



## Relatório de Auditoria n. 1/2019

### 1. Introdução

Trata-se de relatório de auditoria realizada em conformidade com o Plano Anual de Controle Interno (Paci) de 2019 desta Secretaria, com foco no processo “Prover Solução de TIC”. Como parâmetro para subsidiar a avaliação, foi utilizado o processo BAI03 do Cobit 5 – Gerenciar identificação e construção de soluções de TIC<sup>1</sup>.

2. De acordo com o referido modelo, o processo BAI03 tem como principal objetivo implantar soluções tempestivas, efetivas em termos de custo e capazes de suportar os objetivos tanto operacionais quanto estratégicos da organização.

3. O modelo Cobit 5 preconiza ainda que esse processo guarda relação direta com o objetivo de TIC de prover serviços condizentes com os requisitos de negócio da organização. Dessa forma, o processo BAI03 ampara, com outros processos, os seguintes objetivos corporativos:

- a. agregar valor<sup>2</sup> aos investimentos realizados;
- b. possuir cultura de prestação de serviços orientada ao cliente;
- c. responder rapidamente em face de um ambiente mutável;
- d. otimizar a funcionalidade dos processos de negócio.

4. Vale lembrar ainda que o Cobit 5 foi adotado pela gestão desta Casa e pela Secin como um modelo de referência de governança e de gestão de TIC. Ele foi desenvolvido e é mantido pela *Information Systems Audit and Control Association* (ISACA), tendo por objetivo auxiliar as organizações a atingir seus objetivos de governança e de gestão de TIC corporativas. Mais especificamente, auxilia as organizações a criar valor a partir da TIC, mantendo o melhor equilíbrio

---

<sup>1</sup> Cobit 5 – Modelo Corporativo para Governança e Gestão de TI da Organização, Isaca, 2012

<sup>2</sup> Segundo o Cobit 5, o conceito de valor está associado à entrega de benefícios no prazo e com a qualidade acordada, com a otimização dos recursos e dos riscos associados.

possível entre a busca de resultados, os riscos envolvidos e a utilização de recursos.

5. No apêndice A, é descrita uma visão geral do processo “Prover Solução de TIC” na Câmara dos Deputados.

## **2. Abordagem da auditoria**

6. Durante o processo de elaboração do Plano Anual de Controle Interno (Paci) 2019, em conjunto com a Diretoria de Inovação e Tecnologia da Informação (Ditec), o Núcleo de Auditoria em Tecnologia da Informação (Nuati) identificou os principais riscos do referido processo, a saber:

- a. áreas de negócio não assumem a responsabilidade sobre os assuntos de TIC que deveriam assumir, tais como: requisitos funcionais, prioridades de desenvolvimento e avaliação de oportunidades por meio de novas tecnologias;
- b. baixa alocação de recursos à etapa de estudo da solução; e
- c. baixo envolvimento e baixa tempestividade dos gestores de negócio durante todo o ciclo de construção da solução.

7. Posteriormente, mais uma vez em acordo com a Ditec, os riscos das alíneas a e c foram considerados conjuntamente, por serem similares. Desta forma, os principais riscos do processo passaram a ser apenas os dois primeiros listados acima (alíneas a e b).

8. A perspectiva de atuação da auditoria nesse processo foi baseada na ação de controle do tipo “Avaliação da adequação do gerenciamento corporativo de riscos”, previsto no Estatuto de Controle Interno<sup>3</sup>.

9. Em função da escolha dessa abordagem, outro critério aplicado na presente avaliação é o processo Cobit 5 APO12 – Gerenciar Riscos. Esse processo se destina a identificar, avaliar e reduzir continuamente o risco

---

<sup>3</sup> Estatuto de Controle Interno, Secretaria de Controle Interno, Câmara dos Deputados, p. 14. Disponível em: [http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/35419/estatuto\\_controle\\_interno.pdf](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/35419/estatuto_controle_interno.pdf). Acesso em: 31 jul. 2019.



relacionado a TIC dentro dos níveis de tolerância definidos pela gestão executiva da organização.

10. Desta forma, além dos riscos inerentes ao processo de construção de solução de TIC (BAI03), foram considerados também riscos em relação ao processo de gerenciamento de riscos (APO12).

11. Vale destacar que, na presente ação de controle, a avaliação do processo APO12 se resume aos aspectos relacionados à construção de soluções de TIC (processo BAI03). Em outras palavras, a avaliação sobre o processo de gestão de riscos foi limitada, com escopo restrito ao gerenciamento de riscos ligados ao processo “Prover Solução de TIC”.

12. No âmbito da Ditec, o processo APO12 é coberto, em grande parte, pelo processo “Gerir Riscos de TIC”, descrito de forma resumida no apêndice B.

13. Os riscos selecionados para avaliação nesse aspecto (gestão de riscos) foram extraídos diretamente da descrição da ação de controle do tipo “Avaliação da adequação do gerenciamento de riscos corporativo”, constante do Estatuto de Controle Interno, adaptando-os ao contexto da presente auditoria. Os riscos são os seguintes:

- a. os objetivos do processo “Prover Solução de TIC” não suportam ou não estão alinhados com a missão da Casa;
- b. os riscos significativos do processo “Prover Solução de TIC” não são identificados e avaliados;
- c. as respostas aos riscos não são selecionadas de forma a manter o alinhamento com o apetite de risco da Ditec e da Casa; e
- d. as informações quanto aos riscos relevantes não são capturadas e comunicadas de forma oportuna pela Ditec, impedindo que os servidores e a administração cumpram com suas responsabilidades.

14. Somando-se esses quatro riscos aos dois principais riscos inerentes ao processo BAI03, listados anteriormente (após exclusão do terceiro risco, por ser muito semelhante ao primeiro), temos um conjunto de seis riscos considerados na auditoria.

15. Na presente ação de controle, tais riscos foram avaliados, identificando-se os principais controles internos administrativos existentes para mitigá-los. Os controles, por sua vez, foram avaliados em relação ao seu desenho, implementação e efetividade operacional. E por fim foram realizados testes substantivos, analisando-se a efetiva ocorrência dos eventos relatados nos riscos em soluções de TIC entregues pela Ditec no decorrer do ano de 2018.

16. Vale ainda lembrar que o processo BAI03 já foi auditado por esta Secin no ano de 2016, trabalho que resultou no Relatório de Auditoria Nuati n. 01/2016.

17. Naquela ocasião, foram expedidas três recomendações à gestão, a saber:

- a. recomendação 3.1.8 (RA Nuati n. 01/2016, fl. 3v.): Recomendar ao Comitê Estratégico de Tecnologia da Informação e Comunicação (Ceti) que apresente plano de ação para normatização do processo de contratação de soluções de TI, em complemento aos trabalhos do GT criado pela Portaria Dirad n. 125, de 21 de julho de 2015, nos moldes da IN 4/2014-SLTI/MP;
- b. recomendação 3.2.8 (RA Nuati n. 01/2016, fl. 6): Recomendar ao Ceti que apresente plano de ação visando normatizar a participação da alta administração, do gestor de negócio, do gestor de permissões e do gestor técnico no processo de provimento de soluções de TI, à luz do estabelecido pelo Ato da Mesa n. 47/2012, de forma integrada à recomendação disposta no ponto anterior; e
- c. recomendação 3.3.8 (RA Nuati n. 01/2016, fl. 7): Recomendar ao Centro de Informática que apresente plano de ação no sentido de aumentar o grau de adesão de suas equipes de desenvolvimento e manutenção de sistemas ao processo Siga-me.

18. Em monitoramento realizado no ano de 2017, tais recomendações foram consideradas atendidas.



19. É importante salientar que esta ação de controle complementa a realizada anteriormente, abordando outras questões, em especial o tema do gerenciamento de riscos no que diz respeito ao processo de provimento de solução de TIC.

20. Desta forma, a equipe de auditoria listou os possíveis controles internos administrativos, reais e potenciais, que serviriam para mitigar os seis riscos identificados. Essa lista de controles foi validada e complementada pela Ditec.

21. Posteriormente, os controles listados foram avaliados quanto à sua implementação, desenho e efetividade operacional.

22. Por fim, foram realizados testes substantivos, que consistiram na avaliação de uma amostra de onze soluções de TIC efetivamente entregues pela Ditec no ano de 2018, identificando-se para quais delas os riscos apontados efetivamente se materializaram.

23. Para isso, foram analisadas atas de reuniões de comitês, documentos relativos a cada um dos projetos, e as respostas a um questionário enviado a cada um dos gerentes de projetos.

### **3. Boas práticas administrativas observadas**

24. No decorrer da ação de controle, durante a avaliação dos controles internos administrativos, foram identificadas boas práticas de gestão, que efetivamente contribuem para a mitigação dos riscos identificados. As principais são as seguintes:

- a. reuniões de comitês (CDTI, CETI e CGE), cujas atas demonstram a análise e decisões sobre riscos identificados em projetos que se destinam ao provimento de soluções de TIC;
- b. metodologia de projetos com artefatos que contemplam campos específicos voltados à identificação de riscos, a exemplo do Termo de Abertura, Declaração de Escopo e Relatório de Situação;

- c. política corporativa de gestão de riscos formalmente adotada (Ato da Mesa n. 233/2018);
- d. implantação, ainda que em estágio de testes, de metodologias ágeis para gestão de projetos, que podem aumentar a interação entre a área de negócio e a área técnica no desenvolvimento de soluções; e
- e. normativo relativo a papéis e responsabilidades no que diz respeito ao provimento de soluções de TIC (aprovado no decorrer da ação de controle, sendo objeto de nota de auditoria).

#### **4. Nota de auditoria**

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

26. A nota de auditoria, deste modo, diferencia-se do ponto de auditoria por apresentar fato ou situação que, em última análise, não oferece mais risco à Casa, uma vez que já se encontra atendida 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.

##### **4.1. Ausência de normativo relativo a papéis e responsabilidades para soluções de TIC**

27. No decorrer dos trabalhos de auditoria, foi identificado que o risco de haver participação insuficiente do gestor de negócio permanecia sem tratamento adequado, mesmo tendo sido abordado em auditoria anterior no mesmo processo.

28. Um dos controles que poderia mitigar o referido risco seria a atribuição clara, prevista em normativo, que vinculasse os papéis e responsabilidades de cada um dos atores envolvidos no processo de provimento de solução de TIC.



29. No boletim administrativo de 12/7/2019, foi publicada a Portaria DG n. 88, de 29/3/2019, que estabelece atribuições e responsabilidades sobre soluções de Tecnologia da Informação e Comunicação (TIC), na Câmara dos Deputados.

30. A portaria traz uma definição clara sobre os papéis de cada um dos envolvidos no processo de provimento de soluções de TIC, e é um instrumento que vincula a atuação do gestor de negócio ao longo do processo, endereçando de forma adequada o risco citado.

## **5. Pontos de auditoria**

### **5.1. Ausência de critérios norteadores para a decisão sobre o modelo de obtenção da solução de TIC (contratação, desenvolvimento, customização, etc.)**

#### **5.1.1. Situação encontrada**

31. Foi detectada a ausência de critérios norteadores para a decisão sobre o modelo de obtenção da solução de TIC (contratação, desenvolvimento, customização, etc.).

32. Vale destacar que este risco foi abordado em auditoria anterior no mesmo processo, e, após recomendação da Secin, foi elaborado plano de ação para estabelecimento de normativo para disciplinar tais critérios e também as contratações de soluções de TIC, nos moldes da Instrução Normativa SLTI/MP 4-2014 do Ministério do Planejamento, sucedida pela IN 1-2019 do Ministério da Economia.

33. No entanto, a norma ainda não foi publicada, permanecendo o risco sem tratamento adequado.

#### **5.1.2. Critérios**

- a) Norma ABNT NBR ISO/IEC 38500 – Governança corporativa de TI, item 5.4;
- b) Cobit 5, processo BAI03 – Gerir Identificação e Construção de Soluções;

- c) Acórdão 1233/2012/Plenário – Tribunal de Contas da União (TCU) – Governança de TI, itens 9.18 e 9.2.9;
- d) Guia de boas práticas em contratação de soluções de TI/TCU.

### **5.1.3. Evidências**

- a) Os referidos critérios norteadores não foram encontrados na documentação e normativos relacionados ao processo, pesquisados na base de dados de legislação interna e no portal corporativo;
- b) Não há diretrizes do CETI nem do CGE sobre a escolha do modelo de obtenção da solução de TIC (contratação, desenvolvimento, customização, etc.), a exemplo da Decisão CETI n. 1/2013, que perdeu validade em 2017;
- c) Nos testes substantivos, foi identificado que em 4 das 11 soluções de TIC que fizeram parte da amostra houve indícios de problemas associados ao baixo investimento de recursos à etapa de estudo da solução.

### **5.1.4. Causa**

- a) Ausência de controles formalizados capazes de prover critérios para as decisões relativas à etapa de estudo da solução de TIC, em especial a escolha sobre o modelo de obtenção da solução de TIC (contratação, desenvolvimento, customização, etc.).

### **5.1.5. Efeitos**

- a) Ineficácia, ineficiência ou não efetividade de aquisições de TIC (efeito potencial);
- b) Utilização ineficiente de recursos para a construção de soluções de TIC (efeito potencial).

### **5.1.6. Esclarecimentos do auditado**

34. A Ditec informou que “Os critérios norteadores de tais decisões estão em desenvolvimento e foram apresentados preliminarmente ao Diretor-Geral”.



### 5.1.7. Análise

35. Apesar dos trabalhos estarem em andamento, persiste o risco identificado de que a etapa de estudo da solução de TIC, incluindo a importante decisão entre desenvolvimento interno, adoção ou contratação de solução externa, seja executada sem os critérios necessários.

36. Além disso, o tema aquisições é, por si só, de fundamental relevância, conforme os documentos listados como critérios no item 5.1.2.

37. Desta forma, considera-se fundamental que a Casa estabeleça um controle formal que discipline critérios a serem observados na etapa de estudo da solução de TIC, para balizar a decisão sobre o modelo de solução a ser adotado (contratação, desenvolvimento, customização, etc.).

38. Trata-se de um controle essencial para mitigar o risco de que exista baixa alocação de recursos à etapa de estudo da solução, evitando que a decisão entre contratar, desenvolver internamente ou adotar solução externa, com ou sem customização, seja tomada de forma ineficiente ou ineficaz.

39. No aspecto das aquisições, por conciliar as boas práticas e as determinações do TCU relacionadas ao assunto, a IN SLTI/MP n. 4/2014 tornou-se referência para contratação de serviços de TIC na Administração Pública, sendo adotada também pelo Poder Judiciário da União, por meio de resoluções do Conselho Nacional de Justiça<sup>4</sup> (CNJ) e do Conselho da Justiça Federal<sup>5</sup> (CJF) como norma a ser observada pelos órgãos subordinados.

40. Posteriormente, o Ministério da Economia editou a Instrução Normativa 1-2019, atualizando alguns aspectos da referida instrução.

41. Nesse sentido, considerando-se a situação encontrada neste ponto de auditoria, observa-se que a Câmara também pode se beneficiar das práticas

---

<sup>4</sup> Resolução n. 182/2013 do CNJ - Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).

<sup>5</sup> Resolução n. 279/2013 do CJF - Dispõe sobre o Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal - MCTI-JF no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

consolidadas na IN SLTI/MP n. 4/2014, sucedida pela IN n. 1-2019 do Ministério da Economia, utilizando-a como referência para as atividades de aperfeiçoamento normativo em andamento, visando maior qualidade e segurança no estudo do modelo de solução e na contratação de soluções de TIC.

#### **5.1.8. Recomendações**

a) Recomendar ao Comitê de Gestão Estratégica (CGE) que elabore plano de ação, contendo, pelo menos, atividades, responsáveis e prazos, para regulamentar critérios norteadores para a decisão sobre o modelo de obtenção da solução de TIC (contratação, desenvolvimento, customização, etc.), disciplinando ainda o processo de contratação de soluções (nos moldes da IN 1-2019 do Ministério da Economia, que sucedeu a IN 4-2014 do MPOG).

Prazo: 90 dias.

b) Recomendar ao Comitê de Gestão Estratégica (CGE) que implemente o plano de ação para regulamentar critérios norteadores para a decisão sobre o modelo de obtenção da solução de TIC (contratação, desenvolvimento, customização, etc.), disciplinando ainda o processo de contratação de soluções (nos moldes da IN 01-2019 do Ministério da Economia, que sucedeu a IN 04-2014 do MPOG).

Prazo: 180 dias.

### **5.2. Ausência de definição sobre o nível de risco que a gestão está disposta a aceitar na construção de soluções de TIC**

#### **5.2.1. Situação encontrada**

42. Foi detectada a ausência de declaração de apetite a riscos, ou documento similar, capaz de fornecer parâmetros para a seleção de respostas adequadas aos riscos, tanto no âmbito corporativo, quanto no âmbito da Ditec.

43. Sem essa definição quanto ao nível de risco que a gestão está disposta a aceitar, não se pode estabelecer critérios para julgar se a resposta a determinado risco foi ou não adequada.



### **5.2.2. Critérios**

- a) Ato da Mesa n. 233/2018 - Institui a Política de Gestão Corporativa de Riscos da CD;
- b) Cobit 5, processo APO12 – Gerenciar Riscos;
- c) Gestão de Riscos - Avaliação da Maturidade, TCU, 2018;
- d) Norma ABNT/ISO 31000:2018 - Gestão de Riscos - Diretrizes, item 6.3.

### **5.2.3. Evidências**

- a) Embora haja política corporativa de gestão de riscos vigente (Ato da Mesa n. 233/2018), não foi identificada uma declaração de apetite a riscos, capaz de balizar as decisões sobre respostas a riscos, nem a nível corporativo nem na Ditec;
- b) Existem registros de reuniões que tratam de respostas a riscos (embora, no caso do CETI, tenha havido apenas 1 reunião em 2018), mas não há informações claras sobre o nível de risco que a gestão está disposta a aceitar, impedindo que as partes interessadas possam avaliar se as respostas aos riscos são adequadas.

### **5.2.4. Causa**

- a) Ausência de controles formalizados capazes de prover critérios para a seleção de respostas adequadas aos riscos, uma vez que não foi definido um apetite a riscos (nível de risco que a gestão está disposta a aceitar) no processo em pauta.

### **5.2.5. Efeitos**

- a) Respostas inadequadas aos riscos, como por exemplo a aceitação de riscos excessivos ou a adoção de medidas desnecessárias para mitigar adicionalmente riscos que poderiam ser aceitos (efeito potencial).

### **5.2.6. Esclarecimentos do auditado**

44. Em resposta a solicitação de esclarecimentos, a Ditec informou que “[...] entende que a divulgação do apetite de riscos corporativo deve balizar as declarações das unidades administrativas a ela subordinadas. Como ainda não foi publicado tal informação, a Diretoria aguarda o momento para tratar do assunto em iguais proporções e destaque”.

### **5.2.7. Análise**

45. Conforme os critérios elencados no item 6.2.2, a definição do apetite a risco, assim entendido como o nível de risco que a organização está disposta a aceitar, é fundamental para que se possa classificar, priorizar e tratar os riscos identificados.

46. Sem ela, não se pode diferenciar riscos aceitáveis daqueles que não o são, constituindo assim um parâmetro que baliza a atuação do gestor no momento de tratar cada um dos riscos, dando a eles uma resposta a apropriada.

47. Vale ainda destacar que o próprio Ato da Mesa n. 233/2018, que instituiu a política de gestão corporativa de riscos na Casa, impõe que a gestão defina um apetite a riscos:

Art. 8º Compete ao CGE, no tocante à gestão corporativa de riscos:

...

V - identificar o apetite a riscos da Câmara dos Deputados para os planos, processos de trabalho e projetos que se mostram relevantes a essa identificação.

48. É ainda importante registrar que o nível de risco que se pode aceitar ao prover determinada solução de TIC é dependente do nível de risco aceitável naquele processo de trabalho que está sendo atendido pela referida solução. Por isso, embora o foco da auditoria seja o processo de provimento de solução de TIC, é fundamental que a definição do apetite a risco ocorra, ao menos inicialmente, em nível corporativo.

49. Em outras palavras, ao gerenciar o risco durante o processo de provimento de uma solução de TIC, os gestores envolvidos precisam conhecer o apetite a risco relativo àquele processo de trabalho que a solução visa atender.



50. Desta forma, considerando-se a situação encontrada neste ponto de auditoria, observa-se que é fundamental a definição do nível de risco que a gestão está disposta a aceitar.

51. O Ato da Mesa n. 233/2018 prevê que o apetite a risco deve ser identificado pela gestão em relação aos “planos, processos de trabalho e projetos que se mostram relevantes a essa identificação”. Atendendo a esse critério de relevância, é necessário que a gestão da Casa defina tal apetite, no mínimo, em relação aos processos críticos já identificados.

#### **5.2.8. Recomendações**

a) Recomendar ao Comitê de Gestão Estratégica (CGE) que elabore plano de ação, contendo, pelo menos, atividades, responsáveis e prazos, para identificar o apetite a riscos para os planos, processos de trabalho e projetos que se mostrem relevantes a essa identificação, conforme previsto no inciso V, Art. 8º, do Ato da Mesa n. 233 de 24/5/2018, abarcando os processos críticos da Câmara dos Deputados.

Prazo: 90 dias.

b) Recomendar ao Comitê de Gestão Estratégica (CGE) que implemente o plano de ação para identificar o apetite a riscos para os planos, processos de trabalho e projetos que se mostrem relevantes a essa identificação, conforme previsto no inciso V, Art. 8º, do Ato da Mesa n. 233 de 24/5/2018, abarcando os processos críticos da Câmara dos Deputados.

Prazo: 180 dias.

#### **6. Benefícios potenciais da ação de controle**

52. Em cumprimento ao disposto no artigo 3º da Portaria n. 2, da Secretaria de Controle Interno, de 22 de fevereiro de 2013, registre-se que a ação de controle ora relatada visa aos seguintes benefícios potenciais:

- a) maior envolvimento do gestor de negócio no desenvolvimento de soluções de TIC;
- b) maior objetividade nos critérios analisados para a decisão do modelo de provimento da solução de TIC (desenvolvimento, contratação, customização, etc.);
- c) melhorias no processo de contratação de soluções de TIC;
- d) melhoria no processo de gestão de riscos relativos ao provimento de soluções de TIC;
- e) aumento da eficácia, eficiência e efetividade das soluções de TIC entregues à Casa;
- f) aumento no desempenho institucional com maior convergência entre as estratégias da organização e a da própria Ditec.

## **7. Conclusões**

53. Esta auditoria teve por objetivo avaliar o processo de provimento de solução de TIC na Câmara dos Deputados. Como parâmetro para subsidiar a avaliação, foi utilizado o processo BAI03 – Gerenciar identificação e construção de soluções de TIC, do modelo Cobit 5.

54. Foram identificados seis riscos relevantes em relação ao citado processo, dentre os quais três foram considerados adequadamente mitigados pelos controles administrativos existentes, e três foram considerados inicialmente sem tratamento adequado.

55. No decorrer da auditoria, a gestão editou um normativo sobre atribuições e responsabilidades dos gestores envolvidos no provimento de soluções de TIC, o que contribuiu para mitigar adequadamente um dos riscos remanescentes, o que resultou em uma nota de auditoria, tratada no item 4.1.

56. Persistiram ao final dos trabalhos dois riscos sem tratamento adequado, resultando em dois pontos de auditoria, descritos em detalhes nos itens 5.1 e 5.2, com suas respectivas recomendações.



CÂMARA DOS DEPUTADOS  
MESA DIRETORA  
SECRETARIA DE CONTROLE INTERNO  
Núcleo de Auditoria de Tecnologia da Informação

57. Por fim, registre-se o agradecimento aos servidores da Ditec que colaboraram com esta auditoria, cuja valiosa ajuda foi crucial para o desenvolvimento destes trabalhos.

Brasília - DF, 7 de agosto de 2019.

## Apêndice A

### Provimento de solução de TIC na Câmara dos Deputados

Na Diretoria de Inovação e Tecnologia da Informação (Ditec), o processo Cobit 5 BAI03 é coberto, em grande medida, pelo macroprocesso “Prover Solução de TIC”, conforme mostrado na Figura 1.

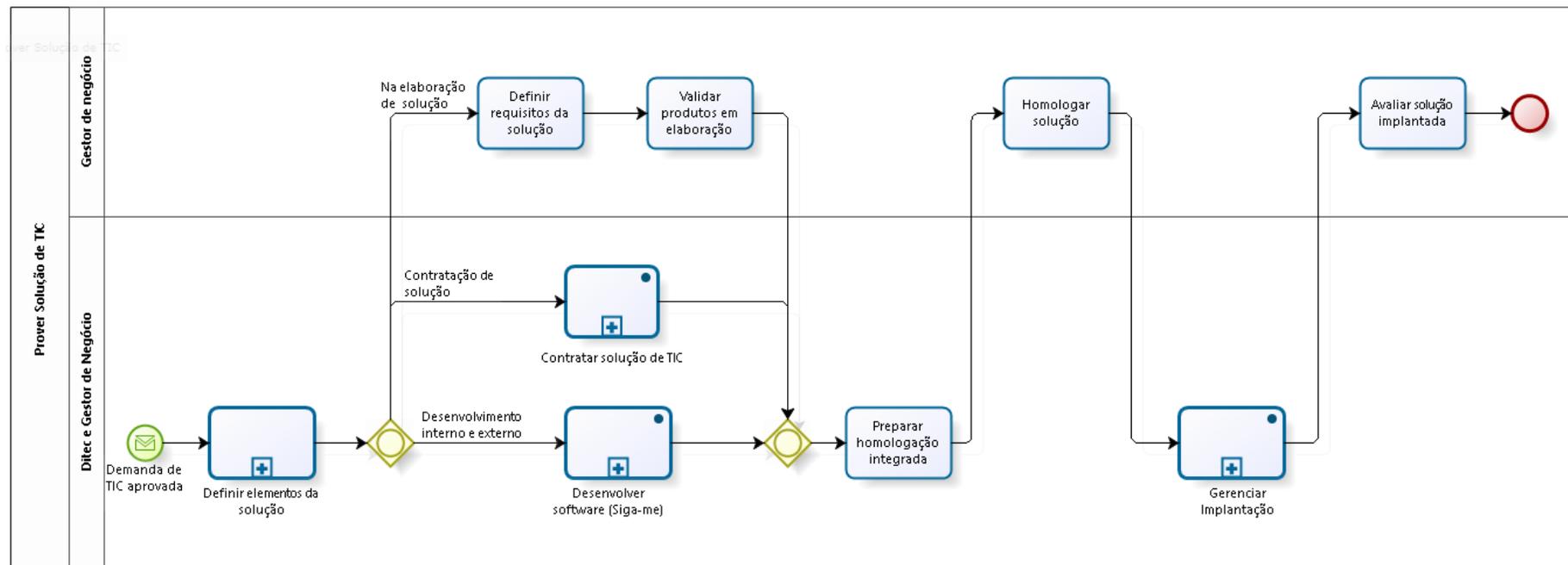
Conforme verificado, esse macroprocesso engloba os seguintes processos:

- **Definir elementos da solução:** compreende a interação entre a área técnica e o gestor de negócio com o objetivo de estudar a melhor forma de prover a solução demandada. Refere-se à definição das necessidades de negócio, identificação de soluções candidatas e seleção da melhor forma de atendimento à demanda.
- **Desenvolver Software (Siga-me):** foi instituído por meio da Instrução Cenin n. 1/2013 como processo organizacional de engenharia de sistemas e de software a ser aplicado nos projetos de desenvolvimento e de manutenção das soluções.
- **Contratar solução de TIC:** não possui documentação disponível no Portal de Processos, mas tem alguns de seus aspectos regulados por meio das Instruções Cenin n. 3/2014 e n. 2/2017.
- **Gerenciar implantação:** tem por principal objetivo assegurar que a solução de TIC seja instalada com êxito no ambiente produtivo da Casa, com o menor impacto possível, garantindo ainda a transferência de conhecimento para as equipes de atendimento, quando necessário. O processo é formalizado pela Instrução Cenin n. 2/2015.

O ponto de partida para o processo “Prover Solução de TIC” consiste nas demandas de TIC aprovadas, oriundas do processo “Gestão de Demandas de TIC”, formalizado pela Instrução Cenin 1/2015.



Figura 1 – Macroprocesso Prover Solução de TIC



Fonte: Portal de Processos (<http://gestaoprocessos.camara.gov.br/gerir-tecnologia-da-informacao/prover-solucao-de-tic>) – Acesso em 23/4/2019



CÂMARA DOS DEPUTADOS  
MESA DIRETORA  
SECRETARIA DE CONTROLE INTERNO  
Núcleo de Auditoria de Tecnologia da Informação

## **Apêndice B**

### **Processo Gerir Riscos de TIC na Câmara dos Deputados**

Na Ditec, o processo APO12 corresponde ao processo “Gerir Riscos de TIC”, que consta como em desenvolvimento no Portal de Processos, e é exposto na Figura 2. Ele inclui a identificação, análise, avaliação, comunicação e tratamento dos riscos de TIC, e baseia-se na norma ISO 31000:2009 - *Risk Management - Principles and Guidelines*.

Conforme exposto, o processo cobre as principais etapas relativas à gestão de riscos, abarcando a identificação, análise, avaliação, tratamento e comunicação.



Figura 2 – Processo Gerir Riscos de TIC

