ESTADO DE ALAGOAS
TRIBUNAL DE CONTAS DO ESTADO

GABINETE DA PRESIDÊNCIA

RESOLUÇÃO ADMINISTRATIVA Nº 1/2026

INSTITUI A POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO TRIBUNAL DE CONTAS DO ESTADO DE ALAGOAS — TCE/AL E DÁ OUTRAS PROVIDÊNCIAS.

O TRIBUNAL DE CONTAS DO ESTADO DE ALAGOAS, no uso de suas atribuições constitucionais, legais e regimentais,

Considerando que o Tribunal mantém grande volume de informações essenciais ao exercício de suas competências constitucionais;

Considerando que o Tribunal produz e recebe informações no exercício de suas competências constitucionais, legais e regulamentares, e que tais informações devem permanecer confiáveis, íntegras, disponíveis, com autenticidade garantida e eventual sigilo resguardado;

Considerando que as informações são armazenadas em diferentes suportes e veiculadas por diversas formas, tais como meio impresso, eletrônico e magnético, sendo, portanto, vulneráveis a desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

Considerando que a adequada gestão da informação precisa nortear todos os processos de trabalho e unidades do Tribunal e deve ser impulsionada por política interna de segurança da informação;

Considerando a Lei 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no Art. 5º, inc. XXXIII, no Art. 37, § 3º, inc. II, e no Art. 216, § 2º, da Constituição Federal, o advento da Lei nº 17.709/2018 (Lei Geral de Proteção de Dados) e demais normas correlatas, e a RESOLUÇÃO NORMATIVA N° 8/2024;

Considerando, por fim, que a ABNT NBR ISO/IEC 27001:2022, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições; e

Considerando que a segurança é aspecto essencial para a adequada gestão da informação,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política Corporativa de Segurança da Informação do Tribunal de Contas do Estado de Alagoas contempla os princípios, objetivos e diretrizes estabelecidos nesta Resolução, observadas as disposições constitucionais, legais e regimentais vigentes.

Art. 2º A Política Corporativa de Segurança da Informação se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, cargo, emprego ou função pública no âmbito desta Corte, bem como usuários externos que, de forma autorizada, façam uso dos recursos informacionais, materiais ou tecnológicos do Tribunal.

Art. 3º Para os efeitos desta Resolução, entende-se por:

I - Ativos de informação: o patrimônio composto por todos os dados e informações gerados e manipulados nos processos do Tribunal;

II - Ativos de processamento: o patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação, necessários para a execução das atividades do Tribunal;

III - Recursos de tecnologia da informação: compreendem o conjunto dos ativos de informação e processamento;

IV - Confidencialidade: o princípio de segurança que trata da garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

V - Autenticidade: princípio da segurança da informação com vistas a assegurar a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

VI - Integridade: o princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento;

VII - Disponibilidade: o princípio de segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário;

VIII - Usuário interno: qualquer servidor ativo ou unidade do Tribunal que tenha acesso, de forma autorizada a informação produzida ou custodiada pelo Tribunal;

IX - Usuário colaborador: prestador de serviço terceirizado, estagiário ou qualquer outra pessoa que tenha acesso, de forma autorizada, a informação produzida ou custodiada pelo Tribunal;

X - Usuário externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada à informação produzida ou custodiada pelo Tribunal e que não seja caracterizada como usuário interno ou usuário colaborador;

XI - Segurança da informação: a preservação da confidencialidade, integridade, credibilidade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas;

XII - Credencial: combinação do login e senha, utilizado ou não em conjunto a outro mecanismo de autenticação, que visa legitimar e conferir autenticidade ao usuário na utilização da infraestrutura e recursos de informática.

XIII - Ciclo de vida da informação: compreende etapas e eventos de produção, recepção, utilização, acesso, alteração, reprodução, transporte, transmissão, distribuição, destinação, arquivamento e eliminação da informação;

XIV - Custodiante da informação: servidor, unidade ou estrutura ad hoc que detenha a guarda, mesmo que transitória, de informação produzida ou recebida pelo Tribunal; não faz parte, em geral, do grupo de acesso e, portanto, não está autorizado a acessar a informação;

XV - Gestor da informação: autoridade, servidor, unidade ou estrutura ad hoc que, no exercício de suas competências, seja responsável pela produção de informações, pela definição de requisitos de soluções de tecnologia da informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues ao Tribunal;

XVI - Incidente em segurança da informação: ocorrência ou série de ocorrências que indiquem uma possível violação da política de segurança da informação ou falhas de controles, com potencial e probabilidade de comprometer as operações do negócio e/ou ameaçar a segurança da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XVII - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XVIII - Classificação da informação: grau de sigilo necessário para a informação;

XIX - Tratamento da informação: conjunto de ações referentes ao estabelecimento de diretrizes de proteção da informação em função do seu nível de classificação, envolvendo todas as etapas do seu ciclo de vida; e

XX - Dados pessoais: qualquer informação que se possa relacionar direta ou indiretamente a uma pessoa natural identificada ou identificável.

Art. 4º A PCSI/TCE/AL tem por finalidade assegurar a proteção dos ativos de informação do Tribunal contra ameaças e vulnerabilidades, bem como, definir procedimentos de segurança da informação, observadas as estratégias organizacionais e as diretrizes da segurança institucional.

Art. 5º A segurança da informação tem como princípios:

I - Garantia e preservação da disponibilidade, integridade e da autenticidade das informações custodiadas, produzidas e recebidas;

II - Confidencialidade das informações com necessidade de restrição de acesso, por meio de sua proteção adequada;

III - Transparência das informações públicas; e

IV - Planejamento das ações de segurança da informação por meio de uma abordagem baseada em riscos.

Parágrafo único. A segurança da informação abrange aspectos físicos, tecnológicos e humanos do Tribunal.

CAPÍTULO II
DA ESTRUTURA DA POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO

Art. 6º A PCSI/TCE/AL é composta pelos seguintes temas:

I - Classificação da informação;

II - Gestão de incidentes em segurança da informação;

III - Gestão e controle de acesso à informação;

IV - Segurança em recursos humanos, conscientização e capacitação em segurança da informação;

V - Gestão de áreas seguras;

VI - Gestão de equipamentos;

VII - Gestão de ativos;

VIII - Gestão de banco de dados (cópias e recuperação);

IX - Gestão de dispositivos móveis e trabalho remoto;

X - Gestão riscos; e

XI - Gestão e análise crítica de vulnerabilidades e segurança da informação.

Parágrafo único. Os temas listados no ***caput***, e outros que venham a surgir, serão definidos em normativos específicos, a ser estruturados e monitorados de forma a permitir sua melhoria contínua.

CAPÍTULO III
DAS COMPETÊNCIAS E DAS RESPONSABILIDADES

Art 7° Compete ao Núcleo de Segurança e Proteção de Dados, grupo colegiado de caráter permanente, de natureza deliberativa:

I - Fomentar e patrocinar as ações relacionadas à implantação e à manutenção das Políticas Corporativa de Segurança da Informação, Privacidade e Proteção de Dados;

II – Subsidiar a elaboração e/ou alteração de políticas, normas e diretrizes relacionadas à segurança da informação, à proteção de dados pessoais e à privacidade;

III - Apoiar o planejamento, execução e monitoramento das estratégias, programas, projetos e iniciativas de segurança da informação, proteção de dados pessoais e privacidade;

IV - Realizar, de forma continuada, a gestão dos riscos relacionados à segurança da informação, à proteção de dados pessoais e à privacidade;

V - Promover o intercâmbio de informações e boas práticas relacionadas à segurança da informação, à proteção de dados pessoais e à privacidade, com outros órgãos e entidades da administração pública;

VI - Prover suporte técnico para adequação do Tribunal de Contas do Estados de Alagoas à Lei Geral de Proteção de Dados Pessoais - LGPD; e

VII – Fornecer as informações necessárias quando requeridas para implementação e adequação à Lei Geral de Proteção de Dados.

Art. 8º O Núcleo é composto por um representante titular e respectivo suplente indicados pelas seguintes unidades administrativas:

I – Presidência;

II - Diretoria Geral;

III - Diretoria de Tecnologia e Informática;

IV - Diretoria de Controle Interno;

V - Diretoria de Coordenação de Técnicos;

VI - Diretoria de Planejamento;

VII - Coordenação de Segurança e Proteção de Dados;

VIII - Ministério Público de Contas; e

IX - Governança e Compliance.

§1º Os membros do Núcleo e os respectivos suplentes serão indicados pelos titulares dos setores que representam e designados em ato do Presidente do TCE/AL.

§2º Os membros titulares do Núcleo serão substituídos pelos respectivos suplentes, em suas ausências ou impedimentos.

§3º A participação no Núcleo da Segurança da Informação será considerada prestação de serviço público relevante, não remunerada.

Art. 9º O Núcleo se reunirá, ordinariamente, a cada 30 (trinta) dias e, extraordinariamente, sempre que convocado pela Presidência.

§ 1º A Presidência designará o responsável por secretariar as reuniões do Núcleo, que poderão ser realizadas na modalidade virtual ou presencial.

§ 2° O quórum de reunião do Núcleo é de 2/3 (dois terços) e o quórum de aprovação é de maioria simples.

§ 3º O Núcleo poderá convidar para participar das reuniões, sem direito a voto, pessoas de órgãos e entidades da administração pública, do setor privado e da sociedade civil relacionados ao tema.

Art. 10 Compete à Coordenação de Segurança e Proteção de Dados indicar as necessidades corporativas de segurança da informação, bem como, conduzir o cumprimento das Políticas Corporativa de Segurança da Informação, Privacidade e Proteção de Dados que disciplinam a matéria.

Art. 11. As medidas de segurança da informação devem ser planejadas, aplicadas, avaliadas, periodicamente pelo Núcleo de Segurança e Proteção de Dados e implementadas pela Diretoria de Tecnologia de acordo com os objetivos institucionais e os riscos para as atividades do Tribunal.

Art. 12. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do Tribunal e não cabe a seus criadores qualquer forma de direito autoral.

Art. 13. A não observância aos dispositivos desta Política pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 14. Cabe à Diretoria de Tecnologia da Informação:

I - Promover as ações necessárias para a disponibilização da infraestrutura técnica de segurança e aplicação das normas de segurança;

II - Executar, monitorar e relatar à Presidência a implementação das políticas definidas pelo Núcleo;

III - Promover a comunicação e dar publicidade das normas e ações derivadas a partir da Política Corporativa de Segurança da Informação;

IV - Promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de segurança da informação e continuidade dos serviços de TI.

Art. 15. São de responsabilidade dos líderes das Diretorias do Tribunal, no que se refere à segurança da informação:

I - Conscientizar os usuários internos e colaboradores sob sua supervisão em relação aos conceitos e as práticas de segurança da informação;

II - Incorporar aos processos de trabalho as práticas inerentes à segurança da informação; e

III - Comunicar ao superior imediato competente em caso de comprometimento da segurança e quaisquer outras falhas, desvios ou violação das regras estabelecidas para adoção de medidas cabíveis

Art. 16. Os usuários deverão utilizar os recursos de tecnologia da informação para o desenvolvimento de atividades institucionais, fazendo uso de suas contas de acesso.

I - As contas de acesso são pessoais e intransferíveis; toda e qualquer ação executada pelo usuário utilizando uma determinada conta será de responsabilidade exclusiva do mesmo, devendo este zelar pelos princípios de confidencialidade e das regras de boas práticas determinadas pela Política de Segurança da Informação;

II - As credenciais de acesso deverão delegar a seu portador somente os níveis de privilégio mínimos ao exercício de sua função;

III - Os direitos de acesso devem ser compatíveis com o cargo/função exercida, conforme diretrizes estabelecidas pelo Manual de Gerenciamento de Permissões de Acesso, encaminhado por solicitação formal à Diretoria de Tecnologia e Informática (DTI), de acordo com a necessidade do serviço, sendo permitido acesso exclusivamente aos recursos e sistemas necessários à consecução de suas atividades;

IV - A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, conforme diretrizes estabelecidas pela Política de Gerenciamento de Senhas.

V - Mudança de lotação, atribuições, afastamento definitivo ou temporário do usuário deverá ser automaticamente comunicado à DTI pela Diretoria de Recursos Humanos, para procedimentos de ajustes ou cancelamento da conta de acesso, cabendo a esta o ônus por qualquer uso indevido da credencial do usuário decorrente da não comunicação de algum dos eventos tratados neste parágrafo;

VI - O acesso dos usuários colaboradores ou usuários externos, às informações produzidas ou custodiadas pelo Tribunal que não sejam de domínio público, fica condicionado ao aceite do termo de sigilo e confidencialidade (individual/empresa);

VII - Zelar pelos recursos de tecnologia da informação e segurança da informação, seguindo os princípios de confidencialidade, integridade, autenticidade e disponibilidade, manuseando corretamente os programas de computador, ligando e desligando adequadamente os equipamentos, fechando ou bloqueando os programas ou sistemas quando não estiverem utilizando; e

VIII - Comunicar imediatamente ao superior hierárquico qualquer suspeita de atos indevidos, extravio de credencial, acesso não autorizado, comprometimento da informação ou qualquer outra suspeita de ação que possa ser lesiva à administração;

Art. 17. É considerado uso indevido dos recursos de tecnologia da informação, ficando sujeito a penalidades previstas em lei:

I - Fornecer, por qualquer motivo, sua credencial de acesso para terceiros; e,

II - Fazer uso da credencial de terceiros para acesso e utilização de recursos de tecnologia da informação.

Art. 18. É proibida a exploração de falhas ou vulnerabilidades porventura existentes nos recursos de tecnologia da informação do Tribunal.

Art. 19. A DTI pode autorizar terceiros ou efetuar testes controlados de sistemas e de infraestrutura com o objetivo de identificar vulnerabilidades e mensurar riscos, adotando as medidas preventivas cabíveis a fim de evitar quaisquer efeitos danosos ou impactos indesejáveis ao ambiente computacional e ao trabalho dos usuários.

Art. 20. O uso dos recursos computacionais pelos usuários da rede do Tribunal está sujeito à monitoração em intervalos planejados, respeitando-se os princípios constitucionais e legais aplicáveis.

Art. 21. É vedado aos agentes públicos não autorizados, alterar, física e logicamente, as estações de trabalho disponibilizadas pelo Tribunal.

Art. 22. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento das informações, de acordo com a sua classificação respeitando a Resolução de Sigilo do TCE/AL (RESOLUÇÃO NORMATIVA Nº 8/2024).

Art. 23. As informações e dados produzidos ou recebidos pelo Tribunal, em regra, serão consideradas públicas, obedecendo a classificação da informação, a lei geral de proteção de dados e demais normas aplicáveis.

Art. 24. Os ativos de informação devem:

I - Ser inventariados e protegidos;

II - Ter identificados os seus proprietários e custodiantes;

III - Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - Ter a sua entrada e saída nas dependências do Tribunal autorizadas e registradas por autoridade competente;

V - Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - Ser regulamentados por norma específica quanto a sua utilização; e

VII - Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 25. A definição do custodiante do ativo de informação deve ser feita formalmente pelos gestores das áreas.

Art. 26. A ausência desta designação pressupõe que o gestor é o próprio custodiante.

Art. 27. O Núcleo de Segurança e Proteção de Dados deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 28. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 29. Durante todo o ciclo de vida de um ativo de informação, sua manipulação e uso observarão medidas especiais de segurança compatíveis com seu grau de sigilo e em conformidade com a legislação vigente e normas complementares adotadas pelo Tribunal.

Art. 30. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite do termo de sigilo e confidencialidade(individual/empresa).

Art. 31. Nos contratos de serviçs relacionados ao provimento,gerenciamento e suporte da infraestrutura computacional de TI, deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de Segurança de Informação por parte do prestador.

Art. 32. É vedado o uso de recursos de tecnologia da informação para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, bem como para veicular opiniões político- partidárias.

Art. 33. Todos os recursos de tecnologia da informação do Tribunal devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 34. É vedado o desenvolvimento e contratação de softwares e sistemas em unidades sem a análise técnica da DTI e suporte do Núcleo para assuntos de Segurança e Proteção de Dados, a fim de que sejam minorados riscos relacionados a seguir:

I - Vulnerabilidades de Segurança: Sistemas desenvolvidos fora da supervisão da DTI podem não seguir práticas adequadas de segurança, resultando em vulnerabilidades que podem ser exploradas por atacantes;

II - Falta de Conformidade: Os sistemas podem não estar em conformidade com regulamentações e padrões de segurança (como LGPD, COBIT, ITIL e ISO 27001:2022), expondo o TCE/AL a riscos legais e multas;

III - Falta de Patches e Atualizações: Sistemas desenvolvidos fora da DTI podem não receber atualizações de segurança regularmente, tornando-os vulneráveis a ataques;

IV - Implementação Inadequada de Controles de Acesso: Controles de acesso inadequados podem permitir que usuários não autorizados acessem dados sensíveis;

V - Exposição a Malware e Vírus: Sem proteções adequadas, esses sistemas podem ser mais suscetíveis a infecções por malware e vírus; e

VI - Gestão Ineficaz de Senhas: Práticas inadequadas de gestão de senhas podem levar a senhas fracas ou reutilização de senhas, aumentando o risco de comprometimento.

Art. 35. Deverá ser definida, em normatização complementar, o processo de análise e avaliação de riscos, que será realizada periodicamente no levantamento de risco nos ativos de informação do TCE/AL, visando à proteção destes ativos.

Art. 36. A normatização mencionada no Art. 34 deverá assegurar que as atividades de análise e avaliação produzam resultados comparáveis e reproduzíveis, de modo a permitir a priorização no tratamento dos maiores riscos.

§ 1° A normatização de que trata o ***caput*** deverá contemplar a definição de níveis aceitáveis de riscos, de acordo com requisitos legais, regulatórios ou internos do Tribunal.

§ 2° Todos os riscos identificados, mesmo os que forem considerados aceitáveis, deverão ter sua evolução acompanhada para permitir a detecção de possíveis mudanças no seu impacto ou probabilidade de ocorrência.

Art. 37. O Tribunal manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos de informação, considerando sua criticidade.

Art. 38. Fica assegurado à DTI, de ofício ou a requerimento do líder das áreas, a qualquer tempo, o poder de suspender temporariamente o acesso do usuário a recurso de tecnologia da informação do Tribunal, quando evidenciados riscos à segurança da informação.

Art. 39. Sobre a gestão de incidentes em segurança da informação, compete a cada unidade do Tribunal, às autoridades, aos servidores e aos colaboradores contribuir, no exercício de suas atribuições e competências, na prevenção, na identificação, no encaminhamento de incidentes em segurança da informação.

Parágrafo único. As competências relacionadas à gestão de incidentes em segurança da informação serão definidas em normativo específico.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 40. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal deverão observar, no que couber, as disposições da PCSI/TCE/AL.

Art. 41. O descumprimento de quaisquer dispositivos da PCSI/TCE/AL sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, civis e penais, nos termos da legislação pertinente, assegurados o contraditório e a ampla defesa.

Art. 42. A PCSI/TCE/AL será revista no máximo a cada 12 (doze) meses, ou por solicitação do Núcleo de Segurança e Proteção de Dados, de modo a atualizá-la frente a novos requisitos corporativos.

Art. 43. Esta Política entra em vigor na data de sua publicação, com prazo de 90 (noventa) dias para adequação dos fluxos e sistemas internos das unidades, devendo ser publicada no Portal da Transparência do TCE/AL e amplamente divulgada aos servidores, terceirizados e estagiários, mediante campanhas de conscientização promovidas pela Coordenação de Segurança e Proteção de Dados.

Sala das Sessões do Tribunal de Contas do Estado de Alagoas, em 12 de maio de 2026.

Conselheiro ***OTÁVIO LESSA DE GERALDO SANTOS***
Vice-Presidente, no exercício do cargo de Presidente - Relator

Conselheira ***ROSA MARIA RIBEIRO DE ALBUQUERQUE***
Ouvidora

Conselheira ***MARIA CLEIDE COSTA BESERRA***
Diretora Geral da Escola de Contas (ausente)

Conselheiro ***ANSELMO ROBERTO DE ALMEIDA BRITO***

ESTADO DE ALAGOAS
TRIBUNAL DE CONTAS DO ESTADO

GABINETE DA PRESIDÊNCIA

Conselheiro ***RODRIGO SIQUEIRA CAVALCANTE***
Corregedor Geral – ausente na votação

Conselheira ***RENATA PEREIRA PIRES CALHEIROS***
(ausente)

Conselheiro ***BRUNO ALBUQUERQUE TOLEDO***

Sessões:

1ª leitura: 28/4/2026;
2ª leitura: 5/5/2026;
Aprovação: 12/5/2026.

Publicada no DO-e/TCE do dia 26/5/2026.