à prévia análise da Secretaria de Tecnologia da Informação a intenção em adquirir ou instalar *software*, equipamento ou serviço que não tenha sido provido pela área de TI e que faça uso ou requeira recursos de tecnologia da informação e comunicação.

Parágrafo único. A STI poderá aprovar ou vetar, por questões de segurança, por falta de compatibilidade ou de padronização com as soluções já adotadas.

Art. 18. Máquinas virtuais poderão ser disponibilizadas quando houver necessidade de acesso a mais do que um ambiente, ou em casos especiais a serem analisados pela STI.

Seção II

Da rede corporativa

Art. 19. São consideradas redes de dados do Tribunal Regional Eleitoral de Goiás, para efeito de controle,

a rede lógica da sede e seus anexos, todas as redes sem fio (*wi-fi*) em suas dependências e por ele providas, o acesso VPN (Rede Virtual Privada), o perímetro para a Internet e as redes lógicas das zonas eleitorais.

Art. 20. A Secretaria de Tecnologia da Informação poderá fazer uso de ferramentas, *softwares* e procedimentos que venham garantir a segurança da rede corporativa do Tribunal e dos dados que nela trafegam.

Parágrafo único. Equipamentos que forem identificados como potencialmente nocivos à rede de dados do Tribunal, seja por contaminação por vírus ou por outro tipo de anomalia, poderão ser postos em quarentena, sem aviso prévio ao(à) usuário(a), somente saindo dessa condição após analisados pela STI.

Art. 21. Somente pessoas autorizadas pela STI possuem permissão para adicionar, configurar ou retirar dispositivos de TI no ambiente corporativo do Tribunal.

Art. 22. É proibida a conexão de qualquer dispositivo não fornecido pelo Tribunal aos ativos que compõe a infraestrutura de sua rede de dados, salvo em redes preparadas para essa finalidade, mediante orientação e anuência da STI.

§ 1º A conexão de qualquer equipamento à rede corporativa do Tribunal será analisada tecnicamente pela STI, ou por terceiros por ela autorizados.

§ 2º Em situações excepcionais o uso de equipamentos particulares para acesso à rede corporativa de forma local ou remota poderá ser admitido, mediante permissão e orientação da STI, ficando este acesso condicionado ao atendimento de requisitos de segurança previamente estabelecidos.

§ 3º Eventual inclusão de equipamentos de terceiros na rede sem fio fornecida pelo TRE-GO será efetuada em sub-rede segura, distinta das demais, quando tecnicamente possível.

Art. 23. A inclusão de equipamentos e usuários(as) na VPN do Tribunal, deverá ser solicitada à STI, por meio de sua Central de Serviços, com autorização do respectivo titular da macrounidade do Tribunal, a ser anexada ao chamado, ou com a indicação do correspondente processo eletrônico onde este acesso foi autorizado.

§ 1º O horário de funcionamento da VPN ou recursos a ela vinculados será definido pelo Comitê Gestor de Segurança da Informação (CGSI), em procedimento interno, e qualquer excepcionalidade deverá ser solicitada à STI, com antecedência mínima de 2 dias;

§ 2º Os acessos à rede de dados devem ser registrados e arquivados por período definido em norma específica (gestão de *logs*), e monitorados com finalidade de identificar acessos indevidos;

§ 3º Deverá ser exigido múltiplo fator de autenticação nas máquinas que acessarem a VPN do Tribunal Regional Eleitoral de Goiás.

Art. 24. Os pontos de acesso sem fio conectados à rede corporativa deverão ser registrados e aprovados pela STI.

Art. 25. As conexões à rede sem fio poderão ser avaliadas pela STI em relação aos requisitos de segurança e deverão atender ao princípio do menor privilégio.

Art. 26. Os dispositivos conectados à rede corporativa, através de conexão sem fio, deverão utilizar as configurações estabelecidas pela STI.

Seção III

Do armazenamento de arquivos

Art. 27. As unidades do Tribunal poderão ter disponível área de armazenamento em rede (diretório compartilhado), com espaço limitado, conforme a disponibilidade da infraestrutura, para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

§ 1º Esses arquivos serão acessíveis apenas internamente, a partir da rede do Tribunal.

§ 2º Apenas informações corporativas de interesse do Tribunal poderão ser armazenadas nesses diretórios.

§ 3º Não serão aceitos arquivos com dados pessoais e particulares, arquivos de imagens, vídeos, filmes, músicas e correlatos, salvo exceção às unidades que necessitam desses tipos de arquivos para desenvolvimento de suas atividades.

Art. 28. O Tribunal se reserva o direito de inspecionar, sem a necessidade de aviso prévio, os computadores e arquivos neles armazenados, nas áreas privativas ou nas áreas compartilhadas da rede, visando assegurar o cumprimento desta norma.

Art. 29. É de responsabilidade de cada unidade verificar os arquivos armazenados na área de armazenamento em rede, de forma que prevaleçam os arquivos que são necessários ao trabalho, os mais recentes e prioritários.

Parágrafo único. Os arquivos que não são mais necessários ou estão em versões obsoletas devem ser excluídos, a fim de garantir a manutenção do espaço disponibilizado às unidades.

Art. 30. É vedada a utilização de serviços em nuvem, de caráter particular, para o processamento ou armazenamento de dados pessoais, sigilosos ou em segredo de justiça, de propriedade ou sob a responsabilidade da Justiça Eleitoral.

§ 1º Constatada a ocorrência descrita no *caput*, a responsabilidade quanto à confidencialidade, integridade, disponibilidade e autenticidade de tais informações recairá, com exclusividade, sobre o(a) usuário(a) do serviço utilizado.

§ 2º O incidente de segurança da informação no Tribunal, resultante da violação ao disposto neste artigo, sujeitará o(à) usuário(a) responsável às penalidades previstas na legislação.

Art. 31. A cópia de segurança dos dados gravados em estações de trabalho e dispositivos móveis (*notebooks*, *smartphones*, *tablets*, entre outros) é de responsabilidade exclusiva do(a) próprio(a) usuário(a).

§ 1º O(a) usuário(a) deverá evitar que em sua estação de trabalho permaneçam armazenados dados pessoais e, de modo algum, armazená-los em pastas de acesso público.

§ 2º Em caso de defeito no dispositivo de armazenamento local, que resulte na perda de dados profissionais ou particulares, que eventualmente não sejam recuperados pela equipe de suporte da STI, em hipótese alguma serão liberados para recuperação em empresas especializadas, de modo a preservar a confidencialidade dos dados institucionais.

Art. 32. A cópia de segurança de dados institucionais, armazenados em servidores de rede do Tribunal, deverá ser operacionalizada pela STI sendo observada a periodicidade do *backup* institucional, definido em norma específica.

Seção IV

Do acesso remoto a recursos de TI

Art. 33. O acesso remoto para suporte técnico aos equipamentos de informática do Tribunal tem por finalidade diminuir a necessidade do deslocamento do técnico do seu local de trabalho para onde estão instalados os equipamentos.

§ 1º O acesso remoto a equipamentos de propriedade do TRE-GO, para prestar suporte e solução de problemas, somente será realizado mediante autorização do(a) usuário(a), durante o atendimento de chamados registrados formalmente.

§ 2º As estações serão previamente configuradas para permitir o acesso apenas à equipe da STI, responsável pelo suporte técnico.

§ 3º O acesso remoto sem autorização do(a) usuário(a), poderá ser realizado somente em regime de

exceção, mediante autorização fundamentada do Secretário de Tecnologia da Informação.

Art. 34. A STI disponibilizará aplicações e serviços na internet e o acesso remoto à rede corporativa do Tribunal, conforme regras específicas e características técnicas de cada serviço.

Art. 35. As aplicações e serviços *web* do Tribunal, que forem disponibilizadas na internet, poderão exigir autenticação de múltiplos fatores.

Art. 36. Nos casos de necessidade, para desempenho do trabalho, os(as) usuários(as) poderão fazer uso do acesso remoto a serviços e sistemas do Tribunal, mediante solicitação justificada da chefia imediata à STI, por meio do canal de atendimento de requisições de serviços.

§ 1º As permissões concedidas devem prezar pelo menor privilégio de acesso e serão restritas aos serviços necessários ao desenvolvimento do trabalho do(a) usuário(a).

§ 2º O acesso remoto dar-se-á por equipamentos fornecidos pelo Tribunal, conforme disponibilidade, sendo vedado o acesso remoto à rede institucional, por meio de computadores e redes públicos.

Art. 37. O acesso remoto poderá ser interrompido a qualquer momento, independente de comunicação ao(à) usuário(a), na hipótese de ser identificada situação de grave ameaça ou alto risco à integridade da rede interna e dos serviços disponíveis.

Art. 38. O extravio de dispositivo ou certificado, utilizado para acesso remoto, deverá ser imediatamente comunicado à STI.

Art. 39. Fica vedada a utilização de aplicativos de acesso remoto não homologados, sem o conhecimento e autorização expressa da STI.

Art. 40. O suporte técnico, para o acesso remoto aos recursos de TI do Tribunal, estará disponível durante o horário de expediente formalmente estabelecido.

Parágrafo único. O acesso remoto para suporte técnico externo, por parte de empresas contratadas, será realizado sob autorização e supervisão técnica da equipe responsável.

Art. 41. A conexão aos serviços, via acesso remoto, deverá ser desconectada imediatamente ao término dos trabalhos.

Seção V

Dos meios de impressão

Art. 42. Os recursos de impressão pertencentes a este Tribunal e disponíveis para o(a) usuário(a) serão utilizados em atividades estritamente relacionadas às suas funções institucionais.

Art. 43. Sempre que possível, o compartilhamento de documentos digitais deve ser priorizado, evitando o uso desnecessário de insumos.

Art. 44. Os meios de impressão, sempre que possível, devem ser compartilhados por mais de uma unidade, visando economicidade dos recursos e às recomendações da área de sustentabilidade.

Seção VI

Do monitoramento dos ativos de TIC

Art. 45. O uso dos recursos de TI da rede corporativa está sujeito a monitoramento pelo Tribunal, com vistas a proteger a integridade da imagem e das informações institucionais, preservar a segurança de seus sistemas corporativos ou de seus(suas) usuários(as) e, também, para fins de apuração de eventual uso indevido, ilegal ou não autorizado, podendo ser auditados, dentre outros, os objetos e eventos abaixo relacionados:

I – dados recebidos e transmitidos, criptografados ou não;

II – arquivos presentes nos ativos de TI e afins;

III – *softwares*, sistemas, programas de computador, inclusive em execução;

IV – bases específicas de registros de eventos (*logs*);

V – acessos realizados a sítios ou serviços na rede corporativa e na internet.

Art. 46. O monitoramento dos ativos de TI da rede corporativa poderá ser utilizado para fins de segurança e controle disciplinar, quando for o caso.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 47. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvindo-se, previamente, o Comitê Gestor de Segurança da Informação (CGSI) do TRE-GO.

Art. 48. Esta norma complementar deve ser revisada a cada 24 (vinte e quatro) meses, ou a qualquer tempo, conforme necessidade.

Art. 49. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria DG nº 78/2022.

HUMBERTO VILANI

Diretor-Geral em substituição

Documento assinado eletronicamente por **HUMBERTO VILANI**, **DIRETOR(A)-GERAL EM SUBSTITUIÇÃO**, em 03/11/2025, às 19:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei4.tre-go.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1247004** e o código CRC **19058E46**.

25.0.000006720-5 1247004v2