Observação: Sessão ordinária Presencial de 23.04.2026 (quinta-feira), às 10h

ATOS DA DIRETORIA-GERAL

PORTARIA

PORTARIA TSE Nº 143 DE 14 DE ABRIL DE 2026.

PUBLICAÇÃO EM : 17/04/2026

Institui norma sobre o uso de *software* e de serviços de computação em nuvem do Tribunal Superior Eleitoral.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, no uso das suas atribuições,

CONSIDERANDO a Resolução CNJ 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), e a Portaria CNJ 162/2021, que aprova Protocolos e Manuais criados pela citada Resolução;

CONSIDERANDO a Resolução TSE nº 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TSE nº 23.650, de 9 de setembro de 2021, que institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;

CONSIDERANDO a Portaria TSE nº 784, de 20 de outubro de 2017, que dispõe sobre a Política de Gestão de Riscos do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001:2022, ABNT NBR ISO/IEC 27002:2022, ABNT ISO/IEC 27017:2016, ABNT ISO/IEC 27018:2021, ABNT ISO/IEC 27701:2026 e ABNT ISO/IEC 22237-1:2023;

CONSIDERANDO a Portaria TSE nº 4, de 7 de janeiro de 2022, que regulamenta o procedimento de Demanda de Soluções de Software; e

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços eleitorais, jurisdicionais e administrativos do Tribunal Superior Eleitoral;

RESOLVE

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a norma de uso de *software* e de serviços de computação em nuvem, 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.

Parágrafo único. A Secretaria de Tecnologia da Informação (STI) manterá, como complemento a este normativo, referencial específico de termos técnicos relacionados a computação em nuvem e operacionalização de serviços, no qual se inclui:

I - modelagem de nuvem;

II - modelos de serviço em nuvem;

III - classificação de criticidade operacional e de dados, com respectivos objetivos de disponibilidade, tempo de recuperação e ponto de recuperação;

IV - métricas operacionais de continuidade e observabilidade;

V - conceitos técnicos especializados de governança de nuvem.

§ 1º Esse referencial será publicado como Glossário Técnico de Nuvem pela STI no primeiro ano de vigência e atualizado conforme evolução de práticas, sem necessidade de alteração deste normativo.

§ 2º O glossário será acessível a todas as unidades demandantes do TSE, sendo sua adoção obrigatória para contratações, especificações técnicas e documentação de requisitos relacionados a nuvem.

Art. 3º Este normativo tem como objetivo estabelecer diretrizes para a seleção de ambientes de execução de demandas computacionais do TSE, entre as opções de seu próprio ambiente de tecnologia da informação e de nuvens comunitárias ou públicas, assim como estabelecer diretrizes de segurança da informação para a execução dessas demandas em serviços ou ambientes de computação em nuvem.

Art. 4º Esta norma é obrigatória para todos os casos de utilização de *software* e serviços em nuvem por parte do TSE, entre os quais se incluem:

I - *software* como serviço (Software as a Service - SaaS), inclusive aqueles disponibilizados para utilização gratuita;

II - infraestrutura como serviço - (Infrastructure as a Service - IaaS);

III - plataforma como serviço - (Platform as a Service - PaaS);

IV - função como serviço - (Function as a Service - FaaS);

V - *containers* como serviço - (Container as a Service - CaaS);

VI - serviço de operação e gerenciamento de recursos em nuvem, incluindo serviços de migração para a nuvem, integração de serviços em nuvem e serviços locais, e consultoria especializada no tema.

Parágrafo único. Quaisquer exceções às disposições deste normativo deverão ser formalmente justificadas e autorizadas pela STI.

Art. 5º O uso de *software* e de serviços de computação em nuvem no TSE será norteado pelos seguintes princípios e diretrizes:

I - soberania nacional, considerando as salvaguardas necessárias para que sejam identificados e controlados os impactos derivados de eventuais ações por parte de governos ou empresas estrangeiras, incluindo proteção contra legislações estrangeiras que possibilitem acesso compulsório a dados;

II - segurança da informação, considerando, no mínimo, os requisitos de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio das informações armazenadas e processadas em nuvem;

III - proteção de dados pessoais, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 (LGPD);

IV - adequação dos recursos de processamento e armazenamento em nuvem aos requisitos da demanda, incluindo as previsões de incremento ou decremento desses requisitos ao longo do tempo, com revisão periódica para otimização contínua;

V - melhor relação custo/benefício, consideradas as diversas opções de *softwares* e serviços em nuvem, bem assim as opções de atendimento da demanda por meio de *softwares* e serviços operacionalizados nas instalações de TI do próprio TSE;

VI - análise estruturada de custo total de propriedade para decisões de médio ou longo prazo, aceitando-se, quando não for possível a comparação de custos por meio de critérios objetivos, o parecer técnico que demonstre a inviabilidade de uso dos *softwares* ou serviços operacionalizados nas instalações do próprio TSE, desde que necessidades específicas, agudas e temporárias assim o justifiquem;

VII - priorização de soluções que viabilizem a evolução tecnológica constante, assim como inovação ao longo de seus ciclos de vida, e promovam economia de custos, escalabilidade e melhor alocação de recursos;
VIII - continuidade dos serviços, com objetivos claros de disponibilidade, tempo de recuperação e ponto de recuperação definidos conforme criticidade de cada demanda;
IX - eficiência operacional através de monitoramento contínuo, observabilidade avançada e automação de controles de segurança, reduzindo-se sobrecarga manual.

CAPÍTULO II

DOS REQUISITOS PARA A SELEÇÃO DO AMBIENTE DE EXECUÇÃO DAS DEMANDAS COMPUTACIONAIS

Art. 6º As unidades requisitantes de soluções de tecnologia da informação devem formalizar suas demandas por meio dos procedimentos institucionais vigentes para solicitação de soluções e serviços de tecnologia da informação.
Art. 7º A partir dos requisitos definidos no formulário de Demanda de Solução ou Serviço de TI (DSS), a STI realizará análise estruturada para determinar o melhor ambiente de execução da demanda, considerando:
I - os princípios e as diretrizes definidos no art. 5º;
II - a matriz de decisão que considere: padrão de utilização (previsível, variável, sazonal), criticidade, classificação de dados, maturidade organizacional, requisitos de latência, escalabilidade esperada, conformidade regulatória e modelo financeiro preferido;
III - a análise de custo total de propriedade para horizonte mínimo de três anos;
IV - a avaliação de portabilidade e risco de dependência de fornecedor;
V - a recomendação estruturada com justificativa documentada.
§ 1º Sempre que necessário, a STI irá consultar as unidades demandantes para dirimir dúvidas ou complementar os requisitos relativos à demanda;
§ 2º A análise da demanda deverá ser acompanhada de análise de riscos de segurança da informação, realizada de acordo com as diretrizes e procedimentos definidos na Política de Gestão de Riscos do TSE, instituída pela Portaria nº 784, de 20 de outubro de 2017, e procedimentos a ela subordinados, englobando-se os princípios e diretrizes constantes do art. 5º, inciso II.
§ 3º No caso de indicação da utilização de ambiente de nuvem comunitária ou pública por parte da STI, a documentação relativa à análise da demanda, conforme os princípios relacionados no art. 5º deste normativo, deverá ser formalizada e, caso necessite de nova contratação, será utilizada como insumo na instrução do processo de contratação dos respectivos serviços em nuvem;
§ 4º No caso de indicação da utilização do próprio ambiente de tecnologia da informação do TSE, a documentação de que trata o parágrafo 3º é dispensada.
Art. 8º A identificação das necessidades de negócio deve ser realizada como parte da avaliação do melhor ambiente para execução da demanda computacional. Caso seja necessária nova contratação, os artefatos de planejamento devem conter os seguintes elementos:
I - descrição da demanda e resultados esperados;
II - diagnóstico da situação atual;
III - requisitos da solução desejada;
IV - classificação de criticidade e respectivos objetivos de acordo de nível de serviço, objetivo de tempo de recuperação e objetivo de ponto de recuperação;
V - classificação de dados quanto a confidencialidade, sensibilidade, conformidade e impacto institucional;
VI - requisitos de segurança da informação;
VII - parâmetros legais, regulatórios e de conformidade vigentes;
VIII - avaliação técnica de viabilidade, portabilidade e risco de dependência;

IX - estimativa de custo total (investimento inicial, custos recorrentes, custos de transição);
X - análise de riscos (de segurança da informação, operacional, financeiro, de conformidade);
XI - requisitos de continuidade, incluindo *backup*, recuperação de desastres e replicação de dados quando aplicável;
XII - sistema de classificação de dados estruturado, com quatro níveis:
a) PÚBLICO: dados sem restrição de acesso (publicações oficiais, editais);
b) INTERNO: dados de uso corporativo sem sensibilidade (*e-mails* funcionais, documentos administrativos ordinários);
c) CONFIDENCIAL: dados sensíveis institucionais ou dados pessoais não sensíveis conforme a LGPD (CPF, endereço, processos em andamento);
d) SIGILOSO: dados estratégicos, segredo de justiça, dados pessoais sensíveis conforme a LGPD (origem racial, saúde, biometria), informações classificadas (Resolução TSE nº 23.435, de 5 de fevereiro de 2015);
§ 1º A classificação deve ser:
I - atribuída pelo demandante no momento da DSS com orientação da STI;
II - validada pela STI antes de aprovação de ambiente em nuvem;
III - revisada anualmente ou quando houver mudança na natureza dos dados;
IV - documentada formalmente e vinculada aos requisitos de segurança correspondentes (criptografia, controle de acesso, *backup*, auditoria);
§ 2º Os elementos dos incisos VI a XI poderão ser delegados à STI caso o demandante não possua habilidade técnica específica.
Art. 9º A STI deve selecionar o tipo de *software* e serviço de computação em nuvem mais adequado entre as opções de IaaS, PaaS, SaaS, FaaS, CaaS e outras variantes que se apresentem, considerando no mínimo:
I - identificação das necessidades de negócio de que trata o art. 8º;
II - interoperabilidade com o ambiente de TI do TSE e com outros serviços externos eventualmente necessários ao atendimento da demanda;
III - portabilidade do serviço, dados e aplicações para outros ambientes (nuvem pública, comunitária ou *on-premise*) com avaliação de custos e cronograma de migração;
IV - estratégia de retorno do atendimento à demanda por meio do ambiente de TI do TSE, diminuindo-se o risco de dependência de fornecedor, ou justificativa para manutenção dos serviços em nuvem por tempo indeterminado, acompanhada de estratégia de dimensionamento de recursos com vistas à elasticidade e à consequente otimização de custos;
V - capacitação da equipe;
VI - capacidades de observabilidade, monitoramento e automação do serviço;
VII - conformidade com requisitos de segurança, com a LGPD e com os demais marcos regulatórios;
VIII - especificações técnicas e requisitos de desempenho (latência, taxa de transferência, disponibilidade);
IX - estimativa de custo total de propriedade com horizonte mínimo de três anos, incluindo custos de implementação, operação e migração;
X - análise de dimensionamento adequado e potencial de redução de custos ao longo do tempo;
XI - capacidades de escalabilidade automática conforme padrão de demanda;
XII - modelo de precificação transparente e previsível, com cláusulas de proteção contra aumentos abruptos.
Parágrafo único. A seleção de que trata o *caput* deste artigo deve ser feita com o apoio das áreas demandantes.

Art. 10. As demandas que tratem as informações com restrição de acesso constantes da Resolução TSE nº 23.435/2015, os dados pessoais sensíveis ou os dados estratégicos institucionais deverão, preferencialmente, utilizar ambientes de nuvem de governo, salvo autorização expressa e fundamentada da STI.

Art. 11. Não é recomendado o tratamento em ambiente de nuvem pública ou comunitária de:

I - informações classificadas em grau de sigilo nos termos da Resolução TSE nº 23.435/2015; e

II - documentos preparatórios que possam originar tais informações, sempre que seja possível a identificação prévia.

Art. 12. As demandas que tratem informações sem restrição de acesso podem ser alocadas em ambientes de nuvem pública ou comunitária, desde que seja garantido:

I - o cumprimento das regras de proteção de dados pessoais definidos na Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral, instituída pela Resolução TSE nº 23.650/2021; e

II - o cumprimento dos requisitos de segurança da informação definidos na Política de Segurança da Informação da Justiça Eleitoral, instituída por meio da Resolução TSE nº 23.644/2021, e das normas de nível tático a ela subordinadas, publicadas por portarias específicas.

Art. 13. A não implementação dos requisitos de segurança previstos no art. 12 somente poderá ocorrer:

I - após a realização de avaliação de risco específica e justificativa técnica registrada em documento formal; e

II - quando autorizada pela STI.

Art. 14. Os dados tratados em *software* e serviços de computação em nuvem deverão, preferencialmente, ser armazenados em território nacional, observados os princípios da soberania, segurança da informação e continuidade dos serviços.

§ 1º O armazenamento persistente de dados fora do território nacional somente poderá ocorrer quando forem observadas as seguintes condições:

I - elaboração de avaliação de risco específica e autorização da STI, observados critérios de equivalência regulatória, contratual e de proteção de dados.

II - manutenção de pelo menos uma cópia de segurança atualizada dos dados em território nacional;

III - garantia do cumprimento das disposições da Lei nº 13.853/2019, no caso de haver tratamento de dados pessoais.

§ 2º O termo de referência das contratações de *software* e serviços de computação em nuvem, ou a ordem de serviço de contrato de *broker* de nuvem já existente, deve estabelecer a obrigação do fornecedor de indicar a região em que os dados estão armazenados, em conformidade com as regras estabelecidas neste normativo.

Art. 15. Antes do início do uso de um novo *software* ou serviço de computação em nuvem, a STI, com o apoio das áreas solicitantes da solução, deve realizar análise técnica prévia para homologação do cumprimento dos requisitos mínimos de segurança da informação, incluindo ao menos criptografia, controle de acessos, registro de *logs* e gestão de vulnerabilidades, desde que aplicáveis.

CAPÍTULO III

DO DIMENSIONAMENTO E MONITORAMENTO DOS RECURSOS DE NUVEM

Art. 16. A STI, na fase de planejamento da contratação de *software* e de serviço de computação em nuvem, deve:

I - indicar as condições mínimas de infraestrutura de tecnologia da informação e comunicação do ambiente de nuvem necessárias para a utilização do *software* ou serviço a ser contratado;

II - estabelecer os parâmetros mínimos para comunicações seguras e estáveis em ambientes de nuvem, seguindo diretrizes de órgãos de referência;
III - estabelecer níveis mínimos de disponibilidade e desempenho da conexão e dos serviços prestados em nuvem, com métricas claras definidas e acompanhadas em periodicidade definida;
IV - definir os requisitos relativos à execução de cópias de segurança (*backup*) dos dados, configurações e demais informações envolvidas na utilização do *software* ou serviço de computação em nuvem;
V - implementar soluções redundantes para garantir continuidade dos serviços em caso de falhas no ambiente de nuvem principal;
VI - definir as funcionalidades de monitoramento do ambiente de nuvem que devem ser disponibilizadas pela contratada ou pelo provedor de nuvem;
VII - definir os parâmetros mínimos de qualidade do serviço de suporte técnico a ser prestado pela contratada;
VIII - definir os requisitos de capacitação das equipes envolvidas na utilização do *software* ou do serviço de computação em nuvem;
IX - definir as certificações e práticas de sustentabilidade a serem cumpridas pela contratada.
§ 1º As condições mínimas de infraestrutura e de segurança para o uso de *softwares* e serviços de computação em nuvem devem ser consolidadas no estudo técnico preliminar que compõe o processo de contratação.
§ 2º O disposto neste artigo aplica-se também a soluções cujo plano de controle, console administrativo ou gerenciamento seja provido no formato *software* como serviço (SaaS).
Art. 17. No monitoramento das condições mínimas de infraestrutura de tecnologia da informação e comunicação, a STI deve adotar, no mínimo, as seguintes práticas:
I - utilização de ferramentas de monitoramento para medir os recursos computacionais envolvidos no uso dos *softwares* e serviços em nuvem, identificar pontos de melhorias e planejar as ações necessárias para sua implementação;
II - uso de ferramentas de monitoramento financeiro da utilização dos serviços contratados, atuando tempestivamente com relação à maximização da eficiência do consumo e do ajuste da execução perante os limites contratuais.
CAPÍTULO IV
DAS RESPONSABILIDADES
Art. 18. Em todos os casos de utilização de *software* ou serviços em nuvem comunitária ou pública deverão ser formalmente estabelecidas as responsabilidades relacionadas à segurança para cada uma das partes envolvidas: TSE, empresa contratada para o fornecimento do *software* ou serviço (*broker*) e provedor efetivo dos serviços e *software* em nuvem;
Parágrafo único. A efetiva observância das responsabilidades de cada parte deverá ser verificada pela STI em intervalos regulares não superiores a um ano.
Art. 19. A STI deve adotar os seguintes controles de segurança relativos aos serviços de computação em nuvem utilizados pelo TSE:
I - manter inventário de cada um dos provedores de serviços de nuvem contratados, incluindo as modalidades de IaaS, PaaS e SaaS;
II - manter inventário de serviços autorizados para uso em cada provedor de serviços em nuvem contratado;
III - manter inventário das contas autorizadas para uso em cada um dos provedores de serviços de nuvem autorizados;
IV - manter um padrão de configuração de cibersegurança para cada um dos provedores de serviços de nuvem contratados;

V - manter um *benchmark* de configuração de cibersegurança para os serviços com uso autorizado em cada um dos provedores de serviços de nuvem contratados e de seus respectivos serviços;
VI - manter um sistema de gerenciamento de vulnerabilidades de configuração em nuvem para verificar regularmente cada um dos provedores de serviços em nuvem contratados e de seus serviços;
VII - garantir que os *logs* apropriados dos provedores de serviços em nuvem contratados estejam habilitados na plataforma;
VIII - garantir a integração dos *logs* ao sistema corporativo de gestão de *logs* ou, enquanto indisponível, sua retenção controlada pela STI;
IX - implantar outros controles de segurança que se façam necessários para atender à Política de Segurança da Informação e suas normas táticas.
Art. 20. As unidades demandantes de serviços e *softwares* disponibilizados em nuvem pública ou comunitária deverão observar e respeitar os requisitos de segurança definidos pela Política de Segurança da Informação da Justiça Eleitoral e seus normativos táticos, assim como os controles de segurança adotados pela STI em atendimento a esses normativos.
Art. 21. Os contratos para prestação de serviços de processamento, armazenamento de dados e computação em nuvem devem conter cláusulas que garantam:
I - a propriedade dos dados pelo TSE;
II - a obrigação da contratada de excluir os dados de seus ambientes após o término do contrato e apresentar uma comprovação da exclusão;
III - a transferência dos dados para eventual nova contratada ou para o TSE em caso de extinção contratual em formato aberto, estruturado e interoperável, garantindo a integridade e a legibilidade das informações;
IV - a obrigação de assinatura de termo de confidencialidade institucional pela empresa contratada;
V - a necessidade de termo individual de responsabilidade, compromisso de manutenção e sigilo de dados por parte de todos os funcionários da contratada que tenham acesso a dados do TSE;
VI - a não utilização dos dados para qualquer finalidade de interesse exclusivo da contratada, sem autorização prévia e explícita do TSE;
VII - os mecanismos contratuais de auditoria e sanções para o caso de descumprimento dessas cláusulas;
Art. 22. A contratada deve estabelecer plano de ação e resposta a incidentes integrado ao processo institucional de tratamento de incidentes de cibersegurança do TSE, contemplando, no mínimo:
I - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes;
II - a área responsável pelo registro e controle dos efeitos de incidentes relevantes, incluindo suas informações de contato;
III - os prazos de notificação e comunicação imediata à STI;
IV - a cooperação durante o tratamento do incidente.
Parágrafo único. A STI deverá avaliar se o plano de que trata o *caput* é adequado ao correto tratamento de incidentes e solicitar à contratada eventuais melhorias.
CAPÍTULO V
DISPOSIÇÕES FINAIS
Art. 23. Os *softwares* e serviços de computação em nuvem contratados ou implantados anteriormente à publicação deste normativo devem ser avaliados quanto a sua conformidade com as regras aqui estabelecidas.

§ 1º A STI deverá elaborar, no prazo de até um ano contado da entrada em vigor deste normativo, plano de adequação dos serviços em operação, priorizando aqueles que representem maior risco ou que suportem processos de negócio estratégicos.
§ 2º Durante o período de transição, os serviços existentes poderão continuar em funcionamento, desde que não apresentem alto risco à segurança da informação, à conformidade legal ou à continuidade das operações institucionais.
Art. 24. A revisão deste normativo ocorrerá a cada três anos ou sempre que se fizer necessária ou conveniente para o TSE.
Art. 25. Este normativo entra em vigor na data de sua publicação.
MIGUEL RICARDO DE OLIVEIRA PIAZZI

COORDENADORIA DE REGISTROS PARTIDÁRIOS, AUTUAÇÃO E DISTRIBUIÇÃO

ATA DE DISTRIBUIÇÃO

PROCESSOS DISTRIBUÍDOS E REDISTRIBUÍDOS NO TSE EM 15/04/2026.

PUBLICAÇÃO EM : 17/04/2026

RECURSO ESPECIAL ELEITORAL Nº 0600124-34.2025.6.15.0000
Origem:
RIACHO DOS CAVALOS-PB
Partes:
RECORRENTE : MINISTÉRIO PÚBLICO ELEITORAL
RECORRIDO : RAILTON CARDOSO DA COSTA
ADVOGADO(A) : ANTONIO EUDES NUNES DA COSTA FILHO
ADVOGADO(A) : FRANCISCO ASSIS FIDELIS DE OLIVEIRA FILHO
ADVOGADO(A) : HARRISON ALEXANDRE TARGINO
ADVOGADO(A) : JESSICA DAYSE FERNANDES MONTEIRO
ADVOGADO(A) : NEWTON NOBEL SOBREIRA VITA
RECORRIDO : RODOLFO CAMPOS DA COSTA
ADVOGADO(A) : ANTONIO EUDES NUNES DA COSTA FILHO
ADVOGADO(A) : FRANCISCO ASSIS FIDELIS DE OLIVEIRA FILHO
ADVOGADO(A) : JESSICA DAYSE FERNANDES MONTEIRO
ADVOGADO(A) : NEWTON NOBEL SOBREIRA VITA
FISCAL DA LEI : PROCURADOR GERAL ELEITORAL
Relatora:
ESTELA ARANHA
Distribuição:
REDISTRIBUÍDO EM 15/04/2026 15:04:14

MANDADO DE SEGURANÇA CÍVEL Nº 0600687-11.2026.6.00.0000
Origem:
BRASÍLIA-DF
Partes:
IMPETRANTE : RAIMUNDO NONATO COELHO PEREIRA
ADVOGADO(A) : WILLIAN VITOR COSTA FURTADO