Câmara dos Deputados
Comitê Gestor de
Segurança da Informação

PLANO DE AÇÃO EM SEGURANÇA DA INFORMAÇÃO

Brasília | 2014

PLANO DE AÇÃO EM SEGURANÇA DA INFORMAÇÃO

MESA DA CÂMARA DOS DEPUTADOS

54ª Legislatura – 4ª Sessão Legislativa

2011-2015

Presidente
Henrique Eduardo Alves

1º Vice-Presidente
Arlindo Chinaglia

2º Vice-Presidente
Fábio Faria

1º Secretário
Márcio Bittar

2º Secretário
Simão Sessim

3º Secretário
Maurício Quintella Lessa

4º Secretário
Biffi

Suplentes de Secretário

1º Suplente
Gonzaga Patriota

2º Suplente
Wolney Queiroz

3º Suplente
Vitor Penido

4º Suplente
Takayama

Diretor-Geral
Sérgio Sampaio Contreiras de Almeida

Secretário-Geral da Mesa
Mozart Vianna de Paiva

Câmara dos Deputados
Comitê Gestor de
Segurança da Informação

PLANO DE AÇÃO EM SEGURANÇA DA INFORMAÇÃO

Centro de Documentação e Informação
Coordenação Edições Câmara
Brasília | 2014

CÂMARA DOS DEPUTADOS

DIRETORIA LEGISLATIVA
Diretor: Afrísio Vieira Lima Filho

CENTRO DE DOCUMENTAÇÃO E INFORMAÇÃO
Diretor: Adolfo C. A. R. Furtado

COORDENAÇÃO EDIÇÕES CÂMARA
Diretora: Heloísa Helena S. C. Antunes

CENTRO DE INFORMÁTICA
Diretor: Luiz Antonio Souza da Eira

Projeto gráfico: Daniela Barbosa
Capa e diagramação: Alessandra Castro
Revisão: Seção de Revisão

Câmara dos Deputados
Centro de Documentação e Informação – Cedi
Coordenação Edições Câmara – Coedi
Anexo II – Térreo – Praça dos Três Poderes
Brasília (DF) – CEP 70160-900
Telefone: (61) 3216-5802; fax: (61) 3216-5810
editora@camara.leg.br

SÉRIE
Gestão Institucional. Programas e projetos corporativos.
n. 4

Dados Internacionais de Catalogação-na-publicação (CIP)
Coordenação de Biblioteca. Seção de Catalogação.

Brasil. Congresso Nacional. Câmara dos Deputados. Comitê Gestor de Segurança da Informação.
Plano de ação em segurança da informação [recurso eletrônico] / Câmara dos Deputados, Comitê Gestor de Segurança da Informação . – Brasília : Câmara dos Deputados, Edições Câmara, 2014.
44 p. – (Série gestão institucional. Programas e projetos corporativos n. 4)

1. Brasil. Congresso Nacional. Câmara dos Deputados. 2. Gestão da informação, Brasil. 3. Segurança de dados, Brasil. I. Título. II. Série.

CDU 342.532:004(81)

SUMÁRIO

INTRODUÇÃO

A Política de Segurança da Informação (PSI) da Câmara dos Deputados, instituída pelo Ato da Mesa nº 47 de 2012, estabelece princípios e diretrizes para o tratamento da informação, reconhecida como ativo valioso e recurso fundamental para que a instituição desempenhe suas atribuições. A PSI atribui responsabilidades e orienta a adoção de ações visando ao aprimoramento da Segurança da Informação nos processos de trabalho da Casa. Para a governança das iniciativas nessa área, a PSI criou o Comitê Gestor de Segurança da Informação (CGSI).

O CGSI é formado por representantes de todas as diretorias e secretarias da Casa, além de representantes do Centro de Documentação e Informação (Cedi) e do Centro de Informática (Cenin). Compete ao comitê a preparação do Plano de Ação em Segurança da Informação, de acordo com o § 1º do art. 14 do Ato da Mesa nº 47/2012. O plano deve contemplar as iniciativas necessárias para a implementação da PSI e das demais normas dela resultantes.

A Segurança da Informação é tema que envolve diferentes aspectos de uma organização, desde os locais onde a informação é guardada até recursos humanos e tecnológicos. Abrange processos de trabalho, relação com fornecedores e prestadores de serviço, uso adequado das ferramentas e serviços de tecnologia da informação, cuidados com o ambiente de trabalho e publicação de normas que regulamentem o tema.

Diante dessas várias linhas de ação possíveis, o CGSI dirigiu os esforços de elaboração deste plano para ações voltadas à estruturação da gestão da Segurança da Informação, buscando atender ao mesmo tempo a aspectos de conformidade em relação ao próprio Ato da Mesa nº 47/2012, às normas nacionais na área de Segurança da Informação e às recomendações dos órgãos de controle.

COMPOSIÇÃO DO CGSI

Diretoria-Geral (DG)	Sérgio Dagnino Falcão Lamberto Ricarte Serra Júnior
Secretaria Geral da Mesa (SGM)	José Cláudio Conceição de Aguiar
Diretoria Legislativa (Dileg)	Luiz Humberto Ferreira Carneiro Sandra Silva Maia
Diretoria Administrativa (Dirad)	Flávio Gomes de Mesquita Cláudia Cristina Aires Gomes
Diretoria de Recursos Humanos (DRH)	Laila Moreira Machado Fabiano Peruzzo Schwartz
Secretaria de Comunicação Social (Secom)	Malva Beatrice Machado Algarte Bruno Paiva Menezes
Centro de Documentação e Informação (Cedi)	Rosinaldo Dourado da Fonseca Júnior Vanderlei Batista dos Santos
Centro de Informática (Cenin)	Fábio Sérgio Cruz Gustavo Vasconcellos Cavalcante

DIRETRIZES

A elaboração deste plano se deu à luz das diretrizes estabelecidas pela Política de Segurança da Informação da Câmara dos Deputados, conforme o art. 6º do Ato da Mesa nº 47/2012:

> 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.

O Ciclo de Gestão Estratégica 2012-2023 da Câmara dos Deputados define, em sua Diretriz 7 – Gestão, as seguintes linhas de atuação a serem seguidas pela Casa:

- Aprimorar o processo decisório, a gestão de projetos, de processos e de riscos corporativos e o uso de indicadores de desempenho;
- Assegurar a infraestrutura adequada e a continuidade dos serviços.

A primeira linha de atuação citada aborda o aprimoramento da gestão dos riscos corporativos, que abarca os riscos decorrentes de ameaças à Segurança da Informação. A segunda

linha de atuação, voltada a ações que assegurem a continuidade dos serviços, carrega implícita a recomendação de adoção da gestão de riscos e da gestão da Segurança da Informação, visando à prevenção de interrupções dos serviços da Casa.

O CGSI, em sua reunião de 27 de fevereiro de 2014, agregou a essas diretrizes a seguinte visão orientadora para a elaboração deste plano:

> O Plano de Ação tem o objetivo de promover, no período dos próximos dois anos:
> » a elevação do grau de consciência quanto à Segurança da Informação na Câmara dos Deputados;
> » a implantação de mecanismos de gestão de riscos e de gestão da Segurança da Informação e
> » a redução de riscos iminentes relativos a Segurança da Informação em processos de trabalho da Casa, priorizados e destacados neste Plano.

JUSTIFICATIVA

O plano atende ao que estabelece o Ato da Mesa nº 47/2012 em seu art. 14:

> 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:
>
> ...
>
> § 1° 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

A promoção de ações que visem preservar a segurança das informações, como a orientação contida na PSI, acha-se alinhada com as atribuições estabelecidas pela Lei nº 12.527, de 18 de novembro de 2011. Ao estabelecer para a Administração a obrigação de divulgar informações de interesse público por meio de sítio da instituição na internet, a Lei de Acesso a Informação atribui às instituições do poder público as seguintes responsabilidades, nos termos de seu art. 6º:

> *Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:*
>
> *I – gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;*

> *II – proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e*
>
> *III – proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.*

Para garantir a disponibilidade e a integridade dessas informações, se faz necessária a adoção de práticas voltadas à preservação desses seus atributos de segurança. A referida lei também determina restrições para o acesso a informações pessoais e a preservação das informações que a legislação ou a autoridade competente tenha classificado como sigilosas. Assim, a restrição de acesso a informação, determinada pela lei, também impõe a adoção de práticas de Segurança da Informação.

A crescente migração para mídia eletrônica dos conteúdos informacionais antes residentes em formatos e suportes tradicionais também impõe à Administração a atenção aos riscos inerentes ao meio digital. A desmaterialização de documentos e a conversão de processos e de fluxos de trabalho para o formato digital demandam a adoção de medidas de proteção típicas da área da tecnologia da informação, de forma a tratar a segurança da informação nascida ou portada para os meios eletrônicos.

Alinham-se ainda às determinações da Lei nº 12.527 e aos Atos da Mesa nº 45/2012 e nº 47/2012, como justificativa para a elaboração do plano, as recomendações dirigidas à Administração por órgãos do controle interno e externo, tratando da necessidade de adoção de ações voltadas à Segurança da Informação.

O Tribunal de Contas da União dirigiu recomendações dessa natureza à Diretoria-Geral da Câmara dos Deputados nos seguintes acórdãos:

» Acórdão 2008-1603/TCU-Plenário – Governança de TI;

» Acórdão 2008-2471/TCU-Plenário – Terceirização de serviços de TI;

» Acórdão 2011-1145/TCU-Plenário – Governança de TI (Monitoramento do Acórdão 2008-1603/TCU-Plenário e outros);

» Acórdão 2012-1233/TCU-Plenário – Governança de TI;

» Acórdão 2012-2585/TCU-Plenário – Governança e riscos de TI.

A Secretaria de Controle Interno da Câmara dos Deputados trata aspectos da Segurança da Informação nos seguintes Relatórios de Auditoria:

» Relatório de Auditoria nº 2/2010/Calip – Processo nº 130.965/2010;

» Relatório de Auditoria nº 8/2011/Calip – Processo nº 148.638/2011;

» Relatório de Auditoria nº 01/2012/Secin – Processo nº 125.426/2012.

Também são observadas leis, regulamentos, normas e boas práticas, nacionais e internacionais, que versam sobre o tema da Segurança da Informação. As seguintes normas e quadros de referência de boas práticas contribuem para o embasamento das ações aqui propostas, voltadas ao aprimoramento da Segurança da Informação:

» ABNT NBR ISO/IEC 38.500:2009 – Governança corporativa de tecnologia da informação;

» ABNT NBR ISO/IEC 27.001:2013 – Sistema de gestão de Segurança da Informação – Requisitos;

» ABNT NBR ISO/IEC 27.002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação;

» ABNT NBR ISO/IEC 27.003:2011 – Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da Segurança da Informação;

» ABNT NBR ISO/IEC 27.005:2011 – Gestão de Riscos de Segurança da Informação;

» *Cobit 5*.

PLANO DE AÇÃO EM SEGURANÇA DA INFORMAÇÃO

Este plano está adstrito a propor à administração da Câmara dos Deputados um conjunto inicial de ações estruturantes que alicercem e amparem a gestão da Segurança da Informação em toda a Casa, alçando-a a um patamar de controles mais elevado que aquele em que hoje se encontra.

A discussão do escopo deste plano pelo CGSI principiou com uma visão ampla de levantamento de riscos conhecidos e de necessidades manifestas em Segurança da Informação em todas as áreas da Casa. Os trabalhos prosseguiram com a classificação dessas necessidades, resultando na seleção de um reduzido conjunto de ações prioritárias, formado por ações estruturantes e por ações de conformidade, consideradas passíveis de execução no espaço de tempo de dois anos a partir de sua propositura.

AÇÕES RECOMENDADAS

Recomenda-se à Diretoria-Geral da Câmara dos Deputados a implementação das seguintes ações:

A) Ações de Conformidade, em atendimento a determinações da PSI:

- » Inventário de ativos (AM 47/2012, art. 14, VIII)
- » Implantação da Gestão de Risco de Segurança da Informação (AM 47/2012, art. 8º, § 3º, VII)
- » Implantação do Sistema de Gestão da Segurança da Informação – SGSI (AM 47/2012, art. 8º, § 3º, V e VI)

B) Outras ações estruturantes de caráter prioritário, que estabelecem as fundações para futuras ações em Segurança da Informação:

» Norma sobre classificação de informações (AM nº 47/2012, art. 14, IV)

» Campanha institucional de conscientização em Segurança da Informação (AM nº 47/2012, art. 6º, II; art. 7º, V e VI; art. 13, I)

Essas ações são a seguir descritas na ordem em que são referenciadas nas normas que constituem o Código de Prática (ABNT NBR 27.002:2013) e os Requisitos de Controle em Segurança da Informação (ABNT NBR ISO/IEC 27.001:2013 – Requisitos). A ordem não indica necessariamente a sequência de execução de tais ações. A precedência das ações que constituem pré-requisito para outras está definida no tópico "8 – Priorização das Ações".

Inventário de ativos

Objetivo:

Elaborar inventário para enumerar e descrever os ativos associados a informação em toda a instituição e definir as devidas responsabilidades pela proteção desses ativos.

Descrição da ação:

Ativo é tudo aquilo que tem valor para a organização. Assim, pode-se definir ativo como qualquer elemento que sustenta um ou mais processos de trabalho de uma unidade ou de uma área da organização.

Um inventário completo deve abranger ativos pertencentes a várias categorias, por exemplo:

- Processos e atividades do negócio: processos críticos cuja interrupção impossibilita o cumprimento da missão; processos que, se modificados, podem afetar o cumprimento da missão; processos necessários para a conformidade com requisitos legais ou regulatórios; etc.;
- Ativos de Informação: informação vital para o cumprimento da missão; informação de alto custo de obtenção; informação estratégica essencial para a tomada de decisão; informação em papel, em meio digital ou qualquer outro suporte;
- Ativos de *software*: sistemas de informação, *softwares* aplicativos desenvolvidos, licenciados ou adquiridos pela organização, *software* de prateleira, sistemas operacionais, *software* básico, etc.;
- Ativos físicos: dispositivos fixos ou móveis de processamento, periféricos, mídia de armazenamento, instalações físicas, etc.;
- Serviços: serviços de computação de terceiros, rede de dados, serviço de transporte de dados (aluguel de *link*), serviço de fornecimento de energia elétrica, etc.;
- Pessoas: parlamentares, servidores ativos e inativos, CNEs, terceirizados, estagiários, pró-adolescentes, visitantes, etc.;

» Organização: autoridades, estrutura organizacional, subcontratados, fornecedores, empresas prestadoras de serviço, etc.;

» Ativos Intangíveis: imagem da instituição, reputação, credibilidade, etc.

O inventário de ativos associados a informação e aos recursos de processamento da informação deve registrar aqueles relevantes no ciclo de vida da informação e descrever a sua importância para o funcionamento da instituição. O inventário deve ainda explicar o ciclo de vida da respectiva informação: a criação, o processamento, o armazenamento, a transmissão, a exclusão e, ao fim do ciclo, se necessário, o seu descarte seguro. Os ativos devem ser qualificados também por outras informações relevantes, como localização, responsável e modo de recuperação em caso de desastre. Para cada ativo identificado no inventário, é recomendável que seja definido um responsável encarregado de manter os seus controles de segurança, com o objetivo de diminuir chances de que eles tenham a segurança comprometida.

Inventariar os ativos associados a informação e classificá-los de acordo com sua relevância para a organização e seus processos de trabalho é ação que deve preceder iniciativas como a classificação da informação e a análise de risco em Segurança da Informação.

Resultados esperados:

» Conhecimento abrangente dos ativos de informação da instituição, com definição de seus atributos e dos responsáveis por controlar sua segurança.

» Possibilidade de classificação dos ativos de informação como ostensivos, de acesso restrito ou sigilosos, com o respectivo grau de sigilo.

» Possibilidade de gestão dos riscos com base nas características dos ativos inventariados.

Tópicos de conformidade relativos a esta ação:

» Ato da Mesa nº 47/2012, art. 14, VIII;

» ABNT NBR ISO/IEC 27.002:2013, tópicos 8.1 e 8.1.1;

» ABNT NBR ISO/IEC 27.005:2013, tópico 8.2.2;

» Acórdão 2012-1233/TCU-Plenário, tópicos 9.18, 9.13.9.5 e 9.15.12.4.

Norma sobre classificação de informações

Objetivo:

Editar norma que estabeleça critérios, procedimentos e responsabilidades para a classificação das informações segundo o grau de proteção requerido, além de criar os controles voltados a garantir que o grau de proteção atribuído à informação seja efetivamente observado ao longo de seu ciclo de vida. Implantar o processo de classificação preconizado pela norma e implantar o acompanhamento dos controles nela estabelecidos.

Descrição da ação:

A classificação torna possível a adoção de medidas de proteção proporcionais à importância ou à reserva de acesso que caracteriza uma informação específica. Entre os vários critérios aplicáveis à classificação da informação, dois são particularmente importantes do ponto de vista da Segurança da Informação: o valor da informação e seu grau de sigilo. A classificação da informação quanto ao seu livre acesso, ou à restrição de acesso, ou ainda quanto ao seu grau de sigilo (reservada, secreta ou ultrassecreta), é condição necessária para que, nos casos aplicáveis, se possa preservar sua confidencialidade.

Atualmente, a classificação da informação na Casa é regida pela Resolução da Câmara dos Deputados nº 29, de 1993, conjugada às normas posteriores decorrentes da Lei de Acesso à Informação: o Ato da Mesa nº 45 de 2012, e a Portaria nº 71 de 2014. Esta normatização, contudo, não abarca a totalidade dos ativos de informação que carecem de classificação no âmbito da Casa. Assim, faz-se necessária normatização que estenda a classificação da informação, com os procedimentos e responsabilidades que a caracterizam, a todos os ativos de informação constantes do inventário da Casa.

Resultados esperados:

- Proteção das informações classificadas na proporção de seu grau de sigilo ou de restrição de acesso.
- Uso adequado e proporcional de recursos e controles de proteção de informações.

» Conscientização dos colaboradores quanto à necessidade de proteger os ativos de informação.

» Fortalecimento da cultura de Segurança da Informação.

» Atribuição de responsabilidades a quem deve classificar, quem deve proteger e quais cuidados o usuário deve tomar ao lidar com informações classificadas ou de acesso restrito.

» Provimento de elementos necessários à implantação da gestão de riscos, que depende do inventário de ativos e da classificação das informações.

» Integração de controles de confidencialidade quando o SGSI for implantado.

Tópicos de conformidade relativos a esta ação:

» Ato da Mesa nº 47/2012, art. 14, IV;

» ABNT NBR ISO/IEC 27.002:2013, tópico 8.2;

» *Cobit 5,* no processo APO01.06;

» Acórdão 2008-1603/TCU-Plenário, tópicos 9.5 e 9.1.3;

» Acórdão 2008-2471/TCU-Plenário, tópicos 9.17 e 9.6.1;

» Acórdão 2012-1233/TCU-Plenário, tópicos 9.18, 9.13.9.3 e 9.15.12.3.

Implantação de gestão de risco de Segurança da Informação

Objetivo:

Gerir os riscos relativos à Segurança da Informação, visando à redução da incerteza decorrente de ameaças a que a informação está exposta.

Descrição da ação:

A gestão de risco de Segurança da Informação consiste em um conjunto de ações e controles que visam reduzir a possibilidade de materialização de riscos a que uma informação está exposta.

O risco em relação à Segurança da Informação pode ser definido como o potencial de que uma dada ameaça explore vulnerabilidades da organização visando causar dano, perda, acesso indevido ou indisponibilidade aos ativos de informação.

A implantação da Gestão de Riscos em Segurança da Informação envolve, ao menos, as seguintes atividades:

- Capacitar servidores para a gestão de risco de Segurança da Informação.
- Selecionar metodologia de gestão de risco.
- Identificar, analisar e avaliar os riscos relativos aos ativos de informação da Câmara dos Deputados (requer a realização prévia do Inventário de Ativos).
- Tratar os riscos identificados e avaliados, modificando-os, evitando-os, compartilhando-os ou assumindo-os e, depois, documentar e comunicar os riscos assumidos às partes interessadas.
- Implantar a gestão de risco como processo organizacional, a ser realizado periodicamente em um ciclo PDCA (*Plan – Do – Check – Act*) de melhoria contínua.

Resultados esperados:

» Redução do risco de incidentes que possam resultar em perda, dano, indisponibilidade ou acesso indevido à informação.

» Redução dos custos decorrentes de incidentes.

» Aprimoramento da segurança e disponibilidade dos serviços e sistemas de TIC.

» Impacto positivo na credibilidade da instituição.

» Cumprimento de leis, regulamentos e recomendações do controle.

Tópicos de conformidade relativos a esta ação:

» Ato da Mesa nº 47/2012, art. 8º, § 3º, VII;

» ABNT NBR ISO/IEC 27.001:2013, tópicos 6.1, 8.2 e 8.3;

» ABNT NBR ISO/IEC 27.003:2011, tópico 8.1;

» ABNT NBR ISO/IEC 27.005:2011, toda a norma;

» ABNT NBR ISO/IEC 38.500:2009, tópico 9;

» *Cobit 5*, nos processos EDM03, APO12, APO13 e BAI01

» Relatório de Auditoria nº 2/2010/Calip, tópicos 2.3.7 e 2.4.8;

» Relatório de Auditoria nº 8/2011/Calip, tópico 3;

» Relatório de Auditoria nº 01/2012/Secin, tópico 3.2 e 3.2.6;

» Acórdão 2008-2471/TCU-Plenário, tópicos 9.17 e 9.6.1;

» Acórdão 2012-1233/TCU-Plenário, tópicos 9.18, 9.13.9.3 e 9.15.12.3.

Implantação de Sistema de Gestão da Segurança da Informação (SGSI)

Objetivo:

Dotar a instituição de meios para acompanhar e gerir as iniciativas em Segurança da Informação que permeiam todas as áreas, visando minimizar a ocorrência de incidentes, tais como indisponibilidade, perda, acesso indevido ou alteração indevida da informação, com foco nos controles apropriados aos processos de trabalho da Casa. Um SGSI também torna possível a certificação, por organismos independentes, da conformidade da instituição em relação às boas práticas em Segurança da Informação previstas nas normas brasileiras.

Descrição da ação:

O Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de ações e controles que administram a Segurança da Informação, incluindo recursos humanos, infraestrutura e processos, com o intuito de prover indicadores para acompanhamento das ações. O sistema possibilita a redução de incidentes de Segurança da Informação a um nível aceitável, em atendimento às diretrizes estratégicas, às necessidades do público interno da instituição e às expectativas da sociedade.

A partir de uma lista de controles definidos na norma brasileira (ABNT NBR ISO/IEC 27.001:2013), elabora-se uma Declaração de Aplicabilidade da qual constem somente aqueles controles que se aplicam às necessidades da instituição e aos seus processos de negócio. Esses controles são então implantados e monitorados.

A gestão da Segurança da Informação deve constituir um processo em permanente execução, contemplando as fases de um ciclo PDCA (*Plan – Do – Check – Act*) de melhoria contínua.

A concepção e implementação de um SGSI são influenciadas pelas necessidades e objetivos de cada organização e também por seus requisitos de segurança, seus processos de trabalho

e seu tamanho e estrutura. A implantação do SGSI deve ser precedida por um levantamento que permita sua contextualização e delimitação de escopo, envolvendo, no mínimo:

» O entendimento e descrição da organização e avaliação de seu contexto, tanto interno quanto externo, uma vez que o contexto pode influenciar significativamente a estrutura para gestão de riscos;

» A determinação das partes interessadas relevantes e seus requisitos e necessidades acerca da Segurança da Informação;

» A determinação do escopo do SGSI, considerando o contexto, as partes interessadas, seus requisitos de Segurança da Informação e as interfaces e dependências da instituição com outras organizações.

Um SGSI deve ser dinâmico e deve evoluir em conjunto com os objetivos estratégicos de segurança da organização. É recomendável que a implementação de um SGSI se baseie nas normas brasileiras ABNT NBR ISO/IEC 27.001:2013, ABNT NBR ISO/IEC 27.002:2013 e ABNT NBR ISO/IEC 27.005:2011.

Resultados esperados:

» Alinhamento dos objetivos de Segurança da Informação com os objetivos corporativos.

» Acompanhamento, pela administração, do desempenho das ações relativas à Segurança da Informação em toda a instituição.

» Adoção de controles para o aprimoramento da disponibilidade, da integridade e da confidencialidade das informações, com o consequente ganho para a segurança dos processos de trabalho que delas dependem.

» Redução de ocorrência de incidentes de Segurança da Informação.

» Redução dos custos decorrentes de incidentes de Segurança da Informação.

» Proteção a informações pessoais, informações sigilosas, aos serviços prestados ao público interno e à sociedade brasileira.

» Melhoria nos níveis de confiança dos usuários e da sociedade quanto ao tratamento da informação pela instituição.

» Controle abrangente sobre todos os aspetos relacionados com a Segurança da Informação, não se limitando às questões tecnológicas.

» Conformidade da instituição com leis, regulamentos, normas e recomendações dos órgãos de controle.

» Implantação de um processo de melhoria contínua da Segurança da Informação.

» Confirmação do comprometimento da alta direção na segurança de suas informações.

» Possibilidade de certificação, por instituição independente, dos controles de Segurança da Informação implantados e de atendimento aos requisitos de governança corporativa da Segurança da Informação.

» Melhoria da imagem da instituição.

Tópicos de conformidade relativos a esta ação:

» Ato da Mesa nº 47/2012, art. 6º, II; art. 7º, V, VI e art. 13, I;

» ABNT NBR ISO/IEC 27.001:2013, toda a norma;

» ABNT NBR ISO/IEC 27.003:2011, toda a norma;

» *Cobit* 5, no processo APO13.01.

Campanha institucional de conscientização em Segurança da Informação

Objetivo:

Assegurar a conscientização de parlamentares, servidores, estagiários, pró-adolescentes, prestadores de serviço e fornecedores em relação a responsabilidades e atitudes no sentido de preservar a Segurança da Informação no âmbito da Câmara dos Deputados.

Descrição da ação:

A ação de sensibilização dos colaboradores ao tema da Segurança da Informação é iniciativa fundamental para torná-los cientes das suas responsabilidades e conhecedores das práticas e métodos aplicáveis à proteção da informação. É importante que os conceitos e a relevância da Segurança da Informação passem a fazer parte da cultura organizacional por uma campanha permanente que promova essa transformação.

A campanha deve estar alinhada com as políticas e os procedimentos relevantes para a proteção da disponibilidade, da integridade e, quando for o caso, da confidencialidade dos ativos de informação. Deve divulgar a importância da informação para a instituição, o comprometimento da direção com a preservação da Segurança da Informação, as responsabilidades estabelecidas na Política de Segurança da Informação para as unidades administrativas e para os usuários, além dos procedimentos e controles a serem adotados com vistas à proteção da informação.

Uma campanha, para ser efetiva, requer o emprego de diferentes formas de comunicação da informação, como ciclos de palestras, cartazes, folhetos, notas informativas, boletins periódicos e sítio intranet sobre o tema. Deve levar em conta os diferentes papéis desempenhados pelos colaboradores na instituição. Deve ainda prever que as ações de conscientização sejam revistas regularmente, de forma a atingir novos colaboradores que passem a integrar os quadros da instituição. É recomendável que a campanha contemple sensibilização específica para os colaboradores que venham a ocupar novas posições na instituição, preferencialmente antes de assumirem as novas atribuições.

A própria campanha deve ser atualizada regularmente, de modo a permanecer alinhada com as políticas e os procedimentos da instituição e incorporar lições aprendidas a partir de incidentes de Segurança da Informação reais vividos pela instituição.

Resultados esperados:

» Colaboradores conscientes da importância de se preservar a Segurança da Informação em seus processos de trabalho e treinados em como mantê-la.

» Redução da ocorrência de incidentes de Segurança da Informação.

Tópicos de conformidade relativos a esta ação:

» ABNT NBR ISO/IEC 27.002:2013, tópico 7.2.2;

» *Cobit* 5, no processo APO13.2 e DSS06.03, atividade 5.

BENEFÍCIOS ESPERADOS

As ações recomendadas neste plano almejam a conquista de um conjunto de benefícios para os processos de trabalho da Casa, com desdobramentos positivos para os serviços prestados à sociedade. Destacam-se, entre esses benefícios esperados:

» Alinhamento dos objetivos em Segurança da Informação com as diretrizes estratégicas e as linhas de atuação da Câmara dos Deputados;

» Conhecimento dos riscos de segurança que podem afetar os ambientes e os processos de trabalho nos quais a informação é criada, tratada ou mantida;

» Capacidade de identificar, avaliar e tratar os riscos aos quais a informação possa estar exposta;

» Alocação adequada dos recursos para o tratamento de riscos;

» Proteção da informação, de forma a preservar sua disponibilidade, sua integridade e, quando for o caso, sua confidencialidade, no grau que atenda às necessidades da instituição;

» Aprimoramento dos controles, reduzindo os riscos identificados, mediante o estabelecimento de nível de segurança adequado à criticidade dos processos de negócio envolvidos;

» Melhoria na conscientização dos colaboradores da Casa quanto à sua responsabilidade, à conduta adequada e ao comportamento desejável em relação à preservação da Segurança da Informação;

» Criação de regulamentos e procedimentos com o objetivo de orientar os usuários quanto às melhores práticas de uso e proteção da informação;

» Prevenção de incidentes de Segurança da Informação que possam ser danosos aos processos de trabalho da Casa, à imagem da instituição e aos serviços prestados à sociedade;

» Preservação da disponibilidade dos serviços de Tecnologia da Informação (TI) usados pela instituição e pela sociedade;

» Atendimento aos requisitos de governança corporativa relacionados à Segurança da Informação e à gestão de riscos;

» Atendimento às leis, às normas e às recomendações dos órgãos de controle quanto à Segurança da Informação;

» Adoção dos controles e processos necessários para a certificação, por organismo independente, da implantação de um Sistema de Gestão da Segurança da Informação pela instituição;

» Fortalecimento da imagem da instituição perante a sociedade, os parlamentares, os servidores, os prestadores de serviço e as demais instituições com as quais interage.

PRIORIZAÇÃO DAS AÇÕES

Entre as ações aqui propostas, algumas mantêm vínculo de precedência entre si: a *análise de riscos*, para ser efetiva, necessita dispor do resultado da *classificação das informações*. A *classificação*, por sua vez, para ser abrangente, deve ser precedida pelo *inventário de ativos*. Assim, recomenda-se que essas três ações sejam adotadas seguindo-se esta ordem de precedência:

1) Inventário de ativos
2) Classificação de informações
3) Gestão de risco

A implantação do Sistema de Gestão de Segurança da Informação é condicionada aos requisitos de contexto organizacional tratados no tópico "Implementação de Sistema de Gestão de Segurança da Informação (SGSI)" deste plano, os quais devem ser determinados antes que se inicie o planejamento desta ação.

A Campanha de Conscientização em Segurança da Informação não está condicionada a outras iniciativas. É ação que pode ser principiada a qualquer momento, sendo recomendável que seu início ocorra o quanto antes, por ser uma das ações em Segurança da Informação que resulta em benefício mais imediato e efetivo.

ACOMPANHAMENTO DAS AÇÕES

O CGSI propõe que seja feito, trimestralmente, o acompanhamento das ações aqui recomendadas, por meio de solicitação de informações às áreas responsáveis por desenvolver as ações propostas neste plano.

Se acatada essa proposta, o CGSI produzirá, a cada avaliação trimestral, um relatório de acompanhamento do plano de ação, a ser encaminhado à alta administração, com informações consolidadas acerca do andamento das ações.

CONSIDERAÇÕES FINAIS

A Política de Segurança da Informação da Câmara dos Deputados constitui marco na evolução da proteção à informação na Casa. Por meio da PSI, a alta administração afirma a importância da informação como recurso imprescindível para o cumprimento da missão institucional, define prioridades em Segurança da Informação e exorta os colaboradores e aos órgãos que compõem a Câmara dos Deputados a zelarem para que a informação tenha preservadas suas qualidades de integridade, disponibilidade e, quando aplicável, confidencialidade.

Todavia, para que a PSI constitua um instrumento efetivo de promoção da Segurança da Informação, é preciso que as iniciativas previstas na norma se concretizem. As ações que este plano propõe são os passos iniciais rumo a uma cultura de proteção à informação, a ser formada por meio da conscientização dos colaboradores e da implantação de processos que privilegiem o tratamento seguro da informação.

Considerando os benefícios decorrentes das ações aqui propostas, o CGSI manifesta a expectativa de que a Administração acolha este Plano de Ação em Segurança da Informação, reconheça o seu caráter estratégico para os processos de trabalho da Casa e que, consequentemente, priorize a implementação das ações no contexto do planejamento da Câmara dos Deputados.

Subscrevem este plano os integrantes do Comitê Gestor de Segurança da Informação da Câmara dos Deputados:

Bruno Paiva Menezes

Cláudia Cristina Aires Gomes

Fabiano Peruzzo Schwartz

Fábio Sérgio Cruz

Flávio Gomes de Mesquita

Gustavo Vasconcellos Cavalcante

José Cláudio Conceição de Aguiar

Laila Moreira Machado

Lamberto Ricarte Serra Júnior

Luiz Humberto Ferreira Carneiro

Malva Beatrice Machado Algarte

Rosinaldo Dourado da Fonseca Júnior

Sandra Silva Maia

Sérgio Dagnino Falcão

Vanderlei Batista dos Santos

GLOSSÁRIO

Ameaça

Causa potencial de um incidente indesejado, que pode comprometer os ativos (como informações, processos e sistemas) e, consequentemente, resultar em dano para as organizações. Ameaças podem ser de origem natural ou humana, podem ser acidentais ou intencionais e podem surgir de dentro ou de fora da organização.

Ativo

Algo ou característica, tangível ou intangível, que tenha valor para a organização e que, portanto, requeira proteção. São exemplos de ativos: instalações físicas, *hardware*, s*oftware*, informações, redes de computadores, processos organizacionais, estrutura organizacional, recursos humanos, serviços utilizados pela organização, imagem da organização, etc.

Ativo de informação

É a informação em si, os sistemas de informação, os meios de armazenamento, transmissão e processamento dessa informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Autenticidade

Atributo da informação que permite atestar sua proveniência, veracidade e fidedignidade, garantindo que a informação não tenha sofrido mutações ao longo de um processo.

Ciclo PDCA

Método interativo de gestão, utilizado para controle e melhoria contínua de processos e produtos. O ciclo PDCA é composto de quatro etapas:

» P (*Plan*, Planejar) – desenhar ou revisar os processos organizacionais;

» D (*Do*, Fazer) – executar o que foi planejado e gerenciar o processo;

» C (*Check*, Verificar) – medir e comparar o resultado obtido em relação ao resultado esperado;

» A (*Act*, Agir) – realizar as mudanças visando a melhorias no processo.

Cobit 5

O Cobit 5 é um guia de referência para a governança e a gestão da tecnologia da informação e comunicação (TIC) no ambiente corporativo. Ele visa promover a adequação dos investimentos em TIC, garantir a entrega de tais serviços e prover métricas para o acompanhamento do desempenho da governança e da gestão de TIC na organização. O Cobit 5 consolida as boas práticas em um modelo de domínios e processos com as práticas congregadas em uma estrutura lógica e gerenciável. As boas práticas contidas no Cobit representam o consenso de especialistas em governança e gestão de TIC em todo o mundo.

Comitê Gestor de Segurança da Informação (CGSI)

Grupo multidisciplinar que reúne representantes das diversas áreas da Câmara dos Deputados, indicados pelas suas respectivas diretorias e secretarias, e aprovados pela alta administração, com o papel de promover e acompanhar as estratégias para implantação e manutenção da análise de riscos, da normatização, de um Sistema de Gestão de Segurança da Informação e das demais iniciativas relativas à segurança da informação. O CGSI foi instituído em conformidade com o art. 6º do Ato da Mesa nº 47, de 16 de julho de 2012, que estabeleceu a Política de Segurança da Informação da Câmara dos Deputados. Suas competências estão definidas no § 3º do art. 6º desse Ato.

Confidencialidade

Atributo que define o grau de sigilo ou de restrição de acesso definido em lei ou atribuído por autoridade competente a um dado, a uma informação ou a um documento.

Declaração de Aplicabilidade

Documento no qual a organização relaciona quais controles de segurança da informação recomendados pela norma ANBT/NBR ISO/IEC 27001:2013 são aplicáveis a seus processos de trabalho e ativos de informação. Esses controles devem compor o Sistema de Gestão de Segurança da Informação (SGSI). A Declaração de Aplicabilidade também enumera os controles que não são aplicáveis aos processos e ativos da organização, com as devidas justificativas.

Disponibilidade

Atributo que define que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Gestão de risco

Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

Governança corporativa

Sistema pelo qual as organizações são dirigidas e controladas.

Incidente

Evento simples ou série de eventos indesejados, inesperados ou adversos, que tenham probabilidade de comprometer um ou mais princípios básicos de segurança da informação: confidencialidade, integridade e disponibilidade.

Informação reservada

A informação classificada como reservada tem prazo máximo de restrição de acesso de 5 (cinco) anos a partir da data de sua produção (art. 24, III, da Lei nº 12.527/2011).

Informação secreta

A informação classificada como secreta tem prazo máximo de restrição de acesso de 15 (quinze) anos a partir da data de sua produção (art. 24, II, da Lei nº 12.527/2011).

Informação sigilosa

É aquela submetida temporariamente a restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado (art 4º, III, da Lei nº 12.527/2011).

Informação ultrassecreta

A informação classificada como ultrassecreta tem prazo máximo de restrição de acesso de 25 (vinte e cinco) anos a partir da data de sua produção (art. 24, I, da Lei nº 12.527/2011).

Integridade

Atributo da informação que se encontra completa e que não sofreu nenhum tipo de dano ou alteração não autorizada, não documentada ou acidental.

Política de Segurança da Informação

Conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

Restrição de acesso

A Lei de Acesso a Informação prevê os seguintes casos de restrição de acesso a informação, tendo como princípio a observância da publicidade como preceito geral e do sigilo como exceção (art 3º, I, da Lei nº 12.527/2011):

- Quando uma informação for declarada sigilosa pelas autoridades competentes, por ter sido considerada imprescindível à segurança da sociedade e do Estado (art. 24 da Lei nº 12.527/2011);
- Quando se tratar de informações pessoais, ou seja, aquelas relativas à intimidade, vida privada, honra e imagem de um indivíduo (art. 31 da Lei nº 12.527/2011);
- Quando as informações forem consideradas de acesso restrito em razão das demais hipóteses legais de sigilo (art. 22 da Lei nº 12.527/2011).

As informações pessoais terão seu acesso restrito à própria pessoa, a alguém por ela autorizada ou a agentes públicos legalmente autorizados pelo prazo máximo de 100 (cem) anos a contar da sua data de produção (art. 31 da Lei nº 12.527/2011).

Risco

Resultado da combinação entre a probabilidade de ocorrência de um determinado evento e o impacto resultante, caso ele ocorra.

Segurança da Informação

Proteção da informação frente a ameaças que podem comprometer seus atributos de integridade, disponibilidade, autenticidade e confidencialidade, com o objetivo de resguardar o valor que a informação possui para um indivíduo ou uma organização.

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.

Vulnerabilidade

Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Conheça outros títulos da Edições Câmara no portal da Câmara dos Deputados:
www.camara.leg.br/editora