CÂMARA DOS DEPUTADOS
Centro de Documentação e Informação

ATO DA MESA Nº 47, DE 16/07/2012

Institui a Política de Segurança da Informação da Câmara dos Deputados e dá outras providências.

A MESA DA CÂMARA DOS DEPUTADOS, no uso de suas atribuições regimentais,

Considerando a necessidade de que a alta direção da Casa e os usuários tenham 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 nº 12.527, de 18 de novembro de 2011;

Considerando o disposto na Política de Gestão de Conteúdos Informacionais da Câmara dos Deputados;

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 dos Deputados;

Considerando a necessidade de manter as informações íntegras, autênticas, disponíveis e, quando for o caso, sigilosas ou de acesso restrito;

Considerando que as informações geradas, recebidas, mantidas, transmitidas e tratadas pela Câmara dos Deputados 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 dos Deputados, 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;

RESOLVE:

SEÇÃO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação da Câmara dos Deputados, que compreende princípios, objetivos, diretrizes e 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 dos Deputados.

Art. 3º Para os fins desta Política, entende-se como:

I - Autenticação: processo pelo qual o usuário apresenta sua identificação ao recurso computacional para obtenção de acesso válido. Pode se dar por 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 dos Deputados;

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 dos Deputados, 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. Também é o responsável 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 do órgão gestor dos recursos computacionais da Câmara dos Deputados (Resolução 16/1997, art. 2º, e Portaria 34/2009/DG, art. 5º).

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: qualquer evento que, se ocorrer, afeta o alcance de algum objetivo organizacional; *(Inciso com redação dada pelo Ato da Mesa nº 233, de 24/5/2018)*

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 dos Deputados, podendo ser unidade administrativa, Deputado, servidor efetivo, secretário parlamentar, ocupante de cargo de natureza especial, prestador de serviços terceirizado, estagiário ou membro do Programa de Apoio ao Trabalho do Adolescente (Pró-Adolescente), bem como pessoa física ou jurídica externa à Casa.

SEÇÃO II - DOS PRINCÍPIOS E OBJETIVOS

Art. 4º São princípios desta 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; e

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 Com vistas à observância aos princípios descritos no artigo 4º, esta Política está voltada aos seguintes objetivos:

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 dos Deputados; e

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 dos Deputados:

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 as normas e boas práticas, nacionais e internacionais, aplicáveis.

SEÇÃO IV - DOS REQUISITOS

Art. 7º A Política de Segurança da Informação, no âmbito da Câmara dos Deputados, 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 os 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 - Diretoria-Geral;

II - Secretaria Geral da Mesa;

III - Diretoria Legislativa;

IV - Diretoria Administrativa;

V - Diretoria de Recursos Humanos;

VI - Secretaria de Comunicação Social;

VII - Centro de Documentação e Informação;

VIII - Centro de Informática.

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

§ 2º A coordenação do Comitê Gestor de Segurança da Informação será alternada, a cada dois anos, entre os representantes do Centro de Documentação e Informação e do Centro de Informática, que a exercerá no primeiro biênio.

§ 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 da informação no Plano Plurianual de Gestão de Conteúdos Informacionais e em suas atualizações.

§ 4º O Comitê Gestor será assessorado por uma Câmara Técnica, composta pelos seguintes membros permanentes, indicados pelos respectivos diretores:

I - dois servidores do Centro de Documentação e Informação;

II - dois servidores do Centro de Informática;

§ 5º A depender da necessidade, a Câmara Técnica convidará membros temporários para apoiá-la em suas atividades.

§ 6º Portaria do Diretor-Geral tratará da instalação e do funcionamento do Comitê Gestor e de sua Câmara Técnica.

Art. 9º Compete à Diretoria-Geral da Câmara dos Deputados, no que diz respeito à política de segurança da informação:

I - supervisionar sua implantação e execução;

II - assegurar a adequada alocação de recursos humanos, materiais, orçamentários e financeiros necessários à sua implantação e execução;

III - 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. 10. Compete conjuntamente ao Centro de Documentação e Informação - Cedi e ao Centro de Informática - Cenin:

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. 11. São atribuições das unidades administrativas da Câmara dos Deputados:

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 esta política, submetendo-os à apreciação do Comitê Gestor de Segurança da Informação;

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

Art. 12. 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 a chefia imediata sobre violações identificadas em relação a esta Política e às normas e procedimentos dela decorrentes.

Art. 13. São direitos dos servidores, em relação à Política de Segurança da Informação:

I - receber treinamento adequado ao exercício de suas atribuições;

II - propor aperfeiçoamento desta Política e de seus instrumentos de gestão.

SEÇÃO VI - DAS DISPOSIÇÕES TRANSITÓRIAS

Art. 14. 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 - acesso, proteção e guarda da informação, em especial a informação sigilosa;

II - aquisição, desenvolvimento e manutenção de sistemas informatizados;

III - autenticação e controle de acesso à rede de dados, aos serviços de tecnologia da informação e comunicação e aos sistemas de informação da Câmara dos Deputados;

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

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 - inventário dos recursos computacionais e dos conteúdos informacionais, em consonância com a Política de Gestão de Conteúdos Informacionais, enfatizando os aspectos de responsabilidades e de uso aceitável;

IX - Plano de Continuidade de Negócio;

X - 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;

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

§ 1º No período máximo de 180 (cento e oitenta) dias a contar da entrada em vigor deste Ato, o Comitê Gestor de Segurança da Informação aprovará plano de ação contemplando as iniciativas necessárias para a implementação da Política de Segurança de Informação da Câmara dos Deputados e das normas dela resultantes, em especial as citadas no *caput*.

§ 2º Os processos decorrentes do plano de ação receberão o selo de "Gestão Estratégica", previsto pela Portaria do Diretor-Geral nº 234/2009, e os projetos relacionados comporão o Plano Plurianual de Gestão de Conteúdos Informacionais.

Art. 15. Este Ato entra em vigor na data de sua publicação.

Sala de Reuniões da Mesa, 16 de julho de 2012.

Deputado Marco Maia
Presidente

Deputada Rose de Freitas
Primeira-Vice-Presidente

Deputado Eduardo da Fonte
Segundo-Vice-Presidente

Deputado Eduardo Gomes
Primeiro-Secretário

Deputado Jorge Tadeu Mudalen
Segundo-Secretário

Deputado Inocêncio Oliveira
Terceiro-Secretário

Deputado Júlio Delgado
Quarto-Secretário

JUSTIFICAÇÃO

Na Câmara dos Deputados a informação assume papel preponderante na consecução de suas atribuições institucionais, seja a de legislar sobre as questões de interesse nacional de competência da União, seja a de fiscalizar os atos do Poder Executivo. É também essencial o papel da informação na interação entre a sociedade brasileira e a Câmara dos Deputados. Nesse sentido, tanto a informação quanto as soluções de tecnologia da informação e comunicação que dão apoio a tais atividades na Casa revestem-se de importância estratégica.

A informação pode residir em suportes físicos de diversas naturezas. Pode estar gravada no tradicional papel, por escrita ou impressão. Pode estar em meio digital, ou ainda registrada em filmes e vídeos, falada em discursos ou debates e preservada em gravações de áudio. Independentemente da conformação física que a informação adquira ao ser produzida, armazenada, transmitida ou compartilhada, é imprescindível que se garantam sua integridade, sua disponibilidade e, nos casos em que esteja resguardada por sigilo, a sua confidencialidade.

A informação, bem como os processos de trabalho e os meios analógicos e digitais que lhes dão suporte, são ativos valiosos para toda organização. O leque de ameaças que podem causar dano a esses ativos é variado, incluindo desastres naturais, acidentes tais como incêndios ou desabamentos, atos de vandalismo, fraudes através de computadores, vírus de computador, ação de *hackers*, ataques deliberados para causar indisponibilidade dos serviços, sabotagem, espionagem e vazamento de informação sigilosa. As técnicas de ataque deliberado à segurança da informação tem se diversificado e se sofisticado. Proteger esses ativos contra essas ameaças é importante para assegurar a continuidade e a normalidade dos trabalhos da instituição, prevenir a indisponibilidade de serviços prestados à sociedade, prevenir danos à imagem da instituição, minimizar prejuízos decorrentes de danos à informação e proteger a informação classificada com algum grau de sigilo.

Por essas razões, a Política de Segurança da Informação proposta visa promover o comportamento desejável dos responsáveis, dos custodiantes e dos usuários da informação no sentido de proteger a informação dos riscos a que possa estar exposta, de possibilitar a identificação das responsabilidades em caso de materialização dos riscos e de propiciar o tratamento da informação em conformidade com as leis, com as normas brasileiras que versam sobre o tema, com as boas práticas e com as recomendações dos órgãos de controle, a exemplo do Acórdão TCU-Plenário nº 1603/2008, que recomenda às instituições públicas, incluindo nominalmente a Câmara dos Deputados, que “orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.”