RESOLUÇÃO ADMINISTRATIVA Nº 24/2023

Institui a Política de Segurança da Informação do Tribunal de Contas do Estado do Ceará e dá outras providências.

O **TRIBUNAL DE CONTAS DO ESTADO DO CEARÁ**, no uso das atribuições legais e regimentais, e

CONSIDERANDO a Resolução Administrativa nº 01/2021, publicada em 09 de fevereiro de 2021, que dispõe sobre o Plano Estratégico 2021-2026 do Tribunal de Contas do Estado do Ceará, bem como a Portaria nº 71/2023, publicada em 03 de fevereiro de 2023, aprovando o "Aperfeiçoamento da Segurança de TI do Tribunal" como projeto estratégico priorizado para o portfólio 2023;

CONSIDERANDO a Resolução Administrativa nº 14/2022, de 24 de agosto de 2022, que instituiu a Política de Privacidade e de Proteção dos Dados Pessoais no âmbito do Tribunal;

CONSIDERANDO a Resolução Administrativa nº 21/2022, publicada em 14 de dezembro de 2022, que instituiu a Política de Gestão de Riscos do Tribunal de Contas do Estado do Ceará e cria o Comitê de Gestão de Riscos (CGR);

CONSIDERANDO a Resolução Administrativa nº 19/2016, de 21 de dezembro de 2016, que instituiu o Comitê Gestor de Acesso, Segurança e Tratamento da Informação, alterada pela Resolução Administrativa nº 06/2021, de 12 de abril de 2021;

CONSIDERANDO a Resolução Administrativa nº 01/2023, publicada em 15 de fevereiro de 2023, que atualizou a composição e as competências do Comitê Gestor de Segurança da Informação (CGSI), instituído pela Resolução Administrativa nº 06/2012;

CONSIDERANDO a necessidade de estabelecer princípios e diretrizes para a gestão da segurança da informação pelo Tribunal de Contas do Estado do Ceará,

RESOLVE, por unanimidade de votos:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação do Tribunal de Contas do Estado do Ceará (PSI-TCE Ceará), com o objetivo de estabelecer os princípios e diretrizes para implementação das ações relacionadas a segurança da informação, garantindo proteção, integridade, confidencialidade, autenticidade e disponibilidade das informações críticas, ao mesmo tempo em que assegura o cumprimento das leis e regulamentações aplicáveis e a manutenção da confiança nos serviços de tecnologia disponibilizados pelo órgão.

Art. 2º A Política de Segurança da Informação deve ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes, em desenvolvimento ou que venham a ser adquiridos, como também às atividades de todos os servidores, colaboradores, entes conveniados, contratados/fornecedores, consultores externos e

estagiários que exercem atividades do TCE/CE ou a quem quer que venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

Art. 3º Para os efeitos desta Resolução, entende-se por:
I – segurança da informação: proteção de informações, dados e ativos digitais contra ameaças, acessos não autorizados, perdas, danos ou qualquer tipo de violação;
II – cibersegurança: prática de proteger redes, dispositivos, aplicativos, sistemas e dados de ameaças cibernéticas;
III – integridade: garantia de que as informações são precisas, confiáveis e completas ao longo de todo o seu ciclo de vida;
IV – disponibilidade: garantia de que as informações estão disponíveis quando necessário, sem interrupções não planejadas ou indevidas de serviços ou sistemas;
V – confidencialidade: proteção dos dados contra acesso não autorizado ou divulgação a pessoas não autorizadas;
VI – autenticidade: garantia de que os dados são genuínos, originais e não foram alterados ou adulterados de forma não autorizada;
VII – usuários: pessoas que usam ou podem usar os produtos, serviços ou ativos de TI disponibilizados pelo TCE/CE, podendo ser classificados como: a) usuário interno: membros, servidores, colaboradores e estagiários da instituição; b) usuário externo: fornecedores, visitantes, representantes de entidades públicas fiscalizadas pelo Tribunal e demais cidadãos.

CAPÍTULO II
DA SEGURANÇA DA INFORMAÇÃO

SEÇÃO I
Dos princípios e diretrizes

Art. 4º A segurança da informação no TCE/CE alinha-se às estratégias organizacionais e aos seguintes princípios:
I – alinhamento estratégico: a segurança da informação integra a estratégia organizacional, contribuindo para o cumprimento dos objetivos estabelecidos em seu planejamento estratégico;
II – diversidade organizacional: as diretrizes, normas e controles de segurança da informação levam em consideração a diversidade das atividades desenvolvidas na instituição, respeitando a sua natureza e finalidade;
III – conformidade: a segurança da informação é pautada pela legislação vigente e atualizações vindouras;
IV – desenvolvimento de capacidades e competências técnicas: esforços envidados na capacitação técnica e desenvolvimento de competências para a segurança da informação conforme tendências e novas tecnologias disponíveis;
V – melhoria contínua do órgão: incremento da capacidade de reação a mudanças e de integração a oportunidades de inovação, reduzindo a repetição de esforços e evasão de conhecimento;
VI – proteção da imagem do órgão: a segurança da informação está direcionada para garantir a proteção dos dados e a disponibilidade dos produtos e serviços de TI ofertados.

Art. 5º A implantação da segurança da informação no TCE/CE observará as seguintes diretrizes:
I – integração e alinhamento ao Sistema de Governança Institucional, considerando os mecanismos de estratégia, controle e liderança, com enfoque no processo decisório e na cultura organizacional;

II – conformidade com os normativos do Tribunal referentes à privacidade e proteção de dados pessoais, à gestão de riscos, ao sigilo de documentos e informações e demais legislações vigentes relacionadas ao assunto;
III – responsabilidade de todos os membros, servidores, colaboradores e estagiários do TCE/CE, em qualquer vínculo, função ou nível hierárquico pela proteção e salvaguarda dos ativos físicos, tecnológicos, dados e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, independente das medidas de segurança implementadas;
IV – análise e implementação de um novo cenário de controle a fim de viabilizar os objetivos da organização caso ocorra conflito entre os controles de segurança e uma necessidade de negócio específica;
V – submissão de todos os ativos, processos, produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados a um processo formal de gestão de riscos, visando atingir o grau de segurança adequado para o Tribunal;
VI – estabelecimento de um conjunto de estratégias e planos de ação documentados, testados e revisados periodicamente para garantir que os seus serviços essenciais sejam devidamente identificados, preservados e entregues, mesmo diante da ocorrência de um desastre até o retorno à situação normal de funcionamento da instituição;
VII – classificação de todas as informações e os respectivos recursos tecnológicos que as suportam, de acordo com seu grau de sigilo e receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida;
VIII – 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;
IX – responsabilidade de todos os usuários pela segurança da informação, e qualquer violação será tratada de forma apropriada;
X – obrigação dos usuários de reportar imediatamente, por meio dos canais da Ouvidoria ou Central de Serviços de TI, quaisquer incidentes de segurança que tomaram conhecimento, de modo que possam ser registrados, avaliados e tratados;
XI – auditoria periódica da prática de segurança da informação de forma a avaliar a conformidade das ações dos usuários internos e externos em relação ao estabelecido pela Política de Segurança da Informação e demais normativos aplicáveis;
XII – direito da Instituição de monitorar o acesso e utilização de seus ambientes físicos, assim como dos ambientes lógicos, equipamentos e sistemas tecnológicos, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente;
XIII – revisões e análises críticas do conjunto de documentos, que compõe a Política de Segurança da Informação, serão realizadas periodicamente ou sempre que ocorrer fato ou evento relevante que motive sua revisão antecipada;
XIV – capacitação regular dos usuários dos serviços de TI do TCE/CE por meio de campanhas de conscientização e treinamentos, de acordo com suas funções, garantindo assim maior efetividade e eficácia das ações de segurança da informação;
XV – disponibilidade de infraestrutura adequada será assegurada de forma a garantir a segurança da informação e a continuidade dos serviços;
XVI – metas corporativas de segurança da informação são estabelecidas e regularmente monitoradas.

SEÇÃO II
Das competências e responsabilidades

Art. 6º As partes envolvidas na segurança da informação no TCE/CE são:
I – Usuários internos e externos dos serviços e soluções de tecnologia da informação;
II – Grupo Gestor de Segurança da Informação, composto por profissionais designados pela Secretaria de Tecnologia da Informação (STI), em seus âmbitos e escopos de atuação, sob a coordenação do Diretor de Operações;
III – Comitê Gestor de Segurança da Informação (CGSI).

Art. 7º Compete aos usuários internos e externos:
I – cumprir os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
II – comunicar ao Gestor da Segurança da Informação qualquer evento que viole esta Política ou tenha potencial de colocar em risco a segurança das informações ou dos recursos computacionais do TCE/CE;
III – assinar o Termo de Confidencialidade, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.

Art. 8º Compete ao Grupo Gestor de Segurança da Informação:
I – realizar a gestão e operacionalização efetiva de segurança da informação no Tribunal tendo como base esta política e demais diretrizes do CGSI;
II – melhorar continuamente a gestão de segurança da informação por meio da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização;
III – apoiar o CGSI em suas deliberações;
IV – elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a Política de Segurança da Informação;
V – identificar e avaliar as principais ameaças à segurança da informação;
VI – apreciar as propostas de novas tecnologias e processos que podem trazer riscos e/ou oportunidades para a melhoria da segurança da informação;
VII – tomar as ações cabíveis para se fazer cumprir os termos desta política;
VIII – realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado;
IX – promover a cultura de segurança da informação.

Art. 9º Compete ao Comitê Gestor de Segurança da Informação (CGSI) as atribuições previstas em normativo específico, bem como fiscalizar o cumprimento e promover a divulgação desta PSI e demais ações para disseminar a cultura da segurança da informação no âmbito do Tribunal.

SEÇÃO III
Da estrutura

Art. 10. As Normas de Segurança da Informação tratarão de riscos, gestão de identidade e controle de acesso, backup e restauração, gestão de *patches*, vulnerabilidade, ativos, acesso remoto, gestão de incidentes, gestão de pessoas, correio eletrônico, acesso à internet e mídias sociais, classificação da informação, segurança física e patrimonial, responsabilidades, dentre outros temas, a fim de estabelecer obrigações, procedimentos e regras de implementação em nível tático e operacional.

Parágrafo único. Os documentos serão aprovados por Ato da Presidência com a classificação de sigilo, podendo ser divulgados com autorização do CGSI, mesmo que parcialmente, somente nos casos em que for imprescindível dar conhecimento aos usuários envolvidos.

SEÇÃO IV
Das penalidades

Art. 11. Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, ações administrativas poderão ser adotadas para averiguar a responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços de tecnologia da informação concedidos aos usuários, reservando-se ao TCE/CE o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, sem prejuízo de ação administrativa, civil ou penal aplicáveis.

Art. 12. A aplicação de sanções e punições será submetida à análise da Corregedoria pelo Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas na legislação pertinente.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 13. A Política de Segurança da Informação deve ser implementada gradativamente, com a priorização e detalhamento dos seus processos e procedimentos, além de ser revista sempre que necessário, no intuito de mantê-la atualizada diante de mudanças no ambiente interno ou externo.

Parágrafo único. A Secretaria de Tecnologia da Informação com o apoio da Secretaria de Governança deverá apresentar ao Comitê Gestor de Segurança da Informação, dentro do prazo de até 120 (cento e vinte) dias a partir da data de publicação desta Resolução, um plano de ação contendo o planejamento para a implementação da Política de Segurança da Informação no TCE/CE.

Art. 14. A Presidência do Tribunal expedirá os atos necessários à regulamentação e à plena implementação desta Resolução, bem como autorizará os recursos necessários para gerenciar a segurança da informação no Tribunal e resolverá os eventuais casos omissos, podendo ser subsidiada pelo Comitê Gestor de Segurança da Informação.

Art. 15. Esta Resolução entra em vigor na data de sua publicação.

Votaram os Exmos. Srs. Conselheiros Valdomiro Távora - Presidente, Alexandre Figueiredo, Soraia Victor, Edilberto Pontes, Rholden Queiroz, Patrícia Saboya e Ernesto Saboia.

TRIBUNAL DE CONTAS DO ESTADO DO CEARÁ, em Fortaleza, 14 de Novembro de 2023.

Conselheiro José Valdomiro Távora de Castro Júnior
PRESIDENTE

Esta Resolução Administrativa foi publicada do DOE-TCE/CE de 17/11/2023