RESOLUÇÃO Nº 11/2015

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

O Tribunal de Contas do Estado de Minas Gerais, no uso de suas atribuições constitucionais e legais, especialmente as previstas no art. 73 e na alínea "b" do inciso I do art. 96, combinados com o art. 75, todos da Constituição da República; no §1º do art. 6º e no inciso XXIX do art. 3º, ambos da Lei Complementar Estadual n. 102, de 17/01/2008, e observadas as recomendações constantes das normas ABNT NBR ISO IEC 27001:2013 e 27002:2013;

RESOLVE:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito do Tribunal de Contas do Estado de Minas Gerais – PSI/TCE, que observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como as disposições constitucionais, legais e regimentais vigentes.

§ 1º Autoridades, servidores, colaboradores e quaisquer pessoas que tenham acesso a informações do Tribunal de Contas do Estado de Minas Gerais sujeitam-se às diretrizes, normas e procedimentos de segurança da informação da Política de que trata esta Resolução, e são responsáveis por garantir a segurança das informações a que tenham acesso.

§ 2º A PSI/TCE compreende o conjunto de normas a serem seguidas em todas as atividades ligadas à Segurança da Informação.

§ 3º Integram, também, a PSI/TCE as medidas e os procedimentos destinados à proteção da informação e à disciplina de sua utilização.

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

I – informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

II – segurança da informação: proteção da informação contra ameaças a sua confidencialidade, integridade, disponibilidade e autenticidade, para minimizar os riscos e maximizar a eficiência e a efetividade das ações;

III – gestor da informação: titular de unidade ou de projeto do Tribunal que, no exercício de suas competências, produz informações ou as obtém de fonte externa, em matéria de competência ou inerente à área de atuação do Tribunal;

IV – custodiante da informação: qualquer pessoa física ou jurídica, interna ou externa, ou unidade do Tribunal que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo Tribunal;

V – incidente de segurança da informação: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação.

VI – usuário interno: qualquer servidor ou unidade do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo próprio Tribunal;

VII – usuário colaborador: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo próprio Tribunal;

VIII – usuário externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal e que não seja usuário interno ou usuário colaborador.

Art. 3º Caberá à Presidência do Tribunal a condução da PSI/TCE, que se orientará pelos seguintes princípios:

I – confidencialidade: garantia de que a informação seja acessada somente pelas pessoas que tenham autorização para tal;

II – integridade: garantia da não violação das informações com o objetivo de protegê-las contra alteração, gravação, ou exclusão indevida, acidental ou proposital;

III – disponibilidade: garantia de que as informações estejam acessíveis aos usuários segundo sua demanda e em conformidade com a Política de Segurança;

IV – conformidade: garantia de que o processo e o sistema estejam aderentes a leis e regulamentações associadas vigentes;

V – autenticidade: garantia de que a origem da informação seja autêntica, de que ela não tenha sido alterada entre a origem (geração) e o destino (consumidor da informação);

VI – não repúdio: garantia de que o emissor da informação não tenha como negar a sua autoria.

Art. 4º Caberá à Diretoria de Tecnologia da Informação, por meio da Supervisão de Segurança Institucional da Informação, a adoção de medidas e procedimentos no âmbito da Política de Segurança da Informação, com os seguintes objetivos:

I – controlar os níveis de acesso, conforme estabelecido pelo Tribunal, de servidores, prestadores de serviços e jurisdicionados, aos sistemas, equipamentos, dispositivos e atividades vinculadas aos sistemas de informação;

II – estabelecer mecanismos que permitam aos usuários seguir padrões de comportamento relacionados à segurança da informação adequados às atividades do Tribunal;

III – capacitar e conscientizar os usuários internos para o desenvolvimento de competência em segurança da informação, permitindo a criação de uma cultura organizacional aderente;

IV – identificar e operacionalizar a classificação dos ativos de informação, conforme definido pelo Tribunal, mapeando suas vulnerabilidades e ameaças;

V – estabelecer e implementar tipos de proteção e controles de acesso que venham a minimizar riscos e impactos na garantia de execução das atividades do Tribunal, considerando:

a) a avaliação da necessidade e do tipo de acesso pelo usuário, adotando-se como parâmetro o grau de confidencialidade da informação;

b) a definição de confidencialidade da informação, conforme estabelecido pelo Tribunal e pela Lei nº 12.527, de 18 de novembro de 2011, em consonância com as atividades desempenhadas pelo usuário, com vistas a garantir a adequada autorização de acesso pelo gestor da informação, que deverá conter os limites de acesso, tais como leitura, atualização, criação e remoção, entre outros;

VI – promover intercâmbio científico e tecnológico entre os órgãos e entidades da Administração Pública direta e indireta da União, Estados e Municípios, bem como instituições de interesse do Tribunal, no que tange às atividades de Segurança da Informação;

VII – garantir a continuidade do uso da informação, com pelo menos uma cópia de segurança atualizada e guardada em local seguro, com o nível de proteção equivalente ao nível de proteção da informação original, observadas as seguintes regras:

a) para a definição das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação de ambiente;

b) os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem ter controle de acesso físico, condições ambientais adequadas e ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências;

c) definição do nível de disponibilidade para cada serviço prestado pelos sistemas de informação, nas situações mencionadas na alínea “b” deste inciso.

Parágrafo único. As medidas a serem adotadas para fins de proteção da informação deverão considerar:

I – os níveis adequados de integridade, confidencialidade e disponibilidade da informação;

II – as instruções e os procedimentos pertinentes, assim como a legislação vigente;

III – os tipos de ativos de informação;

IV – os tipos de proteção e a aplicação conforme suas finalidades;

V – a compatibilidade entre a medida de proteção e o valor do ativo protegido;

VI – o alinhamento com as diretrizes estratégicas do Tribunal;

VII – os aspectos comportamentais e tecnológicos apropriados.

Art. 5º Compete ao gestor da informação:

I – garantir o cumprimento das normas e dos procedimentos relativos à segurança da informação, no âmbito de sua competência;

II – subsidiar o processo de classificação da informação, de forma a viabilizar a correta definição a ela relacionada;

III – responsabilizar-se pela exatidão, integridade e atualização da informação sob sua custódia;

IV – tomar as medidas necessárias para que sejam aplicadas ações corretivas, nos casos de comprometimento da segurança da informação pelos usuários internos e colaboradores sob sua supervisão e informar a Supervisão de Segurança Institucional da Informação;

V – conscientizar usuários internos e colaboradores sob sua supervisão sobre os conceitos e as práticas de segurança da informação.

Art. 6º Compete ao custodiante da informação:

I – garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação;

II – comunicar tempestivamente ao gestor da informação sobre situações que comprometam a segurança das informações sob sua custódia.

Art. 7º São deveres dos usuários das informações produzidas ou custodiadas pelo Tribunal:

I – responsabilizar-se, no âmbito de sua atuação, pela proteção e segurança da informação que lhe é confiada, devendo conhecer e cumprir a PSI/TCE estabelecida nesta Resolução, bem como as diretrizes e instruções correlatas, zelando por sua correta aplicação;

II – fazer uso correto e responsável dos recursos tecnológicos, pautando-se pela legalidade e pela conduta ética, sempre em conformidade com os princípios da Segurança da Informação e com as normas previstas na Resolução nº 04, de 11 de setembro de 2013, a qual aprovou o Código de Ética dos Servidores do Tribunal de Contas do Estado de Minas Gerais;

III – comunicar ao seu superior hierárquico ou à Supervisão de Segurança Institucional da Informação qualquer incidente de segurança ou situação de risco no âmbito de sua atuação.

Art. 8º A não observância da PSI/TCE pelos usuários poderá configurar descumprimento de dever funcional.

Art. 9º Fica instituído o Comitê de Segurança da Informação, órgão colegiado de natureza consultiva e de caráter permanente.

§ 1º O Comitê de Segurança da Informação tem por finalidade formular e conduzir diretrizes para a PSI/TCE, analisar periodicamente sua efetividade e propor normas e mecanismos institucionais para melhoria contínua.

§ 2º A competência, a composição e o funcionamento do Comitê de Segurança da Informação serão regulamentados em ato normativo próprio.

Art. 10. Esta Resolução entra em vigor na data de sua publicação.

Plenário Governador Milton Campos, em 09 de dezembro de 2015.

Conselheiro Sebastião Helvecio Ramos de Castro – Presidente

Conselheiro Cláudio Couto Terrão – Vice Presidente

Conselheiro Mauri José Torres Duarte – Corregedor

Conselheiro José Alves Viana – Ouvidor

Conselheiro Wanderley Geraldo de Ávila

Conselheiro Gilberto Pinto Monteiro Diniz

Conselheiro Substituto Hamilton Antônio Coelho