RELATÓRIO DE AUDITORIA N. 1/2017

1 INTRODUÇÃO

Trata-se de relatório de auditoria previsto no Plano Anual de Controle Interno (PACI) de 2016 desta Secretaria, com o objetivo de avaliar a gestão da segurança da informação na Câmara dos Deputados sob o prisma do processo COBIT 5 APO01 – Gerenciar a estrutura de Gestão de TI. Essa análise foi feita usando-se a prática de gestão APO01.06 – Definir proprietários da informação e dos sistemas, que tem como finalidade, resumidamente, definir e manter responsabilidades pela custódia da informação e de sistemas de informação com vistas a garantir a segurança de ambos.

1.1 Apresentação

2. A partir do mapa de riscos do processo APO01 e, mais especificamente, do risco "R_016-04 – Falhas nos mecanismos de proteção e resguardo de informações classificadas como sigilosas"[1], esta ação de controle foi pautada pela verificação da execução do Plano de Ação de Segurança da Informação (PASI), criado em observância ao disposto no artigo 14, § 1º, do Ato da Mesa n. 47/2012[2], e posteriormente aprovado pelo Diretor-Geral em março de 2015, conforme processo n. 102.148 do mesmo ano. O relatório de auditoria n. 1/2015 (processo n. 133.172/2015), baseado no processo COBIT 5 DSS05 - Gerir serviços de segurança, já havia registrado a criação do PASI e a sua submissão à alta gestão da Casa.

3. O trabalho de levantamento das ações previstas no PASI culminou no envio de e-mail à Diretoria-Geral, em 27 de outubro de 2016, com solicitação de justificativas para as seguintes questões:

- a ausência de inventário de ativos de informação; e

[1] Conforme cadastrado no Sicoi – Sistema de Gestão de Ações de Controle Interno.
[2] Institui a Política de Segurança da Informação da Câmara dos Deputados.

- a ausência de associação entre políticas e diretrizes para a classificação da informação e inventário de ativos.

4. Uma vez que ainda durante os trabalhos de auditoria foram observadas ações pertinentes da gestão no tocante a mitigar os riscos associados a esses dois temas, tais questões serão apontadas em notas de auditoria (v. seção 4 deste relatório), sem a necessidade de suscitar pontos de auditoria nem consequentes recomendações.

5. No dia 22 de novembro de 2016, em reunião com os membros do Núcleo de Auditoria de TI, o Comitê Gestor de Segurança da Informação (CGSI[3]) afirmou que a resposta à solicitação de esclarecimentos, então em elaboração, seria formalizada por meio de processo, tendo em vista a relevância do tema e seu alcance na Casa.

6. De fato, em 16 de janeiro de 2017, a Secretaria de Controle Interno recebeu o processo n. 130.508/2016 com os esclarecimentos às duas questões anteriormente citadas, consignados em texto intitulado “Relatório sobre Implementação de Ações Previstas no Plano de Ação de Segurança da Informação” (fl. 2-4v.), produzido pelos membros do Comitê Gestor de Segurança da Informação e assinado por seu coordenador.

2 BOAS PRÁTICAS ADMINISTRATIVAS OBSERVADAS

7. Plano de Ação de Segurança da informação, formalizado e aprovado pela Diretoria-Geral (Processo n. 102.148/2015).

8. Comitê Gestor de Segurança da Informação, criado pelo Ato da Mesa n. 47/2012, que instituiu a Política de Segurança da Informação da Casa.

3 CRITÉRIOS UTILIZADOS

9. A partir do mapa de riscos do processo COBIT 5 APO01 e, mais especificamente, do risco "R_016-04 – Falhas nos mecanismos de proteção e resguardo de informações classificadas como sigilosas", foram utilizados os seguintes critérios para esta ação de controle:

[3] Criado pelo Ato da Mesa n. 47/2012, que instituiu a Política de Segurança da Informação da Câmara dos Deputados. É composto por um servidor como representante de cada uma das seguintes unidades administrativas da Casa: Diretoria-Geral, Secretaria Geral da Mesa, Diretoria Legislativa, Diretoria Administrativa, Diretoria de Recursos Humanos, Secretaria de Comunicação Social, Centro de Documentação e Informação e Centro de Informática. A composição do CGSI para o biênio 2016/2018 foi designada pela Portaria n. 214/2016, da Diretoria-Geral.

- Ato da Mesa n. 46/2012 – Institui a Política de Gestão de Conteúdos Informacionais da Câmara dos Deputados;
- Ato da Mesa n. 47/2012 – Institui a Política de Segurança da Informação (PSI) da Câmara dos Deputados; e
- Plano de Ação de Segurança da Informação da Câmara dos Deputados.

4 NOTAS DE AUDITORIA

10. A nota de auditoria tem por finalidade registrar situação encontrada que, em um primeiro julgamento, é entendida como risco à organização, mas, caso tenha sido devidamente justificada ou prontamente corrigida pelo auditado ao longo dos trabalhos, perde esse caráter.

11. A nota de auditoria, desse modo, diferencia-se do ponto de auditoria por apresentar fato ou situação que, em última análise, não oferece risco à Casa, uma vez que já se encontra endereçada pelos gestores e, por esse motivo, não enseja a expedição de recomendações. Além disso, deixa consignada a eficiência da gestão, quer seja em seus controles internos, quer seja em suas ações corretivas.

12. No presente relatório, são apresentadas duas notas de auditoria, as quais contemplam situações que foram justificadas pela gestão da Casa, mais especificamente, pelo CGSI, no processo n. 130.508/2016.

4.1 Ausência de inventário de ativos de informação

13. O CGSI assim justifica (processo n. 130.508/2016, fl. 3v.):

> Pode-se considerar, portanto, que há, na Casa, um Inventário de Ativos de TIC que, com alguns aprimoramentos, **pode se converter em um Inventário de Ativos de Informação**, permitindo que nele se registrem atributos como os responsáveis por determinado ativo de configuração e a criticidade e o grau de sigilo requerido pelo ativo, criando assim o alicerce para que se proceda e se registre o resultado da classificação do ativo**, procedimento esse a ser estabelecido em norma** (grifos nossos).

4.2 Ausência de associação entre políticas e diretrizes para a classificação da informação e inventário de ativos

14. O CGSI destacou ações implementadas pelo Centro de Documentação e Informação e pelo Comitê Assessor da Lei de Acesso à Informação relacionadas à classificação e ao tratamento de informação com restrição de acesso na Câmara dos Deputados (processo nº 130.508/2016, fls. 3v-4).

15. O Comitê afirma ainda que (fl, 4v):

> [...]
>
> Em complemento a essas ações já realizadas, a Direção do Centro de Documentação e Informação – CEDI informou que, para o biênio 2016-2017, pretende atualizar seu inventário de ativos organizacionais físicos, elaborado em 2012, a fim de analisar aspectos sobre a sensibilidade e a criticidade das informações que os compõem.

16. Além disso, vale mencionar o despacho da Assessoria de Projetos e Gestão (processo n. 130.508/2016, fl.10):

> [...]
>
> Acrescentamos que o direcionamento estratégico e a priorização das ações relacionadas à gestão de informações, incluindo a segurança da informação, serão estabelecidos no Plano Plurianual de Gestão de Conteúdos Informacionais da Câmara dos Deputados, previsto no art. 7º do Ato da Mesa n. 46 de 2012, a ser desenvolvido em 2017, conforme decisão do Comitê Estratégico de TI na reunião de 21/12/2016.

4.3 Análise

17. Depreende-se das justificativas supracitadas dois aspectos principais:

- existe a percepção pelo CGSI de que o inventário de ativos informacionais da Câmara dos Deputados realmente não está completo, sendo o Inventário de Ativos de TIC apenas um subconjunto de universo mais abrangente;
- tal percepção está associada a ações planejadas para o ano de 2017 com o intuito de preencher a lacuna existente, não só em termos de ativos de informação, mas também com a proposição de normas e diretrizes que deem o amparo formal e institucional imprescindível a tema de relevância como Segurança da Informação.

18. Convém destacar que, em ação de controle prevista no Plano Anual de Controle Interno para o segundo semestre deste ano, intitulada “Avaliar o processo de gestão da estratégia e da governança institucional”, projetos, ações e respectivos indicadores, metas e resultados relacionados à segurança da informação da Casa poderão ser abrangidos.

5 BENEFÍCIOS DA AÇÃO DE CONTROLE

19. Tendo em vista seu grande potencial de agregar valor à gestão da informação e do conhecimento na Câmara dos Deputados, os benefícios elencados no próprio Plano de Ação de Segurança da Informação (fl. 31-32) também constituem foco para esta ação de auditoria. São eles:

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

6 CONCLUSÃO

20. Os avanços desta Casa nos processos de gestão e de governança corporativa, com relação aos aspectos de segurança da informação, resultaram na definição da Política de Segurança da Informação (PSI) em 2012 e, no ano seguinte, na criação do Comitê Gestor de Segurança da Informação (CGSI).

21. Após alentado trabalho, o CGSI concluiu em 2014 o Plano de Ação de Segurança da Informação (PASI), aprovado pela Diretoria-Geral em 2015, que contempla as ações prioritárias previstas na PSI, além de outras ações de caráter estruturante, baseadas em normativos e guias de referência relacionados ao tema. Esse conjunto de ações, uma vez concretizado e em conjunto com outras iniciativas, como a gestão de riscos, proporcionará a mitigação de riscos relacionados à segurança da informação, ao mesmo tempo que estabelecerá as bases para a adoção de outras ações que assegurem a contínua evolução nos níveis de proteção e disponibilidade da informação registrada, produzida, recebida, adquirida, capturada ou colecionada por esta Casa (Ato da Mesa n. 47 de 2013, art. 3º, V).

22. A presente ação de controle analisou a implementação de duas das ações previstas no PASI, selecionadas a partir do mapa de riscos do processo COBIT 5 APO01 - Gerenciar a estrutura de Gestão de TI, e observou que os resultados esperados pelas duas ações foram contemplados de forma parcial por outras atividades não derivadas diretamente do plano. Entretanto, observou-se

adicionalmente que a gestão corporativa da Casa, com apoio do CGSI, iniciou as medidas necessárias para execução plena das ações previstas no PASI.

23. Nesse sentido, pela adoção tempestiva de providências para complementar os resultados das ações analisadas, optou-se pelo registro das lacunas identificadas em duas notas de auditoria, para as quais não são necessárias recomendações, conforme descrito no item 3 deste relatório.

24. Dada a relevância do tema, reitera-se a importância da priorização das ações previstas no PASI pelas diversas instâncias administrativas envolvidas, coordenadas pela alta gestão, garantindo assim a sua execução tempestiva, além da adoção de outras ações relacionadas que se mostrarem necessárias.

25. Registra-se que novas ações de controle devem revisitar o tema segurança da informação no intuito de contribuir para o aperfeiçoamento da gestão e da governança corporativa desta Casa.

26. Por fim, agradece-se ao CGSI, à Direção do Centro de Informação e Documentação, do Centro de Informática, da Assessoria de Projetos e Gestão e ao Gabinete da Diretoria-Geral pelo empenho em prover as respostas e esclarecimentos essenciais aos trabalhos ora relatados.

Brasília, 20 de fevereiro de 2017.