RESOLUÇÃO Nº 126/99 - TCU[1]

Dispõe sobre a Política de Segurança de Informações do Tribunal de Contas da União - PSI/TCU e dá outras providências.

O TRIBUNAL DE CONTAS DA UNIÃO, no uso de suas atribuições constitucionais, legais e regulamentares; e

CONSIDERANDO que a informação gerada internamente, adquirida ou absorvida pelo Tribunal de Contas da União, 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 microforma, sendo, portanto, vulneráveis a desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO, por fim, os direitos e garantias individuais assegurados nos incisos IX, X, XII e XIV do art. 5º da Constituição Federal, bem como o disposto nos arts. 1º e 10 da Lei n. 9296/96; RESOLVE:

Art. 1° A Política de Segurança de Informações do Tribunal de Contas da União – PSI/TCU rege-se pelos princípios, objetivos e diretrizes estabelecidos nesta Resolução.

Parágrafo único. Integram a PSI/TCU as demais normas e procedimentos complementares e afins relacionados à segurança da informação emanados do Tribunal de Contas da União.

Art. 2º Para os efeitos desta Resolução, entende-se por:

I - **política de segurança de informação:** conjunto de normas destinadas à proteção dessa informação e à disciplina do seu manuseio;

II - **autenticidade:** princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

III - **integridade**: princípio de segurança que garante a confiabilidade da informação, evitando que esta seja adulterada ou destruída sem a permissão de seu gestor;

IV - **confidencialidade**: princípio de segurança que estabelece restrições ao acesso à informação por pessoa não expressamente autorizada pelo gestor;

V - **disponibilidade**: princípio de segurança que se refere à entrega tempestiva da informação aos usuários autorizados;

[1] Publicada no BTCU nº 66 de 08/11/1999.

VI - **criticidade**: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

VII - **contingência**: indisponibilidade ou perda de integridade da informação que os dispositivos de segurança não tenham conseguido evitar;

VIII - **custodiante:** unidade do Tribunal que processa ou armazena a informação;

IX - **gestor**: unidade do Tribunal responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas do uso da informação;

X - **usuário interno**: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao Tribunal;

XI - **usuário externo**: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao Tribunal;

XII - **comunicação oficial**: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas de unidades da Secretaria do Tribunal, de atividades especiais ou de projetos específicos;

XIII - **comunicação informal**: tráfego de documentos, informações ou formulários que não se enquadre na conceituação de que trata o inciso anterior, emitidos por caixas postais eletrônicas individuais de autoridade, servidor, estagiário ou fornecedor de bens e/ou serviços;

XIV - **caixa postal**: local de armazenamento de mensagens integrante da base de dados do servidor de correio eletrônico.

Art. 3º A PSI/TCU tem por objetivos garantir a autenticidade, a integridade, a confidencialidade e a disponibilidade das informações do Tribunal de Contas da União, bem como assegurar que sejam usadas no interesse da Instituição.

Art. 4º O Tribunal providenciará dispositivos de proteção proporcionais ao grau de confidencialidade e de criticidade da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculada, capazes de assegurar a sua autenticidade, integridade e disponibilidade.

Art. 5º As informações devem ser classificadas em função do seu grau de confidencialidade e de criticidade.

Parágrafo único. O disposto no **caput** deste artigo também se aplica às normas e procedimentos complementares a que se refere o parágrafo único do artigo 1º.

Art. 6º A designação do gestor de cada informação, conjunto de informações, sistema ou serviço disponível na rede de computadores do TCU, bem como do respectivo custodiante, deve ser feita mediante portaria da Presidência.

§ 1º Enquanto não for feita a designação de que trata o **caput** deste artigo, a gestão provisória incumbe à unidade do Tribunal responsável pela criação da informação ou, no caso daquela que for adquirida ou absorvida, pelo usuário principal.

§ 2º A competência constante do **caput** deste artigo poderá ser delegada, a critério do Presidente do TCU.

§ 3º Quando for necessário, a gestão da informação poderá ser compartilhada por duas ou mais unidades do Tribunal.

Art. 7º As informações de propriedade de pessoa física ou jurídica que não esteja vinculada administrativamente ao Tribunal, quando utilizadas por usuário interno, ficarão sob a responsabilidade do gestor designado na forma do artigo anterior.

Parágrafo único. As informações de que trata este artigo serão submetidas, adicionalmente, aos cuidados recomendados pelo proprietário.

Art. 8º Os critérios para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que serão especificados pelo gestor.

Art. 9º Nas operações a que se refere o artigo anterior, deverão ser observados os cuidados de segurança adequados aos níveis máximos de confidencialidade e criticidade das informações, quando estas compuserem um conjunto.

Art. 10. Todo acesso à informação deve ser controlado de acordo com a sua classificação, levando-se em conta as necessidades do usuário no desempenho de suas atividades.

Parágrafo único. Para viabilizar esse controle, o usuário deve ser clara e inequivocamente identificado.

Art. 11. O usuário externo que tiver acesso às informações do Tribunal fica sujeito às diretrizes, às normas e aos procedimentos de segurança de informação da PSI/TCU.

Art. 12. São deveres do usuário interno:

I - guardar sigilo das informações obtidas em decorrência do exercício de suas atribuições;

II - comunicar quaisquer falhas ou indícios de falhas de segurança de que tenha conhecimento à autoridade competente, por intermédio da via hierárquica;

III - tornar disponível para a autoridade competente, em tempo oportuno, os dados e informações necessários ao desempenho das atribuições da unidade.

Art. 13. A infração aos dispositivos da PSI/TCU poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurada aos envolvidos ampla defesa.

Art. 14. A Secretaria de Informática - Seinf submeterá à apreciação do Presidente do TCU o Plano de Contingência de Informações do Tribunal de Contas da União - PCI/TCU, constituído de um conjunto de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações.

Parágrafo único. A classificação da informação determina a necessidade e os tipos de procedimentos de contingência que serão definidos no PCI/TCU de que trata o **caput** deste artigo.

Art. 15. Os contratos, convênios e outros instrumentos congêneres celebrados pelo Tribunal devem observar os princípios, objetivos e diretrizes da PSI/TCU.

Art. 16. O correio eletrônico constitui recurso disponível na rede de comunicação de dados do Tribunal para aumentar a agilidade, segurança e economia da comunicação oficial e informal.

§ 1º. O correio eletrônico deve ser utilizado no interesse do serviço;

§ 2º. O sigilo da comunicação e das caixas postais individuais é inviolável, nos termos da Lei n. 9.296/96;

§ 3º. O conteúdo da comunicação oficial pode ser averiguado pelo Tribunal para:

I - verificar a obtenção, retenção, uso e divulgação de informações:

a) por meios ou com fins ilícitos;

b) em desacordo com as normas regulamentares;

II - subsidiar fiscalizações, investigações administrativas ou criminais;

III - garantir o pleno exercício das competências e a continuidade das atividades da Instituição;

§ 4º As normas relativas ao uso do correio eletrônico, no âmbito do Tribunal, serão definidas pela Presidência mediante Portaria.

Art. 17. As informações, os sistemas e os métodos criados pelos servidores do Tribunal, no exercício de suas funções, são patrimônio intelectual da Instituição, não cabendo a seus criadores qualquer forma de direito autoral.

Parágrafo único. Quando as informações, os sistemas e os métodos forem criados por terceiros para uso exclusivo do Tribunal, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

Art. 18. Caberá à Presidência instituir, manter e aprimorar programa de conscientização do quadro de servidores do TCU, que contemple, entre outros, os seguintes aspectos:

I - classificação das informações;

II - uso adequado e seguro de informações;

III - direitos e deveres dos usuários decorrentes do acesso e manuseio das informações.

Parágrafo único. Sem prejuízo do disposto no **caput** deste artigo, as chefias são responsáveis pela conscientização dos usuários sob sua supervisão.

Art. 19. Compete aos dirigentes das unidades básicas, no âmbito da PSI/TCU:

I - assessorar o Presidente no planejamento, na organização, na coordenação, no controle e na supervisão dos assuntos relacionados à segurança da informação;

II - assegurar a implantação das normas e procedimentos decorrentes desta Resolução;

III - propor ao Presidente a adoção de medidas preventivas ou corretivas relacionadas à segurança da informação.

Art. 20. Fica a Presidência do Tribunal autorizada a expedir os atos necessários à regulamentação desta Resolução.

Art. 21. Esta Resolução entra em vigor na data de sua publicação.

Iram Saraiva
Presidente