Boletim SEI - TRE/RN em 06/07/2026
DJe de 06/07/2026, seção única, página 24-35

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

RESOLUÇÃO Nº 180/2026

Dispõe sobre a Política e o Programa de Tratamento e Proteção de Dados Pessoais no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE-RN), revoga as Resoluções TRE-RN n.ºs 48/2021 e 148/2025, e dá outras providências.

O TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo art. 20, inciso XIX, de seu Regimento Interno,

Considerando a Constituição da República Federativa do Brasil, especialmente os direitos fundamentais à intimidade, à vida privada, à honra, à imagem e à proteção de dados pessoais;

Considerando a Lei n.º 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado;

Considerando a Lei n.º 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI), que regula o acesso a informações previsto na Constituição Federal;

Considerando a Recomendação n.º 73, de 20 de agosto de 2020, e a Resolução n.º 363, de 12 de janeiro de 2021, do Conselho Nacional de Justiça, que dispõem sobre medidas preparatórias e ações de adequação dos órgãos do Poder Judiciário à Lei Geral de Proteção de Dados Pessoais (LGPD), respectivamente;

Considerando a Resolução n.º 23.650, de 30 de agosto de 2021, do Tribunal Superior Eleitoral (TSE), que institui a Política de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral e estabelece diretrizes para o tratamento de dados pessoais pelos órgãos eleitorais;

Considerando a Resolução TRE-RN n.º 48, de 15 de dezembro de 2021, que institui a Política de Tratamento e Proteção de Dados Pessoais no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

Considerando o Acórdão n.º 1.372, de 25 de junho de 2025, do Plenário do Tribunal de Contas da União (TCU), que identificou oportunidades de melhoria relacionadas à governança, à gestão de riscos, à transparência e à conformidade no tratamento de dados pessoais pelas organizações públicas, recomendando o aperfeiçoamento contínuo das medidas de adequação à LGPD;

Considerando a necessidade de fortalecimento da governança institucional em proteção de dados pessoais, em consonância com as diretrizes da Justiça Eleitoral, da Agência Nacional de Proteção de Dados (ANPD) e das boas práticas de segurança da informação, gestão documental

e gestão de riscos;

Considerando que a Assessoria de Integração (ASSINT) constitui a unidade técnica competente para coordenar, orientar e acompanhar as ações relacionadas à proteção de dados pessoais no âmbito do Tribunal;

Considerando o inteiro teor do SEI nº 03681/2026 (PJe nº 0600212-97.2026.6.20.0000),

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução institui a Política e o Programa de Tratamento e Proteção de Dados Pessoais no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE-RN), estabelecendo princípios, diretrizes, mecanismos de governança, instrumentos de conformidade e medidas voltadas à proteção de dados pessoais.

§ 1º A Política de Tratamento e Proteção de Dados Pessoais constitui o instrumento estratégico-normativo destinado ao estabelecimento dos princípios, diretrizes, responsabilidades e mecanismos gerais relacionados à proteção de dados pessoais no âmbito do Tribunal.

§ 2º O Programa de Tratamento e Proteção de Dados Pessoais constitui instrumento estruturante destinado à implementação, monitoramento, aperfeiçoamento contínuo e acompanhamento das ações institucionais relacionadas à proteção de dados pessoais, operacionalizadas por meio de Plano de Ação.

§ 3º O Plano de Ação de Proteção de Dados Pessoais constitui instrumento executivo vinculado ao Programa, destinado à definição das ações, metas, prioridades, cronogramas e mecanismos de acompanhamento das iniciativas institucionais relacionadas à proteção de dados pessoais.

Art. 2º Para os fins desta Resolução, consideram-se:

I – Agentes de tratamento: o Controlador e o Operador de Dados Pessoais, conforme definidos na legislação aplicável.

II – Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um(a) titular.

III – Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da legislação de proteção de dados pessoais no Brasil.

IV – Ciclo de vida dos dados pessoais: conjunto de fases pelas quais os dados pessoais passam ao longo de seu tratamento, compreendendo, entre outras, a coleta, o uso, o armazenamento, o compartilhamento e a eliminação, devendo cada etapa observar as disposições desta Política e as medidas de segurança e governança aplicáveis.

V – Controlador: pessoa natural ou jurídica, de direito público ou privado, no caso o TRE-RN (representado pelo(a) titular da Presidência), a quem competem as decisões referentes ao tratamento de dados pessoais, como finalidade, meios e diretrizes do tratamento. Servidores(as), magistrados(as), estagiários(as) e colaboradores(as) atuam funcionalmente em nome do próprio Controlador.

VI – Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

VII – Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

VIII – Encarregado(a): pessoa indicada pelo Controlador para atuar como canal de comunicação entre aquele, os(as) titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

IX – Incidente de segurança com dados pessoais: qualquer evento adverso, confirmado ou sob suspeita, que comprometa a confidencialidade, a integridade ou a disponibilidade de dados pessoais, tais como acessos não autorizados, vazamentos, perda, destruição ou alteração indevida de dados.

X – Mascaramento de dados: técnica de ocultação parcial de dados pessoais, com a finalidade de reduzir riscos de identificação indevida, especialmente em ambientes de teste, compartilhamento ou divulgação restrita.

XI – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador. *Exemplo:* empresa contratada para fornecer sistema informatizado, armazenamento em nuvem, suporte técnico, digitalização documental ou outra solução tecnológica que envolva tratamento de dados pessoais para o Tribunal.

XII – Pseudonimização: tratamento por meio do qual um dado pessoal perde a possibilidade de associação direta a um(a) titular, mantendo-se, porém, a possibilidade de reidentificação mediante uso de informação adicional separada e protegida, podendo envolver técnicas como mascaramento, tarjamento ou substituição de identificadores.

XIII – Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

XIV – Tarjamento: técnica de supressão visual de informações pessoais em documentos, de forma a impedir sua leitura ou identificação, comumente utilizada em processos administrativos ou judiciais.

XV – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

XVI – Tokenização: técnica de proteção de dados pessoais que consiste na substituição de elementos sensíveis por identificadores artificiais (*tokens*), sem valor intrínseco ou significado fora do sistema que os gerou, sendo o dado original armazenado de forma segregada e segura, com possibilidade de reversão apenas mediante mecanismos controlados e autorizados.

XVII – Tratamento de dados pessoais: toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.

Art. 3º O tratamento de dados pessoais no âmbito do Tribunal observará:

I – a legislação aplicável à proteção de dados pessoais;

II – as diretrizes expedidas pela Agência Nacional de Proteção de Dados (ANPD), pelo Conselho Nacional de Justiça (CNJ), pelo Tribunal Superior Eleitoral (TSE) e pelos órgãos de controle, no âmbito de suas competências;

III – as normas institucionais relacionadas à segurança da informação, gestão documental, gestão de riscos, governança, transparência e integridade;

IV – os direitos e garantias fundamentais relacionados à privacidade, à intimidade, à autodeterminação informativa e à proteção de dados pessoais.

Art. 4º As disposições desta Resolução aplicam-se às unidades administrativas e cartórios eleitorais do Tribunal, bem como aos(às) magistrados(as), servidores(as), estagiários(as), colaboradores(as), prestadores(as) de serviço e demais agentes que realizem operações de tratamento de dados pessoais em nome do Tribunal.

CAPÍTULO II

DA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Seção I

Dos Objetivos, Princípios e Diretrizes

Art. 5º Constituem objetivos desta Política:

I – promover a proteção dos dados pessoais tratados pelo Tribunal;

II – assegurar o respeito à privacidade e aos direitos dos(as) titulares;

III – fortalecer a governança institucional em proteção de dados pessoais;

IV – estabelecer mecanismos de conformidade com a legislação aplicável;

V – promover a transparência e a responsabilização no tratamento de dados pessoais;

VI – incentivar a cultura institucional de proteção de dados pessoais.

Art. 6º O tratamento de dados pessoais no âmbito do Tribunal observará a boa-fé, os princípios previstos na legislação aplicável e as diretrizes institucionais de governança, segurança da informação, gestão de riscos, transparência e proteção da privacidade, especialmente:

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao(à) titular;

II – adequação: compatibilidade do tratamento com as finalidades informadas;

III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades;

IV – livre acesso: garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento;

V – qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados pessoais;

VI – transparência: fornecimento de informações claras, precisas e acessíveis sobre o tratamento realizado;

VII – segurança: adoção de medidas técnicas e administrativas aptas à proteção dos dados pessoais;

VIII – prevenção: adoção de medidas destinadas à prevenção da ocorrência de danos;

IX – não discriminação: vedação à realização de tratamento para fins discriminatórios, ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração da adoção de medidas eficazes e capazes de comprovar a observância das normas de proteção de dados pessoais.

Art. 7º Constituem diretrizes desta Política:

I – promover a proteção dos dados pessoais ao longo de todo o seu ciclo de vida;

II – assegurar a integração entre proteção de dados pessoais, segurança da informação, gestão documental e gestão de riscos;

III – estimular a adoção de medidas preventivas e corretivas voltadas à mitigação de riscos relacionados ao tratamento de dados pessoais;

IV – promover a transparência e o adequado atendimento aos(às) titulares;

V – assegurar a rastreabilidade das operações de tratamento de dados pessoais;

VI – incentivar a adoção de soluções e processos estruturados segundo os conceitos de privacidade desde a concepção (*Privacy by Design*) e privacidade por padrão;

VII – promover a capacitação e conscientização contínuas acerca da proteção de dados pessoais;

VIII – promover o monitoramento contínuo da conformidade institucional em proteção de dados pessoais, observadas as orientações, recomendações e boas práticas aplicáveis à Administração Pública e ao Poder Judiciário;

IX – fortalecer os mecanismos de governança, monitoramento e melhoria contínua relacionados à proteção de dados pessoais;

X – promover a atualização contínua do Programa de Tratamento e Proteção de Dados Pessoais (PTDP), dos planos de ação, dos instrumentos de governança e dos mecanismos institucionais de conformidade, observadas as diretrizes dos órgãos direcionadores e de controle e o nível de maturidade institucional alcançado pelo Tribunal.

Art. 8º O tratamento de dados pessoais de crianças e adolescentes observará o disposto no art. 14 da Lei Geral de Proteção de Dados Pessoais (LGPD), devendo ser realizado em seu

melhor interesse, com observância das orientações, guias e diretrizes expedidos pela Agência Nacional de Proteção de Dados (ANPD).

Parágrafo único. O Tribunal adotará medidas proporcionais destinadas à proteção reforçada dos dados pessoais de crianças e adolescentes, consideradas a natureza do tratamento, os riscos envolvidos e a vulnerabilidade dos(as) titulares.

Seção II

Da Governança e das Responsabilidades

Art. 9º O Tribunal manterá estrutura organizacional voltada à governança, à conformidade e à proteção de dados pessoais, integrada pelas unidades administrativas e cartórios eleitorais que, em razão de suas competências institucionais, realizem operações de tratamento de dados pessoais ao longo de seu ciclo de vida.

§ 1º As unidades administrativas e cartórios eleitorais responsáveis pelo tratamento de dados pessoais deverão adotar medidas destinadas à conformidade com esta Política, incluindo ações relacionadas à identificação, ao mapeamento, à atualização, à classificação, à proteção e ao adequado descarte das informações sob sua responsabilidade.

§ 2º O mapeamento das operações de tratamento de dados pessoais será realizado pelas unidades responsáveis pelo tratamento, sob orientação metodológica da ASSINT.

§ 3º O mapeamento de que trata o § 2º deverá contemplar o registro estruturado das atividades realizadas pelas unidades administrativas e cartórios eleitorais, incluindo, no mínimo:

I – a finalidade do tratamento;

II – a categoria dos dados pessoais tratados;

III – a identificação dos agentes de tratamento envolvidos;

IV – a base legal que fundamenta o tratamento;

V – o fluxo de compartilhamento de dados, quando existente;

VI – as medidas de segurança adotadas;

VII – os prazos de retenção dos dados pessoais.

Art. 10. Compete ao Tribunal, por meio de suas unidades e estruturas de governança:

I – promover a conformidade institucional com a legislação aplicável à proteção de dados pessoais;

II – adotar medidas técnicas e administrativas destinadas à proteção dos dados pessoais;

III – assegurar a atuação do(a) Encarregado(a) pelo tratamento de dados pessoais, nos termos da legislação aplicável;

IV – implementar mecanismos de monitoramento, controle e gestão de riscos relacionados ao tratamento de dados pessoais;

V – promover ações de transparência, orientação e atendimento aos(às) titulares dos dados pessoais;

VI – atuar de forma coordenada com as Comissões Permanentes de Segurança da Informação (CPSI) e de Avaliação Documental (CPAD), observadas as competências institucionais correlatas;

VII – observar as diretrizes da Política de Segurança da Informação da Justiça Eleitoral e as demais normas institucionais aplicáveis;

VIII – elaborar relatórios periódicos relacionados às ações de proteção de dados pessoais e às medidas de governança implementadas;

IX – promover ações contínuas de conscientização, capacitação e disseminação da cultura de proteção de dados pessoais entre magistrados(as), servidores(as), estagiários(as), colaboradores(as) e demais agentes que atuem no Tribunal, inclusive mediante trilhas de aprendizagem, campanhas educativas, materiais orientativos e outras iniciativas correlatas.

§ 1º A ASSINT atuará como unidade técnica especializada e ponto focal institucional em proteção de dados pessoais, competindo-lhe coordenar, orientar, acompanhar e apoiar as ações relacionadas ao tratamento e à proteção de dados pessoais no âmbito do Tribunal.

§ 2º O Tribunal manterá Grupo de Trabalho Técnico destinado a apoiar as ações relacionadas à proteção de dados pessoais, especialmente quanto à governança, conformidade, segurança da informação, gestão de riscos e aperfeiçoamento dos mecanismos institucionais de proteção de dados.

Art. 11. Os(as) agentes de tratamento deverão atuar em conformidade com a legislação aplicável, observando os princípios, diretrizes e mecanismos estabelecidos nesta Política.

§ 1º O Tribunal atuará como Controlador dos dados pessoais tratados no exercício de suas competências institucionais.

§ 2º O Operador realizará o tratamento de dados pessoais em nome do Controlador, observadas as instruções fornecidas e as disposições legais aplicáveis.

§ 3º O(a) Encarregado(a) atuará como canal de comunicação entre o Tribunal, os(as) titulares dos dados pessoais e a ANPD, observadas as atribuições previstas na legislação aplicável.

§ 4º Caso o(a) Encarregado(a) seja designado(a) dentre servidores(as) lotados(as) em unidade diversa da ASSINT, sua atuação deverá ocorrer de forma integrada com essa unidade, observada a coordenação institucional das ações relacionadas à proteção de dados pessoais no âmbito do Tribunal.

§ 5º Os(as) agentes de tratamento deverão observar, no desempenho de suas atribuições, os princípios da necessidade, segurança e responsabilização, asseguradas a minimização de dados pessoais e a rastreabilidade das operações de tratamento, mantendo registros e evidências das operações realizadas, sempre que exigido pelas normas aplicáveis ou pelos mecanismos institucionais de governança.

§ 6º O tratamento irregular de dados pessoais poderá ensejar responsabilização administrativa, civil e penal, nos termos da legislação aplicável.

Seção III

Do Tratamento de Dados Pessoais

Art. 12. No âmbito do Tribunal, o tratamento de dados pessoais deverá estar fundamentado em base legal válida, observadas, especialmente, as hipóteses de cumprimento de obrigação legal ou regulatória, execução de políticas públicas, exercício regular de direitos, execução de competências legais e demais hipóteses previstas na legislação aplicável.

Art. 13. O tratamento de dados pessoais deverá observar medidas técnicas, administrativas e organizacionais adequadas à proteção dos dados pessoais durante todo o seu ciclo de vida, especialmente nas fases de:

I – coleta: obtenção dos dados pessoais necessários ao atendimento da finalidade institucional, observados os princípios aplicáveis;

II – uso e processamento: realização das operações de tratamento compatíveis com as competências legais e institucionais do Tribunal;

III – armazenamento e retenção: manutenção dos dados pessoais em ambiente seguro, pelo período necessário ao cumprimento das finalidades do tratamento e das exigências legais e institucionais aplicáveis;

IV – compartilhamento: transmissão, comunicação ou disponibilização de dados pessoais, observadas as hipóteses legais, a segurança da informação e a finalidade do tratamento;

V – eliminação e descarte: exclusão, anonimização ou eliminação segura dos dados pessoais, observadas as normas aplicáveis.

Parágrafo único. O tratamento de dados pessoais no âmbito do Tribunal deverá observar base legal válida, nos termos da legislação aplicável.

Art. 14. O Tribunal promoverá o aperfeiçoamento de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, observados os padrões de segurança da informação e as diretrizes institucionais aplicáveis, incluindo, entre outras, as seguintes:

I – controles de acesso: implementação de mecanismos que restrinjam o acesso aos dados pessoais aos(às) agentes autorizados(as), conforme a necessidade para o desempenho de suas atribuições;

II – proteção de dados: utilização de técnicas destinadas à redução dos riscos associados ao tratamento de dados pessoais, tais como anonimização, pseudonimização e, quando aplicável, tokenização, podendo incluir procedimentos de mascaramento e tarjamento de informações, especialmente em situações que envolvam maior risco aos(às) titulares;

III – segurança da informação: adoção de medidas voltadas à garantia da confidencialidade, integridade e disponibilidade dos dados pessoais, em consonância com a Política de Segurança da Informação dos órgãos da Justiça Eleitoral;

IV – gestão de riscos: identificação, análise e tratamento de riscos relacionados ao tratamento de dados pessoais, observadas as diretrizes institucionais de gestão de riscos;

V – monitoramento e prevenção: implementação de mecanismos de monitoramento e controle capazes de prevenir, detectar e responder a incidentes de segurança envolvendo dados pessoais;

VI – capacitação e conscientização: promoção de ações contínuas de capacitação e

orientação de magistrados(as), servidores(as), estagiários(as) e colaboradores(as) quanto às boas práticas de proteção de dados pessoais.

Parágrafo único. As medidas previstas neste artigo deverão ser implementadas e continuamente aperfeiçoadas de forma proporcional à natureza dos dados pessoais tratados, à sensibilidade das informações, às finalidades do tratamento e aos riscos envolvidos.

Seção IV

Da Segurança, da Avaliação de Riscos e dos Incidentes de Proteção de Dados Pessoais

Art. 15. O Tribunal elaborará Relatório de Impacto à Proteção de Dados Pessoais (RIPD), sempre que o tratamento de dados pessoais puder gerar riscos relevantes aos(às) titulares, nos termos da legislação vigente e das diretrizes institucionais.

§ 1º O RIPD conterá a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

§ 2º A elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) observará as regras metodológicas de gestão de riscos adotadas pelo Tribunal e considerará, sempre que aplicável:

I – a natureza, a finalidade e o contexto do tratamento de dados pessoais;

II – o volume e a sensibilidade dos dados tratados;

III – o uso de tecnologias emergentes ou automatizadas;

IV – o compartilhamento interinstitucional de dados;

V – a probabilidade e o impacto dos riscos identificados;

VI – os impactos potenciais aos direitos e liberdades dos(as) titulares;

VII – as medidas técnicas, administrativas e institucionais adotadas para mitigação dos riscos.

§ 3º A elaboração do RIPD poderá ser exigida, especialmente, em hipóteses de tratamento de dados em larga escala, tratamento de dados sensíveis, decisões automatizadas com efeitos relevantes, monitoramento sistemático ou compartilhamento significativo de dados pessoais com terceiros.

§ 4º O RIPD será elaborado pela ASSINT com o apoio das unidades responsáveis pelo tratamento dos dados pessoais.

§ 5º O Tribunal manterá registro centralizado dos RIPDs, com vistas ao acompanhamento, à governança e ao aprimoramento contínuo das práticas de proteção de dados pessoais.

Art. 16. No contexto das medidas de segurança, monitoramento, prevenção e gestão de riscos relacionadas ao tratamento de dados pessoais, os incidentes de segurança que possam acarretar risco ou dano relevante aos(às) titulares deverão ser identificados, tratados e comunicados de forma tempestiva, nos termos da legislação vigente.

§ 1º As unidades que identificarem incidente de segurança envolvendo dados pessoais deverão comunicar imediatamente o fato à ASSINT e às áreas responsáveis pela segurança da informação.

§ 2º A ASSINT avaliará a gravidade do incidente e adotará as providências necessárias, inclusive quanto à comunicação ao(à) Controlador(a) e à ANPD, quando cabível.

§ 3º O tratamento de incidentes observará as diretrizes da Política de Segurança da Informação da Justiça Eleitoral e as normas internas do Tribunal, devendo ocorrer de forma coordenada com as Comissões Permanentes de Segurança da Informação (CPSI) e de Avaliação Documental (CPAD) e a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR).

Seção V

Do Compartilhamento e da Transferência de Dados Pessoais

Art. 17. O compartilhamento de dados pessoais pelo Tribunal deverá observar os princípios e as diretrizes estabelecidos nesta Resolução, bem como as disposições da legislação vigente.

§ 1º O compartilhamento de dados pessoais deverá ocorrer mediante justificativa formal, com indicação da finalidade, da base legal e das medidas de proteção adotadas.

§ 2º Sempre que possível, o compartilhamento deverá ser realizado com a utilização de técnicas destinadas à redução dos riscos aos(às) titulares, observadas as medidas de segurança e proteção de dados previstas nesta Resolução.

§ 3º O Tribunal poderá compartilhar dados pessoais com outros órgãos da Justiça Eleitoral, especialmente com o Tribunal Superior Eleitoral e os demais Tribunais Regionais Eleitorais, para o exercício de suas competências legais e institucionais, observadas as normas aplicáveis e os padrões de segurança da informação.

§ 4º O compartilhamento com entidades externas à Justiça Eleitoral deverá observar, além do disposto nesta Resolução, os instrumentos formais aplicáveis, tais como convênios, acordos de cooperação ou outros instrumentos congêneres.

§ 5º O compartilhamento de dados pessoais entre os órgãos da Justiça Eleitoral deverá:

I – observar as finalidades institucionais e o interesse público;

II – ser limitado ao mínimo necessário para o atendimento da finalidade pretendida;

III – assegurar a rastreabilidade das operações realizadas;

IV – adotar medidas de segurança adequadas à proteção dos dados pessoais;

V – observar, sempre que aplicável, os normativos expedidos pelo Tribunal Superior Eleitoral.

Art. 18. A transferência internacional de dados pessoais somente poderá ocorrer nas hipóteses admitidas pela legislação aplicável e pelas diretrizes da ANPD, especialmente mediante decisão de adequação, cláusulas contratuais padrão ou garantias específicas aptas a assegurar a proteção dos dados pessoais e os direitos dos(as) titulares.

Seção VI

Dos Direitos dos(as) Titulares, do Atendimento às Demandas e da Transparência

Art. 19. O Tribunal assegurará aos(às) titulares de dados pessoais o exercício de seus direitos, bem como promoverá a transparência quanto ao tratamento de dados pessoais, nos termos da legislação vigente.

§ 1º Serão disponibilizadas, em meio eletrônico, informações claras, acessíveis e atualizadas sobre o tratamento de dados pessoais realizado pelo Tribunal.

§ 2º As solicitações relacionadas ao tratamento de dados pessoais deverão ser realizadas, preferencialmente, por meio da Ouvidoria Eleitoral, observados os canais institucionais disponíveis, devendo aquelas eventualmente formalizadas por outros meios ser registradas em seu sistema próprio para fins de controle, acompanhamento e resposta.

§ 3º O atendimento às demandas dos(as) titulares seguirá o fluxo estabelecido no Anexo desta Resolução.

§ 4º As unidades responsáveis pelo tratamento dos dados pessoais deverão prestar as informações necessárias ao atendimento das demandas, no prazo e nas condições estabelecidas pela ASSINT.

§ 5º A ASSINT atuará na coordenação do atendimento às demandas, inclusive no relacionamento com a ANPD, quando necessário, sem prejuízo das atribuições do(a) Encarregado(a).

§ 6º O Tribunal manterá página institucional específica sobre proteção de dados pessoais, contendo informações relacionadas à legislação aplicável, atos normativos internos, canais de atendimento, orientações aos(às) titulares, registros de tratamento, materiais educativos e demais instrumentos de transparência ativa relacionados à proteção de dados pessoais.

Art. 20. Os portais, sistemas e aplicações digitais do Tribunal deverão observar boas práticas de transparência e proteção de dados pessoais relacionadas ao uso de cookies e demais tecnologias de rastreamento digital, observadas as diretrizes da Agência Nacional de Proteção de Dados (ANPD) e a legislação aplicável.

Parágrafo único. Sempre que necessário, o Tribunal deverá disponibilizar informações claras sobre a utilização dessas tecnologias e mecanismos de gerenciamento pelo(a) usuário(a).

CAPÍTULO III

DO PROGRAMA DE TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Eixos de Atuação e dos Instrumentos de Governança e Conformidade

Art. 21. O Programa tem por finalidade estabelecer mecanismos estruturantes destinados ao acompanhamento, monitoramento e aperfeiçoamento contínuo das ações institucionais relacionadas à proteção de dados pessoais.

Art. 22. O Programa será estruturado com base nos seguintes eixos de atuação:

I – monitoramento dos instrumentos de conformidade e da maturidade institucional;

II – gestão e monitoramento de riscos relacionados ao tratamento de dados pessoais;

III – acompanhamento da execução do inventário e mapeamento das operações de tratamento;

IV – acompanhamento das ações previstas no Plano de Ação de Proteção de Dados Pessoais;

V – melhoria contínua dos mecanismos institucionais relacionados à proteção de dados pessoais.

Art. 23. O Programa será coordenado pela ASSINT, na condição de unidade técnica especializada em proteção de dados pessoais.

§ 1º Compete à ASSINT, no âmbito específico do Programa:

I – promover o acompanhamento da conformidade institucional relacionada às ações previstas no Programa;

II – acompanhar os indicadores de desempenho e maturidade institucional;

III – consolidar informações relacionadas à execução das ações institucionais de proteção de dados pessoais;

IV – apoiar o monitoramento das medidas de tratamento de riscos relacionadas à proteção de dados pessoais;

V – acompanhar a implementação e evolução dos instrumentos institucionais de conformidade previstos nesta Resolução.

§ 2º As unidades administrativas e cartórios eleitorais responsáveis pelo tratamento de dados pessoais deverão colaborar com a implementação e execução do Programa.

§ 3º O Grupo de Trabalho Técnico de Proteção de Dados Pessoais atuará em caráter consultivo e colaborativo, apoiando tecnicamente a implementação, avaliação e aperfeiçoamento do Programa.

Art. 24. O Programa compreenderá, entre outros, os seguintes instrumentos institucionais de governança e conformidade:

I – inventário de dados pessoais;

II – registro das operações de tratamento de dados pessoais;

III – Relatórios de Impacto à Proteção de Dados Pessoais (RIPD);

IV – matriz de riscos relacionados ao tratamento de dados pessoais;

V – matriz de compartilhamento de dados pessoais;

VI – fluxos institucionais de atendimento aos(às) titulares;

VII – fluxos de tratamento de incidentes envolvendo dados pessoais;

VIII – modelos e cláusulas contratuais relacionadas à proteção de dados pessoais;

IX – mecanismos de monitoramento e avaliação de conformidade;

X – indicadores de desempenho e maturidade institucional;

XI – materiais orientativos, guias e instrumentos de apoio à conformidade;

XII – Plano de Ação de Proteção de Dados Pessoais.

Parágrafo único. Os instrumentos previstos neste artigo poderão ser atualizados, complementados ou substituídos sempre que necessário ao aperfeiçoamento da governança institucional.

Seção II

Dos Riscos e das Medidas de Tratamento

Art. 25. A implementação do Programa observará abordagem baseada em riscos, considerando:

I – a natureza dos dados pessoais tratados;

II – a sensibilidade das informações;

III – o volume de dados tratados;

IV – as finalidades do tratamento;

V – os impactos potenciais aos direitos dos(as) titulares;

VI – a criticidade dos ativos, sistemas e processos envolvidos;

VII – o compartilhamento interno ou externo de dados pessoais;

VIII – a utilização de tecnologias emergentes ou automatizadas;

IX – a probabilidade e o impacto de incidentes de segurança.

§ 1º As medidas de tratamento de riscos deverão observar os critérios metodológicos adotados pelo Tribunal em sua Política de Gestão de Riscos.

§ 2º O Tribunal poderá estabelecer critérios de classificação de risco para priorização das ações de adequação e monitoramento.

Art. 26. O monitoramento contínuo da maturidade institucional em proteção de dados pessoais poderá considerar, entre outros:

I – o nível de conformidade das unidades administrativas e cartórios eleitorais;

II – a evolução dos mecanismos de governança;

III – os resultados das ações de capacitação;

IV – os indicadores relacionados à gestão de riscos;

V – os resultados das avaliações internas;

VI – a evolução dos instrumentos de conformidade;

VII – os incidentes registrados e as medidas corretivas adotadas;

VIII – as recomendações expedidas pelos órgãos de controle e fiscalização.

Parágrafo único. O Tribunal poderá adotar modelos, metodologias ou referenciais de maturidade reconhecidos pela Administração Pública ou pelos órgãos de controle.

Art. 27. O Programa observará o princípio da melhoria contínua, devendo:

I – promover revisões periódicas dos mecanismos institucionais de proteção de dados pessoais;

II – incentivar a atualização contínua dos instrumentos de conformidade;

III – estimular a adoção de boas práticas nacionais e internacionais;

IV – incorporar recomendações expedidas pelos órgãos de controle, auditoria e fiscalização;

V – considerar os resultados obtidos no monitoramento institucional;

VI – promover a evolução gradual do nível de maturidade institucional.

Seção III

Do Plano de Ação

Art. 28. O Plano de Ação de Proteção de Dados Pessoais deverá contemplar, entre outros elementos:

I – ações, projetos e iniciativas institucionais;

II – responsáveis pelas ações;

III – cronogramas e prazos;

IV – prioridades institucionais;

V – indicadores e metas;

VI – entregas previstas;

VII – mecanismos de acompanhamento e revisão.

Parágrafo único. O Plano de Ação poderá ser atualizado periodicamente, observadas as necessidades institucionais, o nível de maturidade alcançado e a disponibilidade administrativa e orçamentária.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 29. A Política e o Programa de Tratamento e Proteção de Dados Pessoais deverão ser observados por todas as unidades administrativas e cartórios eleitorais do Tribunal, no âmbito de suas competências e atribuições.

Art. 30. O Fluxo de Atendimento constante do Anexo desta Resolução estabelece as etapas, responsabilidades e procedimentos relacionados ao atendimento das demandas envolvendo dados pessoais.

Parágrafo único. O instrumento complementar previsto no *caput* poderá ser atualizado sempre que necessário ao aperfeiçoamento das ações de governança, conformidade e proteção de dados pessoais no âmbito do Tribunal.

Art. 31. A Política e o Programa de Tratamento e Proteção de Dados Pessoais serão revisados periodicamente, no prazo máximo de até 3 (três) anos, ou sempre que houver necessidade de atualização decorrente de alterações normativas, institucionais ou de riscos identificados no âmbito do Tribunal.

Art. 32. O Plano de Ação de Proteção de Dados Pessoais deverá ser elaborado no prazo de até 90 (noventa) dias, contado da entrada em vigor desta Resolução.

§ 1º As unidades administrativas e cartórios eleitorais deverão adotar as medidas necessárias à adequação gradual de seus processos, procedimentos e operações de tratamento de dados pessoais às disposições desta Resolução.

§ 2º Enquanto não elaborado o Plano de Ação, poderão ser adotadas medidas prioritárias de adequação, gestão de riscos e proteção de dados pessoais, observadas as diretrizes desta Resolução.

Art. 33. Ficam revogadas as Resoluções TRE-RN n.ºs 48, de 15 de dezembro de 2021, e 148, de 6 de junho de 2025.

Art. 34. Esta Resolução entra em vigor na data de sua publicação.

Sala das Sessões do Tribunal Regional Eleitoral do Rio Grande do Norte, 18 de junho de 2026.

Desembargadora **Maria de Lourdes Azevêdo**

Presidente

Desembargador **Ricardo Procópio**

Vice-Presidente e Corregedor Regional Eleitoral

Juiz da Corte **Hallisson Rêgo Bezerra**

Juiz da Corte **Eduardo Bezerra de Medeiros Pinheiro**

Juíza da Corte **Sulamita Bezerra Pacheco**

Juiz da Corte **Marcello Rocha Lopes**

Juiz da Corte **Daniel Cabral Mariz Maia**

Fernando Rocha de Andrade

Procurador Regional Eleitoral

Documento assinado eletronicamente por **Maria de Lourdes Medeiros de Azevêdo**, **Presidente do TRE-RN**, em 06/07/2026, às 12:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rn.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2524213&crc=9995506B informando, caso não preenchido, o código verificador **2524213** e o código CRC **9995506B**.

ANEXO

FLUXO DE ATENDIMENTO ÀS DEMANDAS RELACIONADAS À PROTEÇÃO DE DADOS PESSOAIS

1. Recebimento da demanda

As solicitações relacionadas à proteção de dados pessoais serão recebidas, preferencialmente, por meio da Ouvidoria Eleitoral, observados os canais institucionais disponibilizados pelo Tribunal.

2. Registro e controle

As demandas recebidas deverão ser registradas em sistema próprio, para fins de controle, rastreabilidade, acompanhamento e monitoramento dos prazos de atendimento.

3. Análise preliminar

A Ouvidoria Eleitoral realizará imediatamente a análise preliminar da demanda e promoverá seu encaminhamento à Assessoria de Integração e, quando necessário, às unidades responsáveis pelo tratamento dos dados pessoais.

4. Instrução da demanda

As unidades responsáveis pelo tratamento dos dados pessoais deverão prestar as informações e esclarecimentos necessários ao atendimento da solicitação, observados os prazos e diretrizes institucionais aplicáveis.

5. Avaliação técnica

A Assessoria de Integração realizará a análise técnica da demanda, inclusive quanto à observância da legislação aplicável, das bases legais do tratamento e dos riscos envolvidos.

6. Elaboração da resposta

A resposta ao(à) titular deverá ser elaborada de forma clara, objetiva e acessível, observadas as hipóteses legais de restrição de acesso, sigilo e proteção de dados pessoais.

7. Encaminhamento da resposta

A resposta será encaminhada ao(à) titular pelos canais institucionais apropriados, observados os registros necessários para fins de rastreabilidade e prestação de contas e o prazo máximo de 15 dias previstos na LGPD, art. 19.

8. Monitoramento e melhoria contínua

As demandas relacionadas à proteção de dados pessoais poderão subsidiar ações de aperfeiçoamento dos mecanismos institucionais de governança, transparência, segurança da informação e proteção de dados pessoais.