ATO Nº 1429/19

Institui a Política de Segurança da Informação da Câmara Municipal de São Paulo e dá outras providências.

CONSIDERANDO a necessidade de que a alta direção da Casa e os usuários mantenham compromisso permanente com a segurança da informação;

CONSIDERANDO a necessidade de aderência aos normativos existentes quanto ao acesso e à divulgação da informação, em especial a Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), o Ato da Mesa nº 1156, de 20 de junho de 2011 e Ato da Mesa nº 1231, de 25 de junho de 2013.

CONSIDERANDO o disposto na Política de Gestão do Processo Legislativo Eletrônico da Câmara Municipal de São Paulo instituída pelo Ato nº 1323, de 1º de dezembro de 2015;

CONSIDERANDO que a informação, em todo o seu ciclo de vida, constitui-se em bem estratégico e em ativo fundamental para o desempenho das atribuições constitucionais e para as atividades administrativas da Câmara Municipal de São Paulo;

CONSIDERANDO a necessidade de manter as informações íntegras, autênticas, disponíveis como preceito geral, e o uso restrito como exceção;

CONSIDERANDO que as informações geradas, recebidas, mantidas, transmitidas e tratadas pela Câmara Municipal de São Paulo estão em diferentes suportes, e que é necessário prevenir incidentes, naturais ou não, de origem humana ou tecnológica, que comprometam a segurança dessas informações;

CONSIDERANDO a necessidade de instituir e manter uma política que norteie o tratamento de informações no âmbito da Câmara Municipal de São Paulo, quanto aos aspectos de segurança;

CONSIDERANDO a necessidade de estabelecer princípios, objetivos, diretrizes e requisitos gerais que promovam a gestão integrada e coerente de processos voltados à segurança da informação, que sejam periodicamente revistos;

CONSIDERANDO que a segurança é uma qualidade da informação que depende de todos os que com ela lidam, em qualquer etapa de seu ciclo de vida; e

CONSIDERANDO a necessidade de esclarecer e determinar aos usuários seus direitos e deveres no tocante à segurança da informação;

A MESA DA CÂMARA MUNICIPAL DE SÃO PAULO, no uso de suas atribuições regimentais, RESOLVE:

SEÇÃO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação da Câmara Municipal de São Paulo, que compreende princípios, objetivos, diretrizes, requisitos e define atribuições e instrumentos para a gestão da segurança da informação no âmbito desta Casa.

Art. 2º Esta Política se aplica a todos os usuários dos conteúdos informacionais e dos recursos de tecnologia da informação providos pela Câmara Municipal de São Paulo.

Art. 3º Para os fins desta Política, são adotadas as seguintes definições:

I - Autenticação: processo pelo qual o usuário apresenta sua identificação ao recurso computacional para obtenção de acesso válido, por meio de senha, dispositivo de segurança (como token ou "chaveiro digital", ou cartão digital de acesso), biometria (impressão digital, palmar ou da íris), entre outros;

II - Autenticidade: atributos que permitem atestar a proveniência, a veracidade e a fidedignidade dos conteúdos informacionais;

III - Ciclo de vida dos conteúdos informacionais: compreende, no todo ou em parte, as etapas de criação, formalização, captura, aquisição, tratamento, armazenamento, preservação, recuperação, acesso, uso, disseminação, avaliação e destinação do conteúdo informacional da Câmara Municipal de São Paulo;

IV - Confidencialidade: qualidade de grau de sigilo, atribuído pela autoridade competente, a dado, informação ou documento;

V - Conteúdo informacional: toda informação registrada, produzida, recebida, adquirida, capturada ou colecionada pela Câmara Municipal de São Paulo, no desempenho de sua missão institucional, qualquer que seja seu suporte;

VI - Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

VII - Disponibilidade: garantia de acesso à informação por usuários autorizados, quando necessário;

VIII - Gestor de negócio: servidor responsável por propor, homologar e aprovar requisitos de negócio implementados em sistemas informatizados, bem como por zelar pela qualidade da informação provida pelos sistemas sob sua alçada e ainda por indicar os gestores de permissões desses sistemas;

IX - Gestor de permissões: servidor, indicado pelo gestor de negócio, responsável por conceder ou revogar permissões de acesso a dados e/ou a sistemas de informação automatizados;

X - Gestor técnico: servidor responsável por um sistema ou serviço de Tecnologia da Informação sob responsabilidade da Câmara Municipal de São Paulo;

XI - Incidente de segurança da informação: evento simples ou série de eventos de segurança da informação indesejados ou inesperados que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XII - Integridade: qualidade da informação que se encontra completa e que não sofreu nenhum tipo de dano ou alteração não autorizada ou não documentada, seja na origem, no trâmite ou na destinação;

XIII - Registros de segurança: registros contendo atividades dos usuários, exceções e outros eventos de segurança da informação;

XIV - Risco: combinação da probabilidade de um evento e de suas consequências;

XV - Segurança da Informação: preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação;

XVI - Sistema de Gestão da Segurança da Informação (SGSI): conjunto que compreende estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos, pessoas e demais recursos que a organização utiliza para, de modo coordenado e com base na abordagem de riscos, tratar os temas da segurança da informação;

XVII - Usuário: aquele que tem acesso autorizado aos conteúdos informacionais, em qualquer etapa de seu ciclo de vida, ou aos recursos de tecnologia da informação providos pela Câmara Municipal de São Paulo, podendo ser Vereador, servidor, prestador de serviços terceirizado, estagiário, bem como pessoa física ou jurídica externa à Casa.

SEÇÃO II - DOS PRINCÍPIOS E OBJETIVOS

Art. 4º São princípios da Política de Segurança da Informação:

I - a atenção e a responsabilidade de todos os usuários quanto à necessidade de segurança da informação;

II - a participação de todos, de modo a prevenir, detectar e responder aos incidentes de segurança da informação;

III - o respeito aos legítimos interesses dos usuários no acesso e uso da informação;

IV - a observância da publicidade como preceito geral e do sigilo como exceção;

V - a contínua análise dos riscos aos quais a informação está sujeita;

VI - a incorporação da segurança como requisito essencial dos sistemas de informação, informatizados ou não;

VII - a gestão sistêmica da segurança da informação;

VIII - a avaliação periódica da segurança da informação, de modo tal a realizar as modificações apropriadas a esta Política, bem como às práticas, demais normas e procedimentos de segurança da informação.

Art. 5º São objetivos da Política de Segurança da Informação:

I - instituir uma cultura organizacional aderente à segurança da informação, compreendendo ações destinadas a fomentar entre os usuários a constante observância quanto às práticas destinadas à preservação dessa segurança;

II - implantar a contínua avaliação dos riscos a que a informação está sujeita;

III - estabelecer mecanismos que visem garantir a segurança da informação, em especial a confidencialidade, a integridade, a disponibilidade e a autenticidade nos projetos, processos e atividades da Câmara Municipal de São Paulo;

IV - implementar a governança da segurança da informação.

SEÇÃO III - DAS DIRETRIZES

Art. 6º São diretrizes da Política de Segurança da Informação, no âmbito da Câmara Municipal de São Paulo:

I - alinhamento das ações de segurança da informação às atividades institucionais e às iniciativas estratégicas da Casa;

II - capacitação adequada dos usuários frente às necessidades de segurança da informação;

III - instituição de normas específicas e procedimentos para a segurança da informação aderentes a esta Política;

IV - observância de leis, regulamentos e obrigações contratuais aos quais os processos de trabalho estão sujeitos, bem como normas e boas práticas, nacionais e internacionais, que sejam aplicáveis.

SEÇÃO IV - DOS REQUISITOS

Art. 7º A Política de Segurança da Informação, no âmbito da Câmara Municipal de São Paulo, atenderá aos seguintes requisitos:

I - estabelecimento, manutenção e contínuo aprimoramento de um SGSI, devidamente documentado e adequado ao contexto das atividades da Casa e aos riscos que ela enfrenta;

II - estabelecimento e aplicação de uma metodologia de análise e avaliação de riscos que dê suporte ao SGSI e que seja adequada aos requisitos legais, regulamentares e de segurança da informação identificados e aplicáveis à Casa;

III - medição contínua da eficácia dos controles do SGSI para verificar se os requisitos de segurança da informação foram atendidos;

IV - observância da proporcionalidade entre as medidas de segurança da informação implementadas e os riscos aos quais a informação está sujeita;

V - exigência de competência e dos conhecimentos necessários para os usuários aos quais forem atribuídas responsabilidades definidas no SGSI;

VI - orientação dos usuários quanto às práticas de segurança da informação.

SEÇÃO V - DA IMPLANTAÇÃO E REVISÃO DA POLÍTICA

Art. 8º Fica criado o Comitê Gestor de Segurança da Informação (CGSI), composto por um servidor indicado como representante de cada uma das seguintes unidades administrativas da Casa:

I - Secretaria Geral Administrativa (SGA);

II - Secretaria Geral Parlamentar (SGP);

III - Secretaria de Documentação (SGP-3);

IV - Centro de Comunicação Institucional (CCI);

V - Consultoria Técnica de Economia e Orçamento (CTEO);

VI - Procuradoria;

VII - Centro de Tecnologia da Informação (CTI);

VIII - Núcleo Técnico de Controle Interno (NTCI).

§ 1º Cada representante será indicado com o respectivo substituto.

§ 2º A coordenação do Comitê Gestor de Segurança da Informação (CGSI) caberá ao Centro de Tecnologia da Informação (CTI) e à Secretaria de Documentação (SGP.3), cada um dentro de sua área de competência.

§ 3º Compete ao Comitê Gestor de Segurança da Informação:

I - avaliar periodicamente e manter atualizadas a Política de Segurança da Informação e as normas dela decorrentes;

II - demandar às unidades administrativas a elaboração de normas específicas relacionadas à segurança da informação em suas áreas de competência;

III - receber, avaliar e validar propostas de normas relativas à segurança da informação;

IV - encaminhar à autoridade competente para deliberação as propostas de atualização da política de segurança da informação e as propostas de normas correlatas;

V - coordenar a implantação e atualização do SGSI a ser adotado pela Casa;

VI - acompanhar e avaliar o sistema implantado conforme o inciso anterior;

VII - coordenar a seleção, implantação e atualização da metodologia de análise periódica de riscos a ser adotada pela Casa, bem como a definição do escopo e abrangência dessas análises;

VIII - planejar e coordenar ações institucionais de segurança da informação;

IX - propor a inclusão das iniciativas relacionadas à segurança e preservação da informação no planejamento institucional pertinentes e suas atualizações.

Art. 9º O Comitê Gestor poderá convidar membros temporários para apoiá-lo em suas atividades, de acordo com a necessidade.

Art. 10. Compete à Secretaria Geral Administrativa e ao Centro de Tecnologia da Informação, no que diz respeito à política de segurança da informação:

I - supervisionar sua implantação e execução;

II - promover a cultura da segurança da informação e o envolvimento de todas as unidades administrativas na consecução dos objetivos, diretrizes e requisitos desta política.

Art. 11. Compete ao Centro de Tecnologia da Informação (CTI) e à Secretaria de Documentação (SGP.3), com o apoio do Comitê Gestor (CGSI):

I - coordenar a divulgação da política de segurança da informação, bem como as normas dela derivadas, e de suas atualizações;

II - assessorar as unidades administrativas da Casa quanto à implementação da segurança da informação em seus processos de trabalho;

III - propor, validar e implementar os requisitos de segurança da informação para os conteúdos informacionais e os recursos computacionais da Casa, em articulação com as unidades administrativas responsáveis pelos processos de trabalho.

Art. 12. São atribuições das unidades administrativas da Câmara Municipal de São Paulo:

I - participar da implantação e da execução da política de segurança da informação;

II - zelar pela segurança da informação no âmbito dos processos de trabalho e atividades sob sua responsabilidade;

III - elaborar normas e procedimentos relacionados à segurança da informação em seus processos de trabalho, em consonância com a política prevista neste Ato, submetendo-os à apreciação do Comitê Gestor de Segurança da Informação;

IV - participar da definição dos requisitos e funcionalidades de segurança da informação dos aplicativos e sistemas de informação vinculados aos seus processos de trabalho, validando-os.

Art. 13. São atribuições dos usuários:

I - zelar pelos requisitos de confidencialidade, integridade, disponibilidade e autenticidade, no tocante aos conteúdos informacionais e aos recursos computacionais com os quais lidam;

II - observar as normas e procedimentos relacionados à segurança da informação.

Parágrafo único. É dever do servidor comunicar à chefia imediata sobre violações identificadas em relação à Política prevista neste Ato e às normas e procedimentos dela decorrentes.

Art. 14. São direitos dos servidores, em relação à Política de Segurança da Informação:

I - receber treinamento adequado ao exercício de suas atribuições;

II - propor aperfeiçoamento da Política prevista neste Ato e de seus instrumentos de gestão.

SEÇÃO VI - DAS DISPOSIÇÕES TRANSITÓRIAS

Art. 15. As demandas iniciais do Comitê Gestor de Segurança da Informação às unidades administrativas competentes para elaboração e revisão de normas e procedimentos relativos à segurança da informação terão como prioridade os seguintes temas, sem prejuízo de eventuais necessidades prementes:

I - autenticação e controle de acesso à rede de dados, aos serviços de tecnologia da informação e comunicação e aos sistemas de informação da Câmara Municipal de São Paulo;

II - acesso, proteção e guarda da informação;

III - aquisição, desenvolvimento e manutenção de sistemas informatizados;

IV - classificação da informação, observado o disposto na Lei n.º 12.527, de 2011 e em sua regulamentação específica no âmbito da Câmara Municipal de São Paulo;

V - coleta e preservação de registros de segurança;

VI - cópias de segurança de dados e de sistemas informatizados;

VII - gestão de incidentes de segurança da informação;

VIII - criação de Grupo de Trabalho para elaboração da Política de Preservação Digital;

IX - inventário dos recursos computacionais e dos conteúdos informacionais, enfatizando os aspectos de responsabilidades, preservação e de uso aceitável;

X - elaboração de Plano de Continuidade de Negócio;

XI - segregação de ambientes de tecnologia da informação e comunicação, com a implementação de ambientes distintos de desenvolvimento, teste, homologação e produção de sistemas computacionais, feita em atendimento ao princípio da separação de funções, com a definição de papéis e responsabilidades, específicos para cada ambiente;

XII - segurança das instalações e ambientes digitais que hospedam os conteúdos informacionais e os recursos computacionais para os quais essa normatização seja necessária.

Art. 16. Este Ato entra em vigor na data de sua publicação.

São Paulo, 26 de março de 2019.