INSTRUÇÃO Nº 01/20
Aprovada pela Resolução nº 01/2020

Estabelece diretrizes gerais sobre a Política de Segurança da Informação no âmbito do Tribunal de Contas do Município de São Paulo.

SEÇÃO I
DEFINIÇÕES

Art. 1º A segurança da informação é caracterizada pela preservação da:

I – confidencialidade: propriedade da informação relacionada à sua não disponibilização ou divulgação a indivíduos, entidades ou processos sem a devida autorização;

II – integridade: propriedade da informação relacionada à sua não modificação ou destruição, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

III – disponibilidade: propriedade da informação relacionada à sua acessibilidade e utilização sob demanda por indivíduo, entidades ou processos.

Art. 2º Para os fins da Política de Segurança da Informação do Tribunal de Contas do Município de São Paulo – TCMSP considera-se:

I – ativos de informação: meios de armazenamento, transmissão e processamento da informação, inclusive os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

II – autenticidade: garantia de que o conteúdo da informação seja verdadeiro, inclusive quanto aos aspectos relacionados à sua fonte geradora e ao seu destinatário;

III – incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

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

V – não-repúdio: garantia de identificação do autor da informação e prevenção da negação da autoria ou do envio da informação;

VI – recursos computacionais: recursos que transformam, transportam, guardam e descartam informações, os dados e as próprias informações, podendo ser equipamentos, conexões para rede de computadores, serviços de internet, banco de dados, sistemas operacionais, sistemas e aplicativos que manipulam direta ou indiretamente informações;

VII – rede de computadores: grupo de dois ou mais computadores interligados;

VIII – sistemas ou aplicativos: programas ou grupo de programas que automatizam

processos, adquiridos ou desenvolvidos para determinado fim, tais como processador de textos, banco de dados, planilhas eletrônicas ou sistemas específicos;

IX – usuário externo: qualquer pessoa física ou jurídica, não caracterizada como usuário interno, que tenha acesso a informações produzidas pelo TCMSP de forma autorizada;

X – usuário interno: qualquer servidor, prestador de serviço terceirizado, estagiário ou qualquer outro colaborador que tenha acesso às informações produzidas pelo TCMSP de forma autorizada;

XI – vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorado negativamente por uma ou mais ameaças.

SEÇÃO II

OBJETIVOS

Art. 3º São objetivos da Política de Segurança da Informação do TCMSP:

I – dotar as unidades organizacionais do TCMSP de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II – definir os critérios a serem adotados para que as informações mantenham o nível de segurança adequado;

III – estabelecer preceitos, regras e modelos de segurança que possibilitem a criação e a realização de um trabalho seguro e estável;

IV – promover a capacitação de usuários para o desenvolvimento de competência científico-tecnológica em segurança da informação.

SEÇÃO III

DIRETRIZES

Art. 4º A Política de Segurança da Informação do TCMSP tem como diretrizes:

I – elaborar e implementar programas destinados à conscientização e à capacitação dos usuários, visando a garantir a adequada divulgação desta Política e articulação entre as unidades;

II – desenvolver sistema de classificação de dados e de informações quanto à confidencialidade, integridade e disponibilidade, identificando-os de forma a serem adequadamente acessados, manipulados, armazenados, transportados e descartados, com vistas à garantia dos níveis de segurança desejados;

III – revisar e atualizar periodicamente esta Política, na frequência máxima de cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam revisão imediata;

IV – comunicar oficialmente a todos os usuários internos e externos sobre os termos desta Política, visando garantir que todas as pessoas tenham ciência da mesma e a pratiquem;

V – inventariar todo ativo de informação, identificando um proprietário responsável e classificando-o quanto a sua importância, prioridade e nível de proteção requeridos;

VI – monitorar e registrar todos os incidentes que afetem a segurança da informação;

VII – apurar todos os incidentes de segurança;

VIII – controlar a concessão de direitos de acesso a ativos por meio de procedimentos formais;

IX – implementar e testar periodicamente processo de "Gestão da Continuidade", visando reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas de segurança por meio da combinação de ações de prevenção e recuperação;

X – considerar, quando for utilizada computação móvel, os riscos de trabalhar em um ambiente desprotegido e a proteção adequada aplicada;

XI – monitorar os registros das ações no uso dos recursos computacionais;

XII – obedecer em todos os recursos de informática os padrões definidos internamente;

XIII – restringir a utilização de equipamentos de informática apenas àqueles usuários autorizados pelo Núcleo de Tecnologia da Informação.

Art. 5º As informações, os sistemas, os aplicativos e os métodos criados pelos servidores do TCMSP, no exercício de suas funções, constituem patrimônio intelectual da Instituição, não cabendo a seus criadores qualquer forma de direito autoral.

Art. 6º As diretrizes desta Instrução deverão ser regulamentadas por meio de normas e procedimentos a serem criados pela Comissão de Segurança da Informação.

SEÇÃO IV

DIREITOS

Art. 7º Todos os usuários internos do TCMSP têm como direitos, nos termos desta Instrução:

I – fazer uso dos recursos computacionais;

II – possuir conta de acesso ao sistema de rede corporativa;

III – ter acesso às informações que lhe são franqueadas;

IV – participar de treinamentos para utilização da Política de Segurança da Informação e demais políticas específicas.

SEÇÃO V

RESPONSABILIDADES

Art. 8º São responsabilidades do Núcleo de Tecnologia da Informação – NTI:

I – estabelecer condições para uma eficiente, segura e controlada execução de aplicações e de armazenamento de informações sob sua custódia;

II – analisar e homologar os treinamentos necessários para a correta e eficiente utilização dos recursos computacionais;

III – realizar atualizações tecnológicas e manutenção do ambiente informatizado;

IV – manter a documentação do ambiente informatizado atualizada, bem como dos sistemas e aplicativos desenvolvidos;

V – efetuar cópia de segurança e guarda das informações e dos códigos-fonte dos sistemas colocados em produção, bem como autorizar a sua restauração.

Art. 9° São responsabilidades dos usuários internos e externos:

I – garantir a segurança das informações armazenadas nos equipamentos do TCMSP;

II – informar à Comissão de Segurança da Informação as falhas ou desvios constatados das regras estabelecidas nesta Política;

III – assegurar que as senhas para acesso aos ativos de informação estejam protegidas, não devendo ser compartilhadas, preservando-se a sua confidencialidade.

SEÇÃO VI

OBRIGAÇÕES

Art. 10. São obrigações do usuário interno e, no que couber, do usuário externo:

I – cumprir os termos da Política de Segurança da Informação;

II – responder, exclusivamente, pelo uso de sua conta corporativa;

III – zelar por toda e qualquer informação armazenada contra alteração, destruição, divulgação, cópia e acesso não autorizados;

IV – fazer uso dos recursos computacionais exclusivamente para trabalhos de interesse deste Tribunal;

V – responsabilizar-se pela integridade dos ativos de informação a que tem acesso;

VI – responder pelos danos causados em decorrência da não observância das regras das políticas implantadas, bem como do mau uso dos ativos de informação e recursos computacionais, nos termos desta Instrução;

VII – garantir o sigilo das informações a que tiver acesso, tomando o cuidado necessário quanto a sua divulgação interna e externa;

VIII – manter, em caráter confidencial e intransferível, a senha de acesso aos recursos computacionais.

Parágrafo único. A utilização dos recursos de Tecnologia da Informação e Comunicação está condicionada à aceitação desta Política por parte dos usuários mediante assinatura de termo de uso, preferencialmente em meio eletrônico.

SEÇÃO VII

PROIBIÇÕES

Art. 11. É expressamente proibido aos usuários internos e externos:

I – utilizar os recursos computacionais para constranger, assediar, prejudicar ou ameaçar qualquer pessoa;

II – instalar ou retirar componentes eletrônicos dos equipamentos do TCMSP sem autorização formal do NTI;

III – instalar ou remover qualquer “software” dos equipamentos do TCMSP sem autorização formal do NTI;

IV – alterar os sistemas padrões dos equipamentos do TCMSP sem autorização formal do NTI;

V – retirar qualquer recurso computacional do TCMSP sem prévia autorização formal do NTI;

VI – atender, no desempenho de suas funções, a solicitações de serviços de informática em recursos computacionais não pertencentes ao TCMSP;

VII – instalar ou utilizar recursos computacionais não autorizados ou não homologados pelo NTI;

VIII – fazer-se passar por outra pessoa ou esconder sua identidade quando utilizar os recursos computacionais;

IX – efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais;

X – violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas ou sistemas de alarmes;

XI – divulgar ou compartilhar senhas de acesso aos recursos computacionais;

XII – utilizar de informações internas, ou de recursos computacionais, em desacordo com esta Instrução.

SEÇÃO VIII

PENALIDADES

Art. 12. O descumprimento das regras estabelecidas nesta Política sujeitará o usuário às penalidades estabelecidas na Lei Municipal n° 8.989/79, nas Leis Federais n°s 8.069/90, 8.159/91, 9.983/00 e 9.609/98 e nos Decretos-Leis n°s 2.848/40 e 3.688/41, assim como em outras normas eventualmente aplicáveis.

Parágrafo único. As penalidades mencionadas no "caput" poderão ser cominadas conjuntamente.

Art. 13. Considera-se fraude a tentativa, por um usuário não autorizado, de quebrar a segurança do sistema computacional do TCMSP, ou de descobrir a senha de outros usuários, estando o usuário à aplicação de penalidade prevista no Decreto-Lei n° 2.848/40, com as alterações introduzidas pela Lei Federal n° 9.983/00, e de acordo com a Lei Municipal n° 8.989/79.

Art. 14. Caso fique comprovado que um incidente de segurança foi ocasionado pelo não cumprimento dos preceitos estabelecidos nesta Política, bem como nas normas e procedimentos dela decorrentes, e que houve dolo do(s) usuários(s) envolvido(s), interno(s) ou externo(s), serão aplicadas as penalidades previstas no(s) regulamento(s) do TCMSP, assim como na legislação municipal, estadual ou federal pertinente.

Art. 15. A presente Instrução entrará em vigor na data de sua publicação, ficando revogadas as Instruções n°s 01/2007 e 02/2011, e demais disposições em contrário.

Plenário Conselheiro "Paulo Planet Buarque", em 19 de fevereiro de 2020.

a) JOÃO ANTONIO – Conselheiro Presidente; a) ROBERTO BRAGUIM – Conselheiro Vice-Presidente; a) EDSON SIMÕES – Conselheiro Corregedor a) MAURICIO FARIA – Conselheiro; a) DOMINGOS DISSEI – Conselheiro.

Publicada no DOC de 20/02/2020 p. 111-112