TRIBUNAL DE CONTAS DO ESTADO DO TOCANTINS
Av. Joaquim Teotônio Segurado, 102 Norte, Cj. 01, Lts 01 e 02 - CEP 77006-002 - Palmas - TO - www.tceto.tc.br

PORTARIA Nº 742/2024

O TRIBUNAL DE CONTAS DO ESTADO DO TOCANTINS, no uso de suas atribuições, com fundamento no art. 3º da Lei Estadual nº 1.284, de 17 de dezembro de 2001, c/c artigos 276 a 286 do Regimento Interno, e,

Considerando que a Constituição da República Federativa do Brasil de 1988 (CRFB/88) garante o acesso à informação e a proteção aos dados pessoais, conforme inciso XXXIII do art. 5º, o inciso II do §3º do art. 37 e o §2º do art. 216;

Considerando que a Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) determina, como dever do Estado, a proteção das informações pessoais dos cidadãos e a Lei Federal nº 3.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), determina que as instituições adotem mecanismos de tratamento e proteção de dados pessoais, dentre outros diplomas legais que tratam do tema da segurança da informação, comunicação, privacidade e proteção de dados;

Considerando a necessidade de estabelecer princípios, objetivos, diretrizes e requisitos gerais que promovam a gestão integrada e coerente de processos voltados à segurança da informação, privacidade e proteção de dados, e que sejam periodicamente revistos;

Considerando que a criação de nova Política de Segurança foi inserida no Plano de Gestão do TCETO, Biênio 2023-2024, de modo a revogar a Política anterior, que foi instituída há mais de uma década pela Portaria TCETO nº 1031/2012,

RESOLVE:

CAPÍTULO I
DO OBJETIVO, ABRANGÊNCIA E PRINCÍPIOS

Art. 1º Instituir a Política de Segurança da Informação (PSI), no âmbito do Tribunal de Contas do Estado do Tocantins (TCETO), com o objetivo de estabelecer os princípios, diretrizes e requisitos para proteger seus ativos de informação e processamento, bem como aspectos de segurança pessoal, lógica e física, devendo ser observada por todos os usuários na forma desta Portaria.

Art. 2º A PSI será revisada e atualizada sempre que necessário, com base em análises de risco, antecipando-se a potenciais eventos adversos que possam ocorrer no TCETO.

Art. 3º Os princípios fundamentais da PSI incluem a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações.

CAPÍTULO II DAS DEFINIÇÕES

Art. 4º Para fins de compreensão da PSI, consideram-se as seguintes definições:

I – usuários: membros, servidores e estagiários do TCETO, fornecedores de produtos e serviços, seus prepostos e empregados, representantes de órgãos e entidades, jurisdicionados e visitantes

que tenham acesso à rede interna aos ativos de informação e processamento disponibilizados pelo Tribunal;

II – ativo de informação: patrimônio composto por todos os dados e informações gerados, manipulados ou descartados nos processos relacionados às atividades do TCETO;

III – ativo de processamento: patrimônio composto por todos os elementos de hardware e software necessários à execução de processos relacionados às atividades do TCETO, tanto produzidos internamente quanto adquiridos;

IV – hardware: componente ou conjunto de componentes físicos de um computador ou de seus periféricos;

V – software: conjunto de instruções e dados processados pelos computadores, também referenciado como programas, aplicativos ou sistemas;

VI – confidencialidade: garantia de que o acesso ao ativo de informação seja obtido somente por pessoas, entidades ou processos autorizados;

VII – integridade: garantia de que o ativo de informação seja disponibilizado sempre exato e completo;

VIII – autenticidade: garantia de que a origem do dado ou da informação é verdadeira e fidedigna;

IX – disponibilidade: garantia de que os usuários autorizados obtenham acesso aos ativos de informação e processamento sempre que necessário;

X – termo de responsabilidade: documento que formaliza a obrigação de servidores e colaboradores quanto a guarda e tratamento das informações, de acordo com seu nível de confidencialidade estabelecido pelo proprietário, bem como à correta utilização dos recursos computacionais disponibilizados pelo TCETO, conforme o estabelecido em normas específicas;

XI – servidor de rede local: ativo de processamento dedicado ao fornecimento de serviços para a realização das atividades do TCETO;

XII – equipamentos portáteis: dispositivos de pequeno porte com sistema operacional e aplicativos, conectáveis à rede de dados por meio de dispositivos sem fio (smartphone, notebook, tablets);

XIII – equipamentos de impressão: dispositivos projetados para transferir texto e imagens em diversos tipos de superfícies (geralmente papel), variados amplamente em termos de tecnologia, capacidade e finalidade, abrangendo impressoras a jato de tinta, laser, térmicas e multifuncionais;

XIV – ilhas de impressão: estratégia de alocação de equipamentos de impressão em locais específicos, visando maior eficiência no suporte e economia de insumos; e

XV – unidade de gestão de Tecnologia da Informação (TI): Diretoria de Informática (DINFO), a qual possui finalidade de propor e acompanhar políticas e diretrizes na área de TI, coordenar e implementar as atividades e soluções delas decorrentes no âmbito do TCETO.

CAPÍTULO III
DAS DIRETRIZES BÁSICAS

Art. 5º As diretrizes básicas da PSI devem atender às seguintes normas:

I – Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso à informação pública;

II – Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

III – Lei Federal nº 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras

e instrumentos para o Governo Digital e para o aumento da eficiência pública;

IV – Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), art. 307, que estabelece o crime de falsa identidade;

IV – Lei Federal nº 9.983, de 14 de julho de 2000, que altera o Código Penal, e dispõe sobre a responsabilidade civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

VI – Decreto Federal nº 7.724, de 16 de maio de 2012, que regulamenta a Lei n° 12.527, de 18 de novembro de 2011;

VII – Decreto Federal nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

VIII – Norma ABNT NBR ISO/IEC 16167:2013, que estabelece as diretrizes básicas para classificação, rotulação e tratamento das informações de acordo com sua sensibilidade e criticidade para a organização, visando ao estabelecimento de níveis adequados de proteção;

IX – Norma ABNT NBR ISO/IEC 22301:2013, que especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem;

X – Norma ABNT NBR ISO/IEC 27001:2006, que provê um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI);

XI – Norma ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;

XII – Norma ABNT NBR ISO/IEC 27003:2020, que fornece explicações e orientações sobre a ABNT NBR ISO/IEC 27001:2013;

XIII – Norma ABNT NBR ISO/IEC 27007:2018, que fornece diretrizes sobre como gerenciar um programa de auditoria de SGSI, sobre como executar as auditorias e sobre a competência dos auditores de SGSI;

XIV – Norma ABNT NBR ISO/IEC 27014:2013, que fornece orientação sobre conceitos e princípios para a governança de segurança da informação, pela qual as organizações podem avaliar, dirigir, monitorar e comunicar as atividades relacionadas com a segurança da informação dentro da organização;

XV – Norma ABNT NBR ISO/IEC 27018:2018, que estabelece objetivos de controle e diretrizes amplamente aceitas para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade descritos na ISO/IEC 29100, para o ambiente de computação em nuvem pública;

XVI – Norma ABNT NBR ISO/IEC 27032:2015, que fornece diretrizes para melhorar o estado de segurança cibernética, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança;

XVII – Norma ABNT NBR ISO/IEC 27037:2013, que fornece diretrizes para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidências digitais que possam apresentar valor probatório; e

XVIII – Norma ABNT NBR ISO/IEC 29100:2020, que fornece uma estrutura de privacidade que especifica uma terminologia comum de privacidade, especifica os atores e os seus papéis no tratamento de dados pessoais (DP), descreve considerações de salvaguarda de privacidade e fornece referências para princípios conhecidos de privacidade para TI.

CAPÍTULO IV

DA PROPRIEDADE DA INFORMAÇÃO

Art. 6º Todo ativo de informação gerado, adquirido ou custodiado por usuários na realização de atividades para o TCETO é considerado de propriedade do Tribunal e deve ser protegido conforme as regras desta PSI e regulamentações vigentes.

CAPÍTULO V
DA GESTÃO DE ATIVOS

Art. 7º Todos os ativos de informação e processamento devem ser periodicamente inventariados e atribuídos a um responsável.

Art. 8º Os ativos de informação e de processamento disponibilizados pelo TCETO devem ser utilizados estritamente para seus propósitos institucionais.

Parágrafo único. É proibido a qualquer usuário utilizar esses recursos para fins pessoais ou para promover ações que violem a legislação vigente, regulamentações internas ou prejudiquem a imagem do TCETO.

Art. 9º Os ativos de informação e processamento devem dispor de mecanismos que minimizem os riscos de segurança, evitando incidentes acidentais ou intencionais que afetem a integridade, a disponibilidade e a confidencialidade das informações.

Art. 10. Somente técnicos autorizados pela unidade de gestão de TI do TCETO devem realizar manutenções preventivas e corretivas em ativos de informação e processamento do Tribunal.

Art. 11. Arquivos salvos em unidades de armazenamento de estações de trabalho, notebooks ou equipamentos portáteis não possuem garantia de recuperação nos casos de falha, manutenção e formatação.

Parágrafo único. A unidade de gestão de TI do TCETO, juntamente com sua unidade responsável pelo suporte técnico de TI, não é responsável por backup de arquivos pessoais dos usuários.

Art. 12. O usuário deve informar, com a maior brevidade possível, a unidade de gestão de TI do TCETO sobre qualquer problema físico identificado em ativos de informação, processamento ou equipamentos portáteis, para a realização de manutenção ou acionamento de garantia.

Art. 13. É dever do usuário zelar pela conservação e bom funcionamento de todos os ativos de processamento e equipamentos portáteis sob sua responsabilidade, seguindo as boas práticas para o uso seguro de recursos de TI.

Art. 14. O uso de ativos de informação e de processamento do TCETO fora das instalações do Tribunal deve obedecer às regulamentações desta PSI e às normas específicas, sem prejuízo das regulamentações para uso interno.

CAPÍTULO VI
DOS EQUIPAMENTOS PORTÁTEIS INSTITUCIONAIS

Art. 15. As diretrizes básicas para o uso seguro de equipamentos portáteis fornecidos pelo TCETO são:

I – o usuário deve assegurar que os equipamentos portáteis estejam guardados em local seguro, com controle de acesso e garantia de integridade;

II – ao solicitar o empréstimo de equipamentos portáteis, o usuário deve assinar o termo de empréstimo de equipamento junto à Coordenadoria de Material e Patrimônio (COMAP);

III – é responsabilidade dos usuários realizar backups periódicos dos dados em dispositivos portáteis, armazenando-os em local diferente; e

IV – os equipamentos portáteis devem obedecer às mesmas regras estabelecidas para os demais ativos de processamento.

CAPÍTULO VII
DO USO DE SOFTWARES

Art. 16. As diretrizes básicas para uso adequado de softwares no âmbito do TCETO são:

I – a unidade de gestão de TI do TCETO, por meio de suas Coordenadorias, deve manter atualizado o registro dos softwares homologados, número de licenças disponíveis e softwares utilizados em equipamentos institucionais;

II – o usuário será responsabilizado pela instalação, através de seu usuário de rede, de programas e/ou aplicativos indevidos ou prejudiciais à rede do TCETO; e

III – a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida autorização formal da unidade de gestão de TI do TCETO, respeitando a classificação da informação, após identificação e justificativa do solicitante.

Art. 17. A instalação e a utilização de softwares, no âmbito do TCETO, estarão sujeitas aos seguintes requisitos:

I – quantidades de licenças de uso adquiridas e/ou disponíveis;

II – conformidade com a área de atuação da unidade interessada;

III – compatibilidade com os sistemas operacionais e softwares utilizados pelo TCETO;

IV – desempenho do ambiente computacional;

V – impacto entre a necessidade de instalação e a demanda de outras unidades; e

VI – a instalação de software freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, devem ser previamente informadas à unidade de gestão de TI do TCETO.

CAPÍTULO VIII
EQUIPAMENTOS DE IMPRESSÃO

Art. 18. As diretrizes básicas para o uso apropriado de equipamentos de impressão no âmbito do TCETO, são:

I – os equipamentos de impressão devem ser utilizados exclusivamente para atividades administrativas relacionadas ao TCETO, sendo vedado seu uso para fins particulares;

II – somente usuários previamente autorizados poderão acessar os recursos de impressão;

III – o usuário não deve deixar informações críticas, sigilosas ou sensíveis em equipamentos de impressão, de forma que pessoas não autorizadas possam acessá-las;

IV – a impressão de documentos deve ser reduzida ao mínimo necessário, utilizando os meios disponíveis para racionalização;

V – a unidade de gestão de TI do TCETO, por meio de sua unidade responsável pelo suporte técnico de TI, definirá plano para organização das ilhas de impressão;

VI – todo o suporte e manutenção de equipamentos de impressão deve ser registrado por meio do Sistema de Chamados disponibilizado na intranet; e

VII – para evitar desperdício de recursos públicos, as impressoras devem ser configuradas para impressão frente e verso (duplex), sempre que possível.

CAPÍTULO IX
DA SEGURANÇA EM PESSOAS

Art. 19. A PSI deve ser comunicada e disponibilizada a todos os usuários com a finalidade de divulgar as regras de utilização dos ativos de informação e processamento, bem como as responsabilidades decorrentes, visando maior cooperação e efetividade no cumprimento de seus objetivos.

Parágrafo único. Os contratos firmados pelo TCETO com terceiros devem incluir cláusulas que determinem a observância desta Portaria.

Art. 20. Quaisquer incidentes que possam afetar a segurança dos ativos de informação e processamento devem ser imediatamente reportados à unidade de gestão de TI do TCETO.

CAPÍTULO X
DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 21. A unidade subordinada à unidade de gestão de TI do TCETO, responsável pela gestão da segurança da informação, deve realizar avaliações periódicas dos riscos associados ao acesso aos ativos de informação e processamento, bem como às instalações físicas do TCETO, de forma a prevenir, além de acesso não autorizado, dano ou perda de informações que comprometam a continuidade das atividades institucionais.

CAPÍTULO XI
DO CONTROLE DE ACESSO

Art. 22. O acesso aos ativos de informação e de processamento disponibilizados ao usuário deverá ser restrito à execução de suas atividades no TCETO.

Art. 23. A unidade de gestão de TI do TCETO, em conjunto com a Coordenaria de Administração de Redes (COARE), deve estabelecer regras para concessão, controle e direitos de acesso aos ativos de informação, levando em consideração a classificação da informação.

§ 1º Ao usuário deve ser disponibilizada, de forma pessoal e intransferível, identificação de acesso aos ativos de informação e processamento e atribuída responsabilidade por sua guarda e uso.

§ 2º O acesso aos ativos de informação em formato não eletrônico deve seguir, na medida do possível, as mesmas precauções aplicadas aos ativos de informação em formato eletrônico.

CAPÍTULO XII
DO TRÁFEGO NA REDE TCETO

Art. 24. A unidade de gestão de TI do TCETO, em conjunto com a Coordenaria de Administração de Redes (COARE), elaborará e difundirá política de priorização de tráfego e limitação da taxa de transferência ou volume de dados, com o intuito de priorizar ou beneficiar as atividades essenciais do Tribunal.

Art. 25. O acesso à internet na rede interna do TCETO deve obedecer às seguintes diretrizes:

I – a internet disponibilizada nas dependências do TCETO deve ser utilizada exclusivamente para o desenvolvimento das atividades institucionais;

II – em casos excepcionais, alguns usuários poderão utilizar a internet fora das dependências do TCETO, via virtual private network (VPN), mediante formalização de justificativa e assinatura de termo de responsabilidade;

III – a COARE aplicará as restrições de acesso à internet, utilizando ferramenta de filtro de conteúdo e divulgando-as por meio de documento de política específica; e

IV – caso algum usuário identifique algum bloqueio de acesso a sites ou páginas devido à classificação incorreta pela ferramenta de filtro de conteúdo, deve encaminhar o link bloqueado à COARE, solicitando o desbloqueio por meio do Sistema de Chamados ou Sistema Eletrônico de Informações (SEI).

Art. 26. A unidade de gestão de TI do TCETO não garante o desempenho de acesso a sites externos que não estão sob o gerenciamento de qualquer unidade do Tribunal.

Art. 27. A unidade de gestão de TI do TCETO pode adotar e difundir medidas para garantir a disponibilidade e o desempenho do acesso a recursos, serviços e sistemas de informação, tais como:

I – bloqueios totais ou parciais de acesso a sites e serviços inadequados, impróprios, prejudiciais ou não necessários ao desenvolvimento das atividades do TCETO ou de unidades específicas;

II – priorização de acessos a determinados sites e serviços; e

III – limitação de tráfego na rede.

CAPÍTULO XIII
DA GESTÃO DE INCIDENTES DE TECNOLOGIA DA INFORMAÇÃO

Art. 28. A unidade de gestão de TI do TCETO deve adotar procedimentos de gerenciamento de incidentes de segurança e estabelecer controles para identificação e mitigação de riscos, visando limitar as consequências de danos aos ativos de informação e processamento, além de garantir a recuperação rápida, efetiva e ordenada das atividades.

Parágrafo único. Todos os incidentes de TI deverão ser disponibilizados na intranet e repassados às unidades do TCETO que podem ter sido impactadas por eles.

CAPÍTULO XIV
DA GESTÃO DE CONTINUIDADE

Art. 29. A unidade responsável pela gestão da segurança da informação, vinculada à unidade de gestão de TI do TCETO, deve elaborar, implementar, revisar e testar periodicamente um plano de continuidade de negócios, com o objetivo de reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas nos ativos de informação e processamento do TCETO.

CAPÍTULO XV
DO MONITORAMENTO

Art. 30. Respeitados os direitos e garantias individuais, bem como a legislação vigente, o uso dos ativos de informação e processamento disponibilizados pelo TCETO está sujeito a monitoramento e rastreamento.

CAPÍTULO XVI
DAS PENALIDADES

Art. 31. O descumprimento desta PSI e demais normas correlatas sujeita o usuário às sanções penais, cíveis e administrativas cabíveis.

Art. 32. Os usuários devem reportar à unidade de gestão de TI do TCETO quaisquer incidentes que afetem a segurança dos ativos ou o descumprimento desta Portaria.

Art. 33. Os casos omissos devem ser encaminhados à unidade de gestão de TI do TCETO, a qual, em conjunto com o Comitê Estratégico de Tecnologia da Informação (CETI), realizará o devido tratamento.

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

Art. 35. É revogada a Portaria nº 1031/2012.

Publique-se.

Documento assinado eletronicamente por **ANDRE LUIZ DE MATOS GONCALVES**, **PRESIDENTE**, em 19/09/2024, às 18:05, conforme art. 4º da Resolução Administrativa TCE/TO nº 001, de 15 de outubro de 2014.

A autenticidade do documento pode ser conferida no site https://sei.tceto.tc.br/sei/processos/verifica.php informando o código verificador **0760780** e o código CRC **9D5D503C**.
