RESOLUÇÃO Nº 033/2026-TCE, DE 24 DE NOVEMBRO DE 2026

Institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal de Contas do Estado do Rio Grande do Norte e dá outras providências.

O TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE (TCE-RN), no uso das competências que lhe conferem os arts. 1º, § 3º, e 7º, XIX, da Lei Complementar Estadual nº 464, de 5 de janeiro de 2012 - Lei Orgânica do TCE-RN, combinado com os arts. 2º, § 3º, e 12, IX, do seu Regimento Interno, aprovado pela Resolução nº 009, de 19 de abril de 2012; e

CONSIDERANDO a indispensabilidade da tecnologia da informação para a realização das funções institucionais e o alcance dos objetivos estratégicos do TCE-RN;

CONSIDERANDO a crescente complexidade do ambiente digital, o surgimento de novas tecnologias e o aumento das ameaças cibernéticas e crimes digitais;

CONSIDERANDO a necessidade de modernizar e fortalecer as diretrizes de segurança da informação, cibersegurança e proteção de dados pessoais, garantindo a proteção dos ativos e a continuidade dos serviços essenciais;

CONSIDERANDO a observância das boas práticas preconizadas pelas normas técnicas aplicáveis, incluindo as normas ABNT NBR ISO/IEC 27001:2022, ABNT NBR ISO/IEC 27002:2022 e ISO/IEC 27005:2022, bem como a ABNT NBR ISO/IEC 27701 (gestão da privacidade da informação) e a ISO/IEC 42001:2023 (sistema de gestão de inteligência artificial), bem como a conformidade com a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018;

CONSIDERANDO o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais (art. 5º, LXXIX, da Constituição Federal, inserido pela Emenda Constitucional nº 115/2022), e o dever do controlador de adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais e de comunicar os incidentes de segurança (arts. 46 a 49 da LGPD e Resolução CD/ANPD nº 15/2024);

CONSIDERANDO a Lei nº 15.352/2026, que transformou a Autoridade Nacional de Proteção de Dados em Agência Nacional de Proteção de Dados, mantida a

sigla ANPD, e o Projeto de Lei nº 2.338/2023, aprovado pelo Senado Federal em 10 de dezembro de 2024 e em tramitação na Câmara dos Deputados, adotado nesta Política como referência de boas práticas para o uso de inteligência artificial;

CONSIDERANDO a reestruturação da área de tecnologia da informação do Tribunal promovida pela Lei Complementar Estadual nº 796, de 31 de outubro de 2025, e pelas Resoluções nº 037/2025-GP-TCE e nº 039/2025-GP-TCE, que criaram e regulamentaram a Secretaria de Tecnologia da Informação e Comunicação (SETIC);

CONSIDERANDO que a segurança da informação e privacidade é responsabilidade de todos no âmbito deste Tribunal de Contas do Estado do Rio Grande do Norte e principalmente dos gestores e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a informação tenha o devido tratamento na Corte;

CONSIDERANDO a necessidade de aprimorar os mecanismos de proteção e de segurança das informações, ativos e serviços de tecnologia da informação do Tribunal de Contas do Estado do Rio Grande do Norte, bem como de adequar o arcabouço normativo em função de novos paradigmas, como armazenamento em nuvem, uso de inteligência artificial e trabalho remoto;

CONSIDERANDO, por fim, que a PSI deve ser revisada periodicamente, conforme recomenda a norma ABNT NBR ISO/IEC 27002, para assegurar sua contínua pertinência, adequação e eficácia;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) do Tribunal de Contas do Estado do Rio Grande do Norte (TCE-RN), com a finalidade de:

I - estabelecer princípios, diretrizes e responsabilidades para implementação de ações relacionadas à segurança da informação, à cibersegurança e à proteção de dados pessoais;

II - proteger os ativos de informação, garantindo confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade;

III - assegurar conformidade com a legislação e demais normas aplicáveis, em especial a LGPD;

IV - promover a resiliência cibernética, a continuidade dos serviços e a confiança nos processos de auditoria e fiscalização;

V - assegurar o uso ético, transparente e responsável de tecnologias digitais, com implementação de controles de governança algorítmica e supervisão humana das decisões automatizadas, observado o art. 20 da LGPD; e

VI - promover a cultura de segurança digital e conscientização sobre ameaças cibernéticas, incluindo engenharia social, *ransomware* e ataques direcionados.

Art. 2º Esta Política aplica-se a todos os colaboradores, incluindo os membros, servidores, estagiários, terceirizados, fornecedores, e quaisquer pessoas, inclusive advogados, que tenham acesso a informações ou sistemas sob a guarda do TCE-RN, bem como aos operadores e suboperadores que tratem dados pessoais em nome do Tribunal.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º A PSI do TCE-RN alinha-se às estratégias organizacionais e observará, entre outros, os seguintes princípios:

I - publicidade como regra e sigilo como exceção;

II - privacidade e proteção de dados pessoais, em conformidade com a LGPD;

III - planejamento das ações de segurança da informação e privacidade por meio de uma abordagem baseada em riscos;

IV - exigência de que a segurança da informação, a cibersegurança e a proteção de dados pessoais sejam consideradas e implementadas em todas as fases do ciclo de vida dos sistemas, serviços e processos institucionais, desde a concepção até a desativação, observado o art. 46, § 2º, da LGPD (privacidade desde a concepção e por padrão);

V - responsabilidade compartilhada de todos os usuários;

VI - melhoria contínua, alinhada a normas internacionais de segurança da informação;

VII - cooperação institucional e compartilhamento responsável de informações sobre ameaças cibernéticas; e

VIII - necessidade e minimização, limitando-se o tratamento de dados pessoais, inclusive em registros de auditoria e em sistemas de inteligência artificial, ao mínimo necessário para as finalidades (art. 6º, III, da LGPD).

CAPÍTULO III
DAS DIRETRIZES

Art. 4º A implementação da PSI observará as seguintes diretrizes:

I - proteção contra incidentes cibernéticos, ataques, fraudes e vazamentos de dados, incluindo o fortalecimento das estruturas de monitoramento, prevenção e resposta a incidentes, com mecanismos integrados de supervisão operacional e de segurança;

II - classificação da informação segundo grau de sigilo, valor estratégico e impacto, devendo observar os critérios estabelecidos na legislação e nas normas internas aplicáveis, especialmente os princípios da Lei de Acesso à Informação, de modo a assegurar a adequada proteção das informações conforme sua natureza e relevância institucional, observado que as informações pessoais relativas à intimidade, à vida privada, à honra e à imagem têm acesso restrito independentemente de classificação de sigilo (art. 31 da Lei nº 12.527/2011);

III - gestão de identidade e controle de acessos com autenticação forte, devendo ser adotados mecanismos de autenticação reforçada, gestão centralizada de identidades e controle rigoroso de acessos privilegiados;

IV - controle, registro e monitoramento do acesso aos ambientes físicos e computacionais com base nos princípios da necessidade de conhecer e do privilégio mínimo para o desempenho das atividades profissionais;

V - realização de avaliações de impacto à proteção de dados e à segurança da informação em novos sistemas, projetos e processos, inclusive o Relatório de Impacto à

Proteção de Dados Pessoais de que trata o art. 38 da LGPD, com a participação do Encarregado de Dados;

VI - gestão de riscos e continuidade de negócios com planos de contingência testados;

VII - monitoramento, auditoria e revisão periódica dos controles de TI e segurança;

VIII - capacitação contínua e campanhas de conscientização em segurança da informação e privacidade, incluindo conteúdos voltados à ética digital, segurança no uso de novas tecnologias e prevenção a incidentes cibernéticos;

IX - integração com políticas de governança, gestão de riscos e proteção de dados pessoais do TCE-RN;

X - adoção de arquitetura de segurança baseada no princípio da confiança zero, com autenticação multifator obrigatória para todos os acessos a sistemas críticos, segmentação de rede entre ambientes administrativos, de auditoria e de desenvolvimento, e verificação contínua de conformidade dos dispositivos conectados;

XI - estabelecimento de programa de inteligência de ameaças, por meio de um conjunto de processos e tecnologias para coletar, analisar e usar informações sobre ameaças cibernéticas para a defesa proativa contra ataques;

XII - desenvolvimento de capacidade de resposta a incidentes cibernéticos por meio da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

XIII - proteção contra ameaças emergentes identificadas por monitoramento contínuo e inteligência de segurança;

XIV - compartilhamento de informações resultantes de incidentes ou ameaças cibernéticas com autoridades competentes, quando aplicável por lei ou relevância, observadas a LGPD e as restrições de acesso às informações pessoais;

XV- registro das operações de tratamento de dados pessoais (art. 37 da LGPD) e proteção dos registros de auditoria (logs), que conterão apenas os dados necessários e terão acesso restrito; e

XVI - uso seguro e responsável de sistemas de inteligência artificial, na forma do Capítulo VI.

CAPÍTULO IV
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 5º Compete à Presidência do TCE-RN:

I - prover recursos para implementação da PSI;

II - instituir, quando necessário, comitês ou grupos de trabalho voltados à governança e à segurança da informação;

III - garantir a integração da PSI ao Planejamento Estratégico do Tribunal;

IV - assegurar dotação orçamentária específica para tecnologias de proteção e resposta a incidentes cibernéticos;

V - garantir a inclusão de requisitos de segurança da informação e de proteção de dados pessoais nos contratos e convênios firmados pelo TCE-RN; e

VI - designar o Encarregado de Dados, nos termos do art. 41 da LGPD e da Resolução CD/ANPD nº 18/2024.

Art. 6º Compete à Secretaria de Tecnologia da Informação e Comunicação (SETIC):

I - coordenar e acompanhar a implementação da PSI e suas normas complementares em nível operacional e técnico;

II - propor normas, políticas acessórias e mecanismos institucionais para melhoria contínua da PSI;

III - elaborar e executar um plano de resposta a incidentes de segurança em tecnologia da informação e comunicação, bem como a notificação e detecção de incidentes, relatórios, triagem, análise, resposta, contenção, erradicação, recuperação e conclusão, com vistas a identificar as causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento, por meio do Núcleo de Cibersegurança (NCS) e em articulação com o Encarregado de Dados nos incidentes que envolvam dados pessoais;

IV - manter inventário de ativos de TI, incluindo os sistemas de inteligência artificial em uso, em articulação com a Coordenadoria de Soluções de Inteligência Artificial e Automação (CSIA);

V - configurar os equipamentos, ferramentas e sistemas, utilizados no TCE-RN com todos os controles necessários para cumprir os requisitos de segurança estabelecidos pela PSI e pelas normas e procedimentos dela decorrentes, bem como pelas normatizações reguladoras de segurança da informação, quando aplicáveis;

VI - adotar medidas técnicas e controles tecnológicos para assegurar a privacidade e proteção das informações em redes e dos recursos de processamento da informação que as apoiam;

VII - estabelecer as formas de gerenciamento, controle, concessão e revogação de privilégios de acesso aos bancos de dados do TCE-RN, garantindo que apenas usuários autorizados executem operações sobre as bases de dados, com vistas a proteger as informações de qualquer ação, intencional ou acidental, que resulte em perdas ou degradação de parte ou da totalidade da integridade, confidencialidade, disponibilidade e privacidade dos dados, observadas, no que couber, as regras a serem dispostas em norma específica;

VIII - criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos, à Internet e à rede interna de comunicação de dados do TCE-RN, mantidos pelo prazo previsto na Tabela de Temporalidade de Documentos e, no caso dos registros relacionados a incidentes com dados pessoais, por, no mínimo, 5 (cinco) anos (art. 10 da Resolução CD/ANPD nº 15/2024);

IX - avaliar periodicamente as práticas de segurança em tecnologia da informação e comunicações adotadas para garantir a confidencialidade, integridade, disponibilidade, autenticidade e auditabilidade das redes e sistemas de informação do TCE-RN;

X - garantir a continuidade do uso da informação, com pelo menos uma cópia de segurança atualizada e guardada em local seguro, com o nível de proteção equivalente ao nível de proteção da informação original, incluindo cópia isolada ou imutável, protegida contra ataques de *ransomware*, e testes periódicos de restauração, observadas as regras dispostas em norma específica; e

XI - planejar, estruturar e manter a ETIR, de forma compatível com os recursos e capacidade do Tribunal, garantindo pronta resposta a incidentes cibernéticos.

Parágrafo único. A ETIR será implementada de maneira gradual, podendo utilizar recursos internos e medidas provisórias de resposta a incidentes, até atingir plena capacidade operacional, sem prejuízo do cumprimento imediato das obrigações legais de comunicação de incidentes com dados pessoais.

Art. 7º Compete ao Encarregado de Dados, no âmbito desta Política:

I - orientar as unidades e os colaboradores sobre as práticas de proteção de dados pessoais relacionadas à segurança da informação;

II - participar da elaboração do Relatório de Impacto à Proteção de Dados Pessoais e manifestar-se sobre novos sistemas, projetos e processos que tratem dados pessoais;

III - participar da avaliação de risco ou dano relevante dos incidentes com dados pessoais e auxiliar o controlador na sua comunicação à ANPD e aos titulares (art. 48 da LGPD e Resolução CD/ANPD nº 15/2024); e

IV - atuar como canal de comunicação entre o Tribunal, os titulares e a ANPD (art. 41 da LGPD).

Art. 8º Compete à Escola de Contas Professor Severino Lopes de Oliveira, relativamente à segurança da informação em recursos humanos, contemplar a promoção continuada de cursos e eventos de formação, capacitação, aperfeiçoamento e especialização sobre a LGPD, sobre o uso seguro e responsável de inteligência artificial e sobre Segurança da Informação aos membros, servidores, estagiários e terceirizados deste Tribunal.

Art. 9º Compete à Coordenadoria de Comunicação (CCOM), quanto à segurança da informação em recursos humanos, promover, de forma continuada e sistematizada, por meio de Plano de Comunicação, ações de elaboração e divulgação de conteúdo informativo (cartilhas, banners, matérias, vídeos, entre outros) sobre a LGPD e sobre Segurança da Informação.

Art. 10 Compete ao Gabinete de Segurança Institucional, no que concerne à segurança física e patrimonial, elaborar as proposições de normas e políticas acessórias aos procedimentos de segurança física e patrimonial para controlar e prevenir acesso físico não autorizado, danos e interferências nas instalações do TCE-RN.

Art. 11. Compete aos Membros, Secretários e Gestores das Unidades Organizacionais do TCE-RN:

I - assegurar que suas equipes cumpram a PSI;

II - fomentar a participação de suas equipes em treinamentos regulares sobre temas relacionados à segurança da informação e proteção de dados;

III - adotar medidas para proteção das informações físicas e digitais;

IV - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação; e

V - tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas em tempo hábil, em caso de comprometimento da segurança da informação.

Art. 12. Compete aos colaboradores:

I - zelar pelo uso correto dos ativos de informação;

II - reportar imediatamente incidentes de segurança da informação ou vazamento de dados à chefia imediata e ao Núcleo de Cibersegurança da SETIC e, quando envolverem dados pessoais, também ao Encarregado de Dados, uma vez que o prazo de comunicação à ANPD é contado do conhecimento do incidente;

III - assinar Termo de Responsabilidade, Compromisso, Confidencialidade e Não Divulgação dos Recursos de Tecnologia da Informação;

IV - participar de treinamentos sobre segurança da informação e proteção de dados; e

V - utilizar somente ferramentas de inteligência artificial homologadas pelo Tribunal, vedada a inserção de dados pessoais, sensíveis ou sigilosos em ferramentas não homologadas.

CAPÍTULO V

DA GESTÃO DE INCIDENTES CIBERNÉTICOS E CRIMES DIGITAIS

Art. 13. O TCE-RN estabelecerá, de forma gradual, procedimentos específicos para:

I - classificação de incidentes por criticidade e impacto nos serviços essenciais;

II - comunicação obrigatória às autoridades competentes, nos casos que configurarem crimes cibernéticos ou quando houver exigência legal de comunicação;

III - implementação de plano de comunicação de crise para vazamentos de dados ou ataques cibernéticos de grande impacto;

IV - estabelecimento de protocolos de cooperação com outros órgãos e instituições públicas;

V - definição de tempos máximos de resposta e recuperação para diferentes tipos de incidentes;

VI - manutenção de registros detalhados de todos os incidentes para análise de tendências e lições aprendidas;

VII - avaliação de risco ou dano relevante aos titulares e comunicação à ANPD e aos titulares dos incidentes com dados pessoais, no prazo de 3 (três) dias úteis contado do conhecimento de que o incidente afetou dados pessoais (art. 48 da LGPD e arts. 5º, 6º e 9º da Resolução CD/ANPD nº 15/2024); e

VIII - manutenção do registro dos incidentes com dados pessoais, inclusive dos não comunicados, pelo prazo mínimo de 5 (cinco) anos (art. 10 da Resolução CD/ANPD nº 15/2024).

§ 1º Os tempos de resposta para cada tipo de incidente serão definidos em normas complementares, observados, nos incidentes que envolvam dados pessoais, os prazos fixados pela Resolução CD/ANPD nº 15/2024.

§ 2º A implementação gradual prevista no caput não afasta o cumprimento imediato das obrigações previstas nos incisos VII e VIII.

CAPÍTULO VI
DA SEGURANÇA NO USO DE INTELIGÊNCIA ARTIFICIAL

Art. 14. O desenvolvimento, a contratação e o uso de sistemas de inteligência artificial (IA), inclusive de IA generativa e de agentes de IA, observarão esta Política, a LGPD e as normas complementares, adotando-se como referência de boas práticas, enquanto não houver lei específica em vigor, a abordagem baseada em riscos do Projeto de Lei nº 2.338/2023 e a norma ISO/IEC 42001:2023.

§ 1º Somente poderão ser utilizadas ferramentas de IA homologadas pela SETIC, ouvido o Encarregado de Dados quando houver tratamento de dados pessoais, vedados a inserção de dados pessoais, sensíveis ou sigilosos em ferramentas não homologadas e o uso de credenciais institucionais para a criação de contas nessas ferramentas.

§ 2º Os resultados de sistemas de IA têm natureza auxiliar, vedada a adoção de decisões que afetem direitos ou interesses de pessoas naturais unicamente com base em tratamento automatizado, assegurado o direito de revisão previsto no art. 20 da LGPD.

Art. 15. Os sistemas de IA serão protegidos por controles proporcionais ao risco, incluindo, no mínimo:

I – proteção contra injeção de comandos (*prompt injection*), envenenamento de dados, extração de dados de treinamento e manipulação de resultados;

II – minimização, anonimização ou pseudonimização dos dados pessoais antes de seu envio a modelos externos;

III – registro auditável dos comandos, das ações executadas e dos dados acessados;

IV – privilégio mínimo, limites de escopo e aprovação humana prévia para ações de agentes de IA que produzam efeitos jurídicos, alterem ou excluam registros ou compartilhem dados pessoais; e

V – testes de segurança antes da entrada em produção e monitoramento contínuo.

Art. 16. Os contratos de soluções de IA conterão cláusulas que vedem o uso dos dados do Tribunal para o treinamento de modelos, limitem e permitam auditar a retenção de dados, inclusive para fins de monitoramento de abuso, identifiquem os suboperadores e o local de processamento, observados os arts. 33 a 36 da LGPD, e prevejam a comunicação de incidentes ao Tribunal em até 24 (vinte e quatro) horas.

Parágrafo único. Os sistemas de IA de alto risco, assim entendidos os que apoiem decisões que afetem direitos de pessoas naturais, serão precedidos de Relatório de Impacto à Proteção de Dados Pessoais (art. 38 da LGPD) que contemple a avaliação de vieses, de acurácia e de supervisão humana.

CAPÍTULO VII
DAS NORMAS ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO

Art. 17. A presente Política será complementada por Normas de Segurança da Informação (NSIs), aprovadas por ato da Presidência.

Art. 18. Caberá à SETIC propor, revisar e manter atualizadas as NSIs, em articulação com comitês ou colegiados com competência sobre segurança da informação, conforme previsto no art. 5º, inciso II.

Art. 19. As NSIs devem ser implementadas gradativamente, com a priorização e detalhamento dos seus processos e procedimentos, além de serem revistas sempre que necessário, no intuito de mantê-las atualizadas diante de mudanças no ambiente interno ou externo.

Art. 20. As NSIs devem ser disponibilizadas para consulta na intranet do TCE-RN, de modo a garantir acesso e transparência aos colaboradores.

CAPÍTULO VIII
DA GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

Art. 21. A governança da segurança da informação no âmbito do TCE-RN será exercida pela alta direção, com apoio das unidades organizacionais competentes, cabendo a todos zelar pela observância desta Política.

Art. 22. O Tribunal deverá contar com um Comitê de Segurança da Informação e Privacidade (CSIP), de caráter consultivo, devendo sua composição contemplar, no mínimo, o Encarregado de Dados, um representante da área de Segurança da Informação e um servidor com amplo conhecimento das atividades do Tribunal, designados por ato da Presidência, ao qual compete apoiar a governança desta Política, acompanhar a gestão de riscos e os incidentes relevantes e propor a revisão das NSIs.

Art. 23. A governança da segurança da informação compreende, entre outros, os seguintes objetivos:

I - assegurar que as decisões estratégicas da alta direção sejam refletidas na gestão de segurança da informação;

II - garantir a implementação, aplicação e atualização contínua desta Política;

III - promover a articulação entre as unidades organizacionais para a gestão de riscos, incidentes e projetos que envolvam tratamento de dados e segurança da informação;

IV - fomentar a cultura de segurança da informação, por meio de programas de capacitação, comunicação e conscientização; e

V - propor indicadores e relatórios periódicos que permitam avaliar a maturidade institucional e orientar ações de melhoria contínua.

Art. 24. Esta Política deverá ser revisada periodicamente, em prazo não superior a 3 (três) anos, ou antes, sempre que houver alterações legais, mudanças tecnológicas relevantes, incidentes significativos ou reorganizações institucionais que impactem a governança da informação, mediante recomendação da SETIC ou do Comitê de Segurança da Informação e Privacidade.

CAPÍTULO IX
DAS PENALIDADES

Art. 25. O descumprimento desta Política, de suas diretrizes, normas e procedimentos, poderá ensejar a aplicação de sanções, observada a legislação vigente e a gravidade da infração.

§ 1º A aplicação de advertências e outras sanções de menor potencial ofensivo, relativas ao descumprimento desta Política, compete primariamente ao Gestor da Unidade Organizacional a que o servidor estiver vinculado, observados os procedimentos internos do TCE-RN e assegurados o contraditório e a ampla defesa (art. 5º, LV, da Constituição Federal e arts. 152 e 155 da Lei Complementar Estadual nº 122, de 30 de junho de 1994).

§ 2º As violações classificadas como incidentes de segurança graves, que resultarem em prejuízo significativo ou que configurem ilícito disciplinar, deverão ser levadas à ciência da Corregedoria deste Tribunal, nos termos do § 1º do art. 15 da Lei Orgânica do TCE-RN, para apuração e eventual proposição de responsabilização e

aplicação das penalidades previstas no art. 138, incisos I a VI, da Lei Complementar Estadual nº 122, de 30 de junho de 1994.

§ 3º Aplicam-se, ainda, quando cabíveis, a responsabilização civil prevista nos arts. 42 a 45 da LGPD e, quanto aos contratados, as sanções previstas na Lei nº 14.133, de 1º de abril de 2021, e no respectivo contrato.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 26. As normas específicas, operacionais ou complementares à presente Política de Segurança da Informação serão editadas por portaria da Presidência do TCE-RN e publicadas no Diário Oficial Eletrônico do TCE-RN, com vistas a regulamentar aspectos técnicos, definir responsabilidades e orientar os colaboradores quanto às práticas seguras no uso e tratamento da informação institucional.

Parágrafo único. As normas referidas no caput serão amplamente divulgadas aos colaboradores do Tribunal, por meio dos canais institucionais de comunicação, para garantir seu conhecimento e adequada aplicação.

Art. 27. Revoga-se a Resolução nº 021/2021-TCE, de 8 de setembro de 2021.

Parágrafo único. As referências à Comissão de Segurança da Informação constantes de outros atos do Tribunal passam a ser entendidas como feitas ao Comitê de Segurança da Informação e Privacidade de que trata o art. 22.

Art. 28. Esta Resolução entra em vigor na data de sua publicação.

Sala das Sessões do Tribunal Pleno, em Natal (RN), 24 de novembro de 2026.

Conselheiro CARLOS THOMPSON COSTA FERNANDES
Presidente

Conselheiro ANTONIO ED SOUZA SANTANA
Vice-Presidente

Conselheiro PAULO ROBERTO CHAVES ALVES

Conselheiro RENATO COSTA DIAS

Conselheiro FRANCISCO POTIGUAR CAVALCANTI JÚNIOR

Conselheiro ANTONIO GILBERTO DE OLIVEIRA JALES

Conselheiro GEORGE MONTENEGRO SOARES

Fui presente:

LUCIANO SILVA COSTA RAMOS
Procurador-Geral do Ministério Público de Contas