RESOLUÇÃO TCE/PI Nº 11, DE 20 DE JUNHO DE 2024.

Dispões 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, serão 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 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, 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 do Tribunal;

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 custodiada pelo Tribunal;

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

IX - 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;

X - 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; e

XI - 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. Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar a Presidência do TCE-PI nas atividades relacionadas à segurança da informação.

Art. 6º. O Comitê será composto por um representante titular e respectivo suplente indicados pelos seguintes órgãos:

I - Presidência;
II - Ministério Público de Contas;
III - Secretaria de Controle Externo;
IV - Secretaria Administrativa;
V - Secretaria de Tecnologia da Informação.

§1º Os membros do Comitê Gestor da Segurança da Informação e os respectivos suplentes serão indicados pelos titulares dos órgãos que representam e designados em ato do Presidente do TCE-PI.

§2º Os membros de que trata o §1º deverão ser indicados dentre os agentes públicos que possuam atribuição para definir políticas ou normas relacionadas à tecnologia da informação ou à segurança da informação nos respectivos órgãos.

§3º Os membros titulares do Comitê serão substituídos pelos respectivos suplentes, em suas ausências ou impedimentos.

§4º A participação no Comitê Gestor da Segurança da Informação e nos subcolegiados será considerada prestação de serviço público relevante, não remunerada.

§5º O Coordenador do Comitê Gestor da Segurança da Informação aprovará o regimento interno, que disporá sobre a organização e o funcionamento do Comitê.

Art. 7º. O Comitê se reunirá, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu Coordenador.

§1º As reuniões do Comitê ocorrerão, em primeira convocação, com a presença da maioria simples de seus membros ou, quinze minutos após a hora estabelecida, em segunda convocação, com a presença de, no mínimo, um terço de seus membros.

§2º As deliberações do Comitê serão aprovadas pela maioria simples dos membros presentes e o Coordenador, além do voto regular, terá o voto de desempate.

Art. 8º. As medidas de segurança da informação devem ser planejadas, aplicadas, implementadas e, periodicamente, avaliadas pelo Comitê Gestor de Segurança da Informação (CGSI), de acordo com os objetivos institucionais e os riscos para as atividades do Tribunal.

Art. 9º. 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. 10. O uso de recursos de tecnologia da informação do Tribunal será regulamentado em norma específica, respeitando-se os dispositivos legais.

Art. 11. 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. 12. Cabe à Divisão de Rede e Segurança (DIRES) da Secretaria de Tecnologia da Informação (STI):

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;

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. 13. Cabe ao Comitê de Segurança da Informação (CGSI) 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. 14. São de responsabilidade dos Líderes 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. 15. 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 e permissões de acesso serão definidos pelo chefe da unidade gerencial e encaminhado por solicitação formal à DIRES, de acordo com a necessidade do serviço, sendo permitido acesso exclusivamente aos recursos e sistemas necessários à consecução de suas atividades;

IV - O credenciamento de usuários e efetivação das permissões serão realizados pela DIRES por meio de solicitação formal do líder da unidade gerencial;

V - A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio agente público, a qualquer tempo, ou por determinação da DIRES, especialmente quando houver suspeita de sua violação.

VI - A senha de rede valerá por 6(seis) meses, ressalvado o caso da certificação digital, regida por regra específica.

VII - A DIRES divulgará as regras a serem seguidas na definição da senha de rede dos agentes públicos, além de recomendações que visem assegurar a maior privacidade possível da senha.

VIII - Ao receber a conta de acesso, o usuário e/ ou colaborador deverá assinar e cientificar Termo de Responsabilidade de Utilização de recursos de tecnologia da informação do Tribunal;

IX - Mudança de lotação, atribuições, afastamento definitivo ou temporário do usuário deverá ser automaticamente comunicado à DIRES pela Diretoria de Gestão de Pessoas (DGP), para procedimentos de ajustes ou cancelamento da conta de acesso, cabendo a esta chefia o ônus por qualquer uso indevido da credencial do usuário decorrente da não comunicação de algum dos eventos tratados neste parágrafo;

X - 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 responsabilidade;

XI - 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,

XII - Comunicar imediatamente ao superior hierárquico 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. 16. 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. 17. É proibida a exploração de falhas ou vulnerabilidades porventura existentes nos recursos de tecnologia da informação do Tribunal.

Art. 18. A Secretaria de Tecnologia da Informação 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. 19. O uso dos recursos computacionais pelos agentes públicos da rede do Tribunal está sujeito à monitoração, respeitando-se os princípios constitucionais e legais aplicáveis.

Art. 20. É vedado aos agentes públicos não autorizados alterar, física ou logicamente, as estações de trabalho disponibilizadas pelo Tribunal.

Art. 21. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento das informações, de acordo com a sua classificação.

Art. 22. As informações e dados produzidos ou recebidos pelo Tribunal, em decorrência do desempenho de seu mandato, serão considerados públicos, ressalvadas as exceções previstas na legislação aplicável.

Art. 23. 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. 24. Cada ativo de informação do Tribunal deverá ter um gestor designado pelo CGTI.

Art. 25. A definição do custodiante do ativo de informação deve ser feita formalmente pelo gestor do ativo de informação.

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

Art. 27. O CGSI 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 agentes públicos aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 31. Nos contratos de serviços 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 SI 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. É vedado que apenas um usuário possua controle exclusivo de um processo de negócio ou recurso.

Art. 34. Todos os recursos de tecnologia da informação do Tribunal devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 35. Cada recurso de tecnologia da informação deverá ter um gestor formalmente designado.

Art. 36. É vedado o desenvolvimento de sistemas em unidades que não fazem parte da estrutura da STI, a fim de que sejam minorados riscos relacionados a seguir:

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

II. Falta de Conformidade - Tais sistemas podem não estar em conformidade com regulamentações e padrões de segurança (como LGPD, COBIT, ITIL), expondo o TCE/PI a riscos legais e multas;

III. Falta de Patches e Atualizações - Sistemas desenvolvidos fora da STI 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;

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. 37. Deverá ser definida, em normatização complementar, a metodologia de análise e avaliação de riscos, que será realizada periodicamente no levantamento de risco nos ativos de informação do TCE, visando à proteção destes ativos.

Art. 38. A normatização mencionada no Art. 37º 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.

§1º 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.

§2º 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. 39. 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. 40. A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e procedimentos que visem assegurar o funcionamento contínuo ou recuperação antecipada do Tribunal quando da ocorrência de indisponibilidade de recursos de infraestrutura, de tecnologia ou de recursos humanos, isolada ou simultaneamente.

Art. 41. O Plano de Continuidade de Negócios do Tribunal, baseado em metodologias e boas práticas e aprovado pelo CGSI, deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

Art. 42. 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. 43. O descumprimento das disposições constantes nesta Resolução e demais normas sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 44. Fica assegurado à DIRES, de ofício ou a requerimento do líder de unidade administrativa, 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.

Parágrafo único. As normas e procedimentos de que trata o caput desse artigo 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. 45. Esta resolução entrará 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, 20 de junho de 2024.

Cons. Joaquim Kennedy Nogueira Barros - **Presidente**
Cons. Abelardo Pio Vilanova e Silva
Consª. Lilian de Almeida Veloso Nunes Martins
Cons. Kleber Dantas Eulálio
Consª. Rejane Ribeiro de Sousa Dias
Cons. Substituto Jaylson Fabianh Lopes Campelo
Cons. Substituto Jackson Nobre Veras
Proc. Plínio Valente Ramos Neto – **Procurador-Geral do MPC**