RESOLUÇÃO TCE Nº 09/2015, DE 12 DE MARÇO DE 2015.
(REVOGADO PELA RESOLUÇÃO Nº 11, DE 20 DE JUNHO DE 2024)

Dispõe sobre a Política de Segurança da Informação do TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ – PSI/TCE-PI.

O TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ, no uso das atribuições legais e constitucionais; e,

Considerando que a informação gerada internamente, adquirida ou absorvida pelo Tribunal de Contas do Estado do Piauí, é patrimônio da Instituição e, portanto, necessita ser protegida;

Considerando que o Tribunal mantém grande volume de informações essenciais ao exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem manter-se íntegras, disponíveis e, quando for o caso, com o 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, por fim, que a ABNT NBR ISO/IEC 27001:2006, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

RESOLVE:

Art. 1º. Instituir a Política de Segurança da Informação (PSI-TCE/PI), objetivando assegurar que as informações e seus ativos, possuídos ou custodiados, sejam estabelecidos, protegidos e utilizados de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a lei.

Art. 2º. A Política de Segurança da Informação se aplica a todos 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 do Tribunal, e que façam uso de seus recursos materiais e tecnológicos.

Art. 3º. Para efeito 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;

III - recursos de tecnologia da informação – compreende 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 - integridade - o princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento;

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

VII - usuário interno - qualquer servidor ativo ou unidade do Tribunal que tenha acesso, de forma autorizada a informação produzida ou custeada pelo Tribunal;

VIII - usuário colaborador – prestador de serviço terceirizado, estagiário ou qualquer outro pessoa que tenha acesso, de forma autorizada, a informação produzida ou custeada pelo Tribunal;

IX - usuário externo – qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada a informação produzida ou custeada pelo Tribunal e que não seja caracterizada como usuário interno ou usuário colaborador;

X - processo de gerenciamento de risco – é o processo de planejar, organizar, dirigir e controlar os recursos humanos e materiais de uma organização, no sentido de minimizar os efeitos dos riscos sobre essa organização ao mínimo possível;

XI - plano de continuidade – conjunto de estratégias e planos e ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após ocorrência de um desastre;

XII - gestor de sistema – usuário responsável pela definição das funcionalidades de um sistema e que atua como interlocutor entre a área de negócio e a equipe de desenvolvimento de sistemas;

XIII - segurança da informação - a preservação da confidencialidade, integridade, credibilidade e disponibilidade da informação e, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade; e

XIV - credencial – a 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.

Art. 4º. O acesso às informações produzidas e custodiadas pelo Tribunal, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao

desempenho das respectivas atividades dos usuários internos ou usuários colaboradores.

Art. 5º. As medidas de segurança da informação devem ser planejadas, aplicadas, implementadas e, periodicamente, avaliadas pelo comitê gestor de tecnologia da informação, de acordo com os objetivos institucionais e os riscos para as atividades do Tribunal.

Art. 6º. 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. 7º. O uso de recursos de tecnologia da informação do Tribunal será regulamentado em norma específica, respeitando-se os dispositivos legais.

Art. 8º. A não observância aos dispositivos da PSI/TCE-PI 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. 9º. Cabe à Divisão de Segurança da Informação da Diretoria de Informática:

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

II - prestar contas da execução da Política de Segurança ao Comitê Gestor de Tecnologia da Informação, quando solicitado;

III - promover continuamente iniciativas de capacitação para servidores nos procedimentos de segurança que envolvam o uso da Tecnologia da Informação, de forma a minimizar ocorrência de problemas de segurança, sem prejuízo das normas internas específicas sobre capacitação;

IV - promover a comunicação e dar publicidade das normas e ações previstas na Política de Segurança da Informação.

V - promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de continuidade de negócios

Art. 10. Cabe ao Comitê de Tecnologia da Informação do Tribunal de Contas do Estado do Piauí:

I - promover as ações necessárias à elaboração, aplicação e revisão das normas da presente política.

II - revisar a Política de Segurança da Informação e seus instrumentos normativos sempre que se fizer necessário, ou, no mínimo, a cada ano, mantendo-se os controles de versões e revisões;

III - acompanhar e fiscalizar a aplicação das normas da Política de Segurança da Informação.

Art. 11. São de responsabilidade dos gestores das unidades gerenciais do Tribunal no que 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 de sua unidade, ou de sua área, práticas inerentes à segurança da informação; e,
III - comunicar ao superior imediato e a unidade competente em caso de comprometimento da segurança e quaisquer outras falhas, desvios ou violação das regras estabelecidas para adoção de medidas cabíveis.

Art. 12. Os usuários deverão utilizar os recursos de tecnologia da informação para o desenvolvimento de atividades institucionais, fazendo uso de suas credenciais de acesso, de acordo com as seguintes diretrizes:
I - as credenciais de acesso são pessoais e intransferíveis e toda e qualquer ação executada pelo usuário utilizando uma determinada credencial 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 - os direitos e permissões de acesso serão definidos pelo gestor da unidade gerencial e encaminhado por solicitação formal à Divisão de Segurança da Informação, de acordo com a necessidade do serviço, sendo permitido acesso exclusivamente aos recursos e sistemas necessários à consecução de suas atividades;
III - o credenciamento de usuários e efetivação das permissões serão realizados pela Divisão de Segurança da Informação por meio de solicitação formal do gestor da unidade gerencial;
IV - ao receber a credencial de acesso, o usuário e/ou colaborador deverá assinar e cientificar Termo de Responsabilidade de Utilização de recursos de tecnologia da informação do Tribunal;
V - mudança de lotação, atribuições, afastamento definitivo ou temporário do usuário deverão ser comunicados à Divisão de Segurança da Informação pela Divisão de Recursos Humanos, para procedimentos de ajustes ou cancelamento de credencial 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 artigo;
VI - o acesso dos usuários colaboradores ou usuários externos às informações produzidas ou custodiadas pelo Tribunal que não sejam de domínio público, quando autorizado pelo gestor do sistema, é condicionado ao aceite a termo de sigilo e responsabilidade;
VII - os usuários devem zelar pelos recursos de tecnologia da informação e segurança da informação, seguindo os princípios de confidencialidade, integridade 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, não deixando informações importantes desprotegidas, independentemente de sua forma; e,
VIII - os usuários devem comunicar imediatamente ao gestor da unidade gerencial 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. 13. É considerado uso indevido dos recursos de tecnologia da informação, sujeitando o usuário às 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. 14. É proibida a exploração de falhas ou vulnerabilidades porventura existentes nos recursos de tecnologia da informação do Tribunal.

Art. 15. O descumprimento das disposições constantes desta Resolução e demais normas sobre segurança da informação caracteriza infração disciplinar, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 16. 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. 17. Todos os recursos de tecnologia da informação do Tribunal devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 18. Cada recurso de tecnologia da informação deverá ter um gestor formalmente designado.

Art. 19. Deverá ser implementado processo de gerenciamento de riscos, visando à identificação e à mitigação dos mesmos, associados às atividades críticas do Tribunal.

Art. 20. Deverão ser elaborados planos de continuidade de negócio para cada atividade crítica, de forma a garantir o fluxo das informações necessárias em momento de crise e o retorno seguro à situação de normalidade.

Art. 21. Fica assegurado à Divisão de Segurança da Informação, de ofício ou a requerimento do gestor da unidade, necessariamente referendado pela Presidência, 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. 22. As normas e procedimentos de que trata esta Resolução deverão ser elaboradas tomando-se por base os objetivos e controles estabelecidos na ABNT NBR ISO/IEC 27001:2006, quais sejam:

I - organização da segurança da informação;

II - gestão de ativos;
III - segurança em recursos humanos;
IV - segurança física e do ambiente;
V - gerenciamento das operações e comunicações;
VI - controles de acessos;
VII - aquisição, desenvolvimento e manutenção de sistemas de informação;
VIII - gestão de incidentes de segurança da informação;
IX - gestão da continuidade do negócio; e
X - conformidade.

Art. 23. Esta resolução entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

Sala das Sessões do Tribunal de Contas do Estado do Piauí, em Teresina, em 12 de março de 2015.

Cons. Luciano Nunes Santos – **Presidente**
Cons. Abelardo Pio Vilanova e Silva
Cons.ª Waltânia Maria Nogueira de Sousa Leal Alvarenga
Cons. Olavo Rebêlo de Carvalho Filho
Cons.ª Lilian de Almeida Veloso Nunes Martins
Cons. em exercício Jaylson Fabianh Lopes Campelo
Cons. Substituto Delano Carneiro da Cunha Câmara
Representante do MPC - Procurador Geral Márcio André Madeira de Vasconcelos