Relatório de Auditoria nº 01 /2014

1. Introdução

Relatório de auditoria prevista no Plano Anual de Controle Interno (PACI) desta Secretaria para o ano de 2013, com o objetivo de avaliar os seguintes aspectos de governança de TI[1] na Câmara dos Deputados:

- Capacidade;
- Desempenho; e
- Continuidade de negócio.

Originalmente, esta auditoria teve como item para observação dos aspectos acima o Sistema de Informações Legislativas - Sileg. Entretanto, no decurso dos trabalhos, em reuniões com as diversas unidades administrativas relacionadas ao Sileg - Centro de Informática (Cenin), Departamento de Comissões (Decom), Centro de Documentação e Informação (Cedi), Secretaria-Geral da Mesa (SGM), Comitê Gestor do Sileg (CG-Sileg) e Grupo Gestor do Programa de Informatização da Atividade Legislativa (Prolegis) -, verificou-se que esse sistema já recebeu vários diagnósticos. Já houve o levantamento de problemas e respectivas propostas para suas soluções, incluindo a substituição, redesenho ou desenvolvimento de novos sistemas integrados, atividades já iniciadas pelo Cenin.

Assim sendo, os aspectos de capacidade, desempenho e continuidade dos serviços de TI passaram a ser avaliados sob o ponto de vista dos recursos utilizados em âmbito organizacional, não se detendo essa avaliação sobre um único sistema.

Outro aspecto digno de nota é que a auditoria foi conduzida com base na versão 5 do Cobit[2], que ainda não possui versão em português. Quando necessário, será mostrada a correspondência entre os processos da versão 5 e os da versão 4.1, a fim de facilitar-se o entendimento e a harmonização das observações para o público já afeito à versão anterior.

A esse respeito, cumpre observar que por meio do processo 129855/2013 esta Secretaria solicitou à gestão que fosse apresentada avaliação da maturidade e da relevância dos processos Cobit sob a ótica da versão 5. O Centro de Informática já apresentou sua avaliação, que foi submetida ao Comitê Estratégico de TIC para

---

[1] Neste relatório, as siglas TI e TIC serão usadas como sinônimos, salvo quando expressamente necessário estabelecer a distinção.

[2] Cobit – *Control Objectives for IT and related technology*, modelo de governança e gestão de TI internacionalmente reconhecido, amplamente adotado pela Coati em suas avaliações. Esse modelo também é referenciado em diversos acórdãos do Tribunal de Contas da União, como, por exemplo, o Acórdão 2585/2012/Plenário, que avalia a governança de tecnologia da informação na Administração Pública Federal e cuja cópia tramita na Casa sob o processo de nº 128.495/2012.

análise, e que deverá suportar diretrizes para o planejamento do Cenin, daí depreendendo-se a importância desses processos para a governança de TI da Casa.

1.1. Apresentação

Capacidade, desempenho e continuidade de serviços são aspectos cobertos pelos processos DS3 e DS4 do Cobit 4.1 e pelos processos BAI04[3] e DSS04[4] do Cobit 5:

- DS3 – Gerenciar capacidade e desempenho (*Manage Performance and Capacity*);
- DS4 – Assegurar continuidade de serviços (*Ensure Continuous Service*);
- BAI04 – Gerenciar disponibilidade e capacidade[5] (*Manage Availability and Capacity*);
- DSS04 – Gerenciar continuidade[6] (*Manage Continuity*).

Dentre os motivos que levaram à adoção da versão 5 do Cobit para fins de auditoria e avaliações de governança, podem-se citar os cinco princípios basilares da nova versão do modelo:

- Atender às expectativas dos gestores máximos da organização;
- Abranger toda a organização, de ponta a ponta;
- Aplicar um modelo de governança corporativa de TI, reunindo as melhores práticas mundiais;
- Possibilitar uma abordagem integrada sobre governança e gestão;
- Estabelecer de maneira clara a distinção entre governança e gestão.

Vale ressaltar que a versão 5 do Cobit é resultado de um processo coeso de evolução da versão 4.1. O Quadro[7] 1 demonstra isso, apresentando a correspondência entre os objetivos de controle da versão 4.1 e as práticas ou atividades da versão 5 para os processos supracitados.

---

[3] BAI – *Build, Acquire and Implement* – Construir, adquirir e implementar.

[4] DSS – *Deliver, Service and Support* – Entregar, servir e suportar.

[5] Tradução própria.

[6] Idem.

[7] Devido à inexistência de versão em língua portuguesa, os objetivos de controle do Cobit 5 são apresentados segundo tradução própria.

Quadro 1 – Correspondência entre as versões 4.1 e 5 do Cobit para os processos de continuidade, disponibilidade e capacidade de serviços de TI.

Objetivos de Controle do Cobit 4.1	Práticas ou atividades de processo do Cobit 5
DS3.1 Desempenho e planejamento de capacidade.	BAI04.03 Planejar para atender requisitos de serviços novos ou atualizados.
DS3.2 Capacidade e desempenho atuais.	BAI04.01-02 Monitorar desempenho e capacidade atuais tendo em vista limites (*thresholds*) previamente definidos, controlados automaticamente por meio de software onde necessário.
DS3.3 Capacidade e desempenho futuros.	BAI04.01 Medir a disponibilidade, o desempenho e a capacidade atuais, e criar linhas de base para referência futura.
DS3.4 Disponibilidade de recursos de TI.	BAI04.05 Investigar e atacar problemas de disponibilidade, desempenho e capacidade.
DS3.5 Monitoramento e relatórios.	BAI04.04 Monitorar e revisar disponibilidade e capacidade.
DS4.1 Estrutura de continuidade.	DSS04.01-02 Identificar partes interessadas, papéis e responsabilidades principais para a definição e o aceite (acordo) da política e do escopo da continuidade.
DS4.2 Planos de continuidade de TI.	DSS04.03 Desenvolver e implementar um plano de continuidade de negócio.
DS4.3 Recursos críticos de TI.	DSS04.04 Exercitar, testar e revisar o plano de continuidade de negócio.
DS4.4 Manutenção do plano de continuidade de TI.	DSS04.02 Manter uma estratégia de continuidade. DSS04.05 Revisar, manter e aperfeiçoar o plano de continuidade.
DS4.5 Teste do plano de continuidade de TI.	DSS04.04 Exercitar, testar e revisar o plano de continuidade de negócio.
DS4.6 Treinamento do plano de continuidade de TI.	DSS04.06 Realizar treinamento no plano de continuidade.
DS4.7 Distribuição do plano de continuidade.	DSS04.03 Desenvolver e implementar um plano de continuidade de negócio.
DS4.8 Recuperação e retomada dos serviços de TI.	DSS04.03 Desenvolver e implementar um plano de continuidade de negócio.
DS4.9 Armazenamento de cópias de segurança em locais remotos.	DSS04.07 Gerenciar a política de backup.
DS4.10 Revisão pós-retomada dos serviços.	DSS04.08 Conduzir revisão pós-reinício.

Fonte: Cobit 4.1 e 5 (*Enabling Processes)*.

1.2. Metodologia

A metodologia aplicada para realização da auditoria consistiu na realização de:

a) Análise de normativos e padrões pertinentes, utilizados como critérios ao longo deste relatório, mais especificamente na seção que trata dos achados da auditoria;

b) Entrevistas com pessoal técnico do Centro de Informática, incluindo visita aos Centros de Tecnologia (Cetecs) do Anexo IV e do Complexo Avançado da Câmara dos Deputados;

c) Envio ao Centro de Informática de questionários de apoio à auditoria, antes e depois das visitas;

d) Busca documental nos repositórios da Casa.

2. Achados

2.1. Achado: Os processos de negócios críticos não estão definidos nem priorizados

2.1.1. Situação encontrada

Da leitura e análise das respostas do Centro de Informática ao primeiro questionário[8] de apoio a esta auditoria, evidencia-se que a atuação daquele Centro não pode se dar sem a presença de diretrizes e norteadores estabelecidos pela alta gestão da Casa. Não é por outro motivo que se constituiu, durante o andamento dos trabalhos de auditoria, por meio da Portaria nº 406/DG, de 27 de setembro de 2013, o modelo de governança de tecnologia da informação e comunicação da Casa.

A análise das respostas ao questionário permite concluir que não há na Câmara dos Deputados a identificação e o mapeamento formais de seus processos de negócio com sua ordenação em termos de relevância e criticidade, o que nortearia mais eficientemente os trabalhos do Centro de Informática, cujos resultados, por sua vez, poderiam ter maior grau de eficiência e de efetividade.

[8] Enviado via correio eletrônico no dia 4 de junho de 2013.

2.1.2. Critérios

- Cobit 5, processos BAI04 – Gerenciar disponibilidade e capacidade e DSS04 – Gerenciar continuidade;
- Ato da Mesa nº 47, de 16 de julho de 2012, artigo 3º, incisos VIII, IX e X;
- Portaria da Diretoria-Geral nº 406 , de 27 de setembro de 2013, art. 4º e 6º;
- Decisão do Comitê Estratégico de TIC nº 1, de 19 de setembro de 2013, Anexo, itens 7 e 8.

2.1.3. Evidências

a) Respostas ao questionário de apoio a esta auditoria, mais especificamente, respostas ao item "b" da Seção 1 – Avaliação do Desempenho e da Capacidade, e à Seção 3 – Comentários do Centro de Informática;

b) Após entrevistas com servidores dos órgãos citados na introdução e busca no portal da Casa na intranet, o Camaranet, não foi encontrada prova documental de identificação nem de mapeamento dos processos de negócios críticos existentes na Câmara dos Deputados. Disso decorre que os impactos sofridos por esses processos, devido a incidentes ou outros eventos de TI, não são devidamente conhecidos, mapeados e tratados.

2.1.4. Causas

a) Ausência ou ineficácia de ações no sentido de identificar e mapear, formalmente, os processos de negócios críticos da Casa e sua dependência com relação às tecnologias de informação e comunicação.

2.1.5. Efeitos

a) Utilização menos eficiente da capacidade do Centro de Informática (efeito real);

b) Queda do desempenho de serviços essenciais de TI (efeito potencial);

c) Aumento do intervalo de tempo entre inoperância não planejada e volta à normalidade de serviços essenciais de TI (efeito potencial);

d) Em decorrência direta dos itens anteriores, prejuízos tangíveis e intangíveis a processos de negócios críticos da Casa (efeito real).

2.1.6. Esclarecimentos do auditado[9]

2.1.7. Análise

Os processos *BAI04 – Gerenciar disponibilidade e capacidade* e *DSS04 – Gerenciar continuidade* do Cobit 5 possuem, respectivamente, os seguintes propósitos:

- Manter a disponibilidade dos serviços de TI, a gestão eficiente de recursos e a melhora do desempenho de sistemas por meio da previsão de necessidades futuras de desempenho e de capacidade;
- Possibilitar a continuidade de operações críticas da organização e, no caso de uma interrupção significativa, manter a disponibilidade das informações em um nível aceitável pela organização.

É importante estabelecer a diferença entre continuidade e contingência: enquanto esta procura prover recursos alternativos para o provimento de serviços, via de regra em situações de emergência, aquela se preocupa com a garantia de um nível adequado de serviços, mediante critérios de qualidade aceitáveis. Assim, a contingência pode ser entendida como um dos caminhos para a implementação da continuidade. Por sua vez, o Ato da Mesa nº 47 de 2012 define, em seu art. 3º, VII, que disponibilidade é "a garantia de acesso à informação por usuários autorizados, quando necessário".

Segundo o modelo do Cobit, em uma organização os responsáveis diretos pelos propósitos de disponibilidade e de continuidade são os gestores de negócios e a área de Tecnologia da Informação, que são, respectivamente, o cliente e o prestador de serviços.

O Ato da Mesa nº 47, de 2012, que institui a Política de Segurança da Informação da Câmara dos Deputados e dá outras providências, disciplina em seu artigo 3º que:

> Art. 3º. Para os fins desta Política, entende-se como:
>
> (...)
>
> 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;

[9] Não publicados em atendimento ao disposto no Ato da Mesa n. 45/2012, art. 18, VII, b, c e d.

> 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. 5°) (grifos nossos).

Dessa forma, e corroborando os pontos elencados no item 2.1.6, pode-se dizer que cabe aos gestores de negócios da Câmara dos Deputados a identificação e o mapeamento[10] dos processos de negócios críticos da Casa, quer da esfera administrativa, quer da esfera legislativa[11], que dependem ou que venham a depender de recursos tecnológicos. Desse modo, o Centro de Informática poderá neles aplicar os esforços e insumos necessários com respaldo corporativo, de maneira mais orientada e eficiente para ambos, cliente e prestador de serviços.

De fato, esse é o ponto de partida para a obtenção de serviços de TI melhor planejados e dimensionados, com melhor desempenho e maior tempo de disponibilidade, além de proporcionar retornos mais rápidos à operação normal nos casos de interrupções planejadas e não planejadas.

O elenco de processos de negócios críticos de uma organização, em especial quando se trata das dimensões e da relevância da Câmara dos Deputados, perpassa a identificação de quais são os processos de trabalho que devem ser providos e mantidos em condições especiais. Essas condições, por sua vez, envolvem requisitos tais como os que se seguem, mas que não se resumem a eles:

a) Quais são os riscos envolvidos no provimento de tais serviços – que fatores podem impactar em seu fornecimento? Quais são as consequências de uma interrupção não programada?

b) Qual é a taxa de disponibilidade desejada - qual é o período de tempo em que o serviço deve estar “no ar”, ou “rodando”, para atender as necessidades de seus gestores e usuários? Todos os dias por todas as horas do dia (o chamado padrão 7x24)? Todos os dias úteis durante o horário comercial? E assim por diante;

c) Qual é o suporte desejado para o serviço – qual é o tamanho e o perfil da equipe de suporte necessária para apoiar o serviço, e qual é o horário em que essa equipe deve estar disponível? Ela deve atuar nas dependências da Casa ou pode prestar apoio remotamente?

---

[10] Mapear um processo significa detalhar e documentar seu funcionamento com o uso de metodologia definida.

[11] Por exemplo, respectivamente, a folha de pagamento e o processo legislativo da Casa, ambos processos abrangentes, de alta relevância e criticidade para atingir os objetivos a que se propõem os processos de negócios que apoiam, e que dependem de recursos de TI para funcionarem com a agilidade, a segurança e a confiabilidade exigidas.

d) Quais são os requisitos de infraestrutura necessários à prestação do serviço nos níveis adequados – é necessária a duplicação de recursos de infraestrutura tecnológica, como canais de comunicação ou servidores computacionais? É necessário o fornecimento de energia elétrica em níveis diferenciados dos demais serviços?

e) Qual é o nível tolerável de custos em que se quer incorrer para que se ofereçam os serviços com tais níveis de disponibilidade e de qualidade?

Durante os trabalhos de auditoria, foi publicada a já citada Portaria nº 406/2013/DG, que estabelece o modelo de governança de tecnologia da informação e comunicação da Câmara dos Deputados. Tal normativo estabelece, em seus artigos 4º e 6º, literalmente, as seguintes disposições:

> Art. 4º São atribuições do Ceti[12]:
>
> **I - Estabelecer diretrizes, objetivos e metas de tecnologia da informação e comunicação alinhados à estratégia da Câmara dos Deputados;**
>
> **II - Elaborar o Plano Estratégico de TIC (Peti), alinhado à Estratégia da Câmara dos Deputados**;
>
> III - Aprovar o PDTI[13];
>
> IV - Supervisionar a execução do Peti e do PDTI;
>
> V - Propor estrutura organizacional para a área de TIC.
>
> (...)
>
> Art. 6º O Peti é composto por, no mínimo:
>
> **I - Diretrizes estratégicas para a tecnologia da informação e comunicação;**
>
> **II - Indicadores e metas de desempenho de tecnologia da informação e comunicação;**
>
> **III - Alocação de recursos financeiros, humanos e materiais;**
>
> **IV - Estratégia de contratação e terceirização;**
>
> **V - Avaliação dos riscos relacionados à TIC** (grifos nossos).

Percebe-se que as indagações acerca dos processos de negócios críticos encontram eco nas disposições da Portaria nº 406/2013/DG, pois as respostas a tais perguntas devem partir de claras definições advindas da área estratégica: o que é um processo crítico e quais são os processos de negócios críticos da Casa. A partir dessas definições, podem-se traçar algumas das diretrizes, objetivos e metas para a área de

---

[12] Comitê Estratégico de TIC (art.2º, I).

[13] Plano Diretor de TIC, elaborado pelo Comitê Diretivo de TIC (art. 8º, I).

TIC. Resta claro, ainda, que a realização de tais propósitos e o atingimento de tais objetivos somente se darão com a devida alocação de recursos (financeiros, humanos e materiais), com a execução eficiente de uma estratégia adequada de contratações e de terceirizações e com uma avaliação de riscos de amplo espectro, que oriente a tolerância a riscos que se pode adotar nas ações a serem levadas a cabo.

Em ação conjunta à Portaria nº 406/2013/DG, foi publicada a Decisão nº 1 do Comitê Executivo de TIC, de 19 de setembro de 2013, que dispõe sobre as diretrizes de tecnologia da informação e comunicação da Câmara dos Deputados para o quadriênio de 2014 a 2017. Essa Decisão, nos itens 7 e 8 de seu Anexo, estabelece que:

> 7. As demandas por **novas soluções** de automação de processos, quando enviadas à Área responsável pela TIC, **devem ser precedidas da modelagem e documentação do processo**, além da informação a ele associada.
>
> 8. **Os serviços de TIC críticos, assim definidos pelo Comitê Estratégico de TIC (Ceti),** devem ser providos de forma a garantir os níveis e variáveis de qualidade acordados com as unidades administrativas demandantes (grifos nossos).

Assim, observa-se que a alta gestão da Casa já percebe a necessidade de proceder à identificação dos serviços de TI críticos, entendidos como aqueles que suportam os processos de negócios críticos, em comum acordo com as áreas que os demandam. É patente, além disso, que a definição de tais processos e do nível que se considera adequado para o provimento dos serviços tecnológicos que lhes dão suporte requer uma ação de cunho corporativo, com o pleno alinhamento desse esforço às iniciativas da gestão estratégica. Pode-se notar claramente que uma visão setorial de criticidade não seria capaz de abarcar de modo adequado o espectro dessa iniciativa, podendo redundar em retrabalho e em eventual desperdício de recursos.

Outra consideração que se mostra essencial nesse contexto é que o elenco dos processos de negócios críticos da Casa extrapola as fronteiras da TI. As tecnologias vêm ao real auxílio dos negócios quando os processos de trabalho estão definidos e seus requisitos são conhecidos, com critérios de qualidade, objetivos e metas bem definidos. Desse modo, entende-se que a definição dos processos de negócios críticos e dos níveis em que devem ser providos quando suportados pela TI deve ser feita em um fórum abrangente e que contemple os diferentes atores diretamente interessados em tais definições, além de serem os responsáveis por elas. Atualmente, na Câmara dos Deputados, esse fórum é representado pelo Comitê de Gestão Estratégica, criado pela Portaria do Diretor-Geral nº 233, de 28 de dezembro de 2009, que estabelece o modelo de gestão estratégica da Casa.

A recomendação a seguir procura orientar os entendimentos acima dispostos em termos materiais e cronológicos, à luz das constatações a que se chegou durante os trabalhos de auditoria. Além disso, busca-se estender o processo de modelagem para soluções de TI que não são novas (item 7 do Anexo da Decisão nº 1 de 2013), mas que têm alto nível de criticidade e que compreendem um vasto conjunto.

2.1.8. Proposta de encaminhamento

a) Recomendar ao Comitê Estratégico de TIC que, ouvido o Comitê de Gestão Estratégica, apresente plano de ação, com cronograma, que contemple:

   i. Identificação, mapeamento e ordenação em termos de relevância e criticidade dos processos de negócios da Câmara dos Deputados que dependem de serviços de Tecnologia da Informação para operarem segundo parâmetros e requisitos de qualidade previamente definidos;

Prazo: 180 dias.

2.2. Achado: Ausência de um Plano de Capacidade e Desempenho atual e futuro para os serviços de TI

2.2.1. Situação encontrada

O Centro de Informática não possui plano de capacidade e desempenho de seus recursos, nem apresentou processo formal definido que tenha como objetivo esse plano.

2.2.2. Critérios

- Cobit 5, processo BAI04 – Gerenciar disponibilidade e capacidade;
- Portaria da Diretoria-Geral nº 406, de 27 de setembro de 2013, artigos 4º e 6º;
- Decisão nº 1 do Comitê Estratégico de TIC, de 19 de setembro de 2013, item 3 do anexo.

2.2.3. Evidências

a) Respostas ao questionário de apoio a esta auditoria, mais especificamente, as relativas à seção 1;

b) Busca, sem sucesso, nas bases de informação da Casa por evidências de plano de capacidade e desempenho dos serviços de TI.

2.2.4. Causas

a) Situação retratada no item 2.1: processos de negócios críticos não definidos nem priorizados;

b) Ausência ou ineficiência de diretrizes, indicadores e metas passados pela governança corporativa à gestão da Tecnologia da Informação da Câmara dos Deputados.

2.2.5. Efeitos

a) Utilização menos eficiente da capacidade do Centro de Informática (efeito real);

b) Queda do desempenho de serviços essenciais de TI (efeito potencial);

c) Aumento do período entre inoperância não planejada e volta à normalidade de serviços essenciais de TI (efeito potencial);

d) Em decorrência direta dos itens anteriores, prejuízos tangíveis e intangíveis a processos de negócios críticos da Casa (efeito potencial).

2.2.6. Esclarecimentos do auditado[14]

2.2.7. Análise

À luz do processo BAI04 – Gerenciar disponibilidade e capacidade[15] (*Manage Availability and Capacity*) do Cobit 5 pode-se dizer que um plano de desempenho e capacidade resulta de prática de gestão que avalia e mede regularmente a disponibilidade, o desempenho e a capacidade dos serviços e recursos de TI. Essa prática tem o fim de assegurar que tais serviços e recursos estejam disponíveis para atender as necessidades da organização, com seus custos justificados e em conformidade com os acordos de níveis de serviços, os quais devem ser regidos por processo próprio, estabelecidos e devidamente monitorados.

Essa prática de gestão leva em conta, entre outros, os seguintes elementos:

- Necessidades dos clientes e usuários[16];
- Objetivos e prioridades da organização;
- Impactos no orçamento de TI e da organização;
- Taxas de utilização dos recursos de TI;

[14] Não publicados em atendimento ao disposto no Ato da Mesa n. 45/2012, art. 18, VII, b, c e d.

[15] Tradução própria.

[16] O Ato da Mesa nº 47/2012 estabelece em seu art. 3º, XVII, que: usuário é "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".

- Monitoramento da capacidade e desempenho reais, e sua comparação com limites estabelecidos e controlados por meio de software onde possível e necessário;
- Identificação e acompanhamento de todos os incidentes causados por capacidade ou desempenho inadequados;
- Avaliação constante de desempenho, em todos os níveis, em conformidade com os acordos de níveis de serviços e as mudanças no ambiente.

O Item 3 do Anexo da Decisão 1 de 2013 estabelece que:

> **A Câmara dos Deputados adotará padrões e boas práticas de gestão e de governança que permitam administrar, controlar e acompanhar o desempenho da Área Responsável pela TIC e das atividades prestadas nas demais unidades administrativas como parte do modelo híbrido adotado** (grifo nosso).

Vale repetir, ainda uma vez, o que dispõe a Portaria nº 406/2013/DG, em seus artigos 4º e 6º:

> Art. 4º São atribuições do Ceti:
>
> I **- Estabelecer diretrizes, objetivos e metas de tecnologia da informação e comunicação alinhados à estratégia da Câmara dos Deputados**;
>
> II - **Elaborar o Plano Estratégico de TIC (Peti), alinhado à Estratégia da Câmara dos Deputados**;
>
> III - Aprovar o PDTI;
>
> IV - Supervisionar a execução do Peti e do PDTI;
>
> V - Propor estrutura organizacional para a área de TIC.
>
> (...)
>
> Art. 6º O Peti é composto por, no mínimo:
>
> I - **Diretrizes estratégicas para a tecnologia da informação e comunicação**;
>
> II - **Indicadores e metas de desempenho de tecnologia da informação e comunicação**;
>
> III - **Alocação de recursos financeiros, humanos e materiais**;
>
> IV - **Estratégia de contratação e terceirização**;
>
> V - **Avaliação dos riscos relacionados à TIC** (grifo nosso).

O que se conclui a partir do elencado no item “2.2.6 – Esclarecimentos do auditado”, é que o Centro de Informática vem observando, em certa medida, o que aconselha o processo descrito resumidamente acima. Faz isso, entretanto, à sua própria maneira, dentro de suas limitações e conforme o ambiente, as circunstâncias e as peculiaridades organizacionais lhe permitem – o que se evidencia, por exemplo,

pelo fato de a Casa não ter ainda definido nem priorizado seus processos de negócios críticos, situação retratada no item 2.1 deste relatório.

Mediante o acima disposto, restam claras as oportunidades de melhoria na relação entre as instâncias de governança e de gestão, relacionadas na proposta de encaminhamento a seguir, e que guardam estreita relação com as do achado anterior. As recomendações abaixo dispostas procuram associar os esforços da gestão com os anseios da governança, expressos na Decisão nº 1 de 2013 do Comitê Estratégico de TIC e na Portaria nº 406/2013/DG.

2.2.8. Proposta de encaminhamento

a) Observadas as dependências em relação à recomendação do item anterior, recomendar ao Centro de Informática que apresente plano de ação, com cronograma, para:

   i. Implantação de processo de planejamento de capacidade e desempenho dos serviços e recursos de TI, contemplando as informações dos processos de negócios críticos e do BDGC;

   ii. Aprimoramento do processo de monitoramento da capacidade e desempenho dos serviços e recursos de TI;

   iii. Integração dos processos acima com o processo de gestão de nível de serviços.

   Prazo: 180 dias, a contar do recebimento pelo Centro do plano de ação previsto no item 2.1.8.

2.3. Achado: Ausência de Plano de Continuidade de Negócio

2.3.1. Situação encontrada

Não há na Câmara dos Deputados plano de continuidade de negócio, nem processo formal definido que tenha como objetivo esse produto.

2.3.2. Critérios

- Cobit 5, processo DSS04 – Gerenciar continuidade[17] (*Manage Continuity*);
- Ato da Mesa nº47/2012, que instituiu a Política de Segurança da Informação na Câmara dos Deputados;

[17] Tradução própria.

- Norma ABNT ISO 22301 – Segurança da Sociedade – Sistema de gestão de continuidade de negócios – requisitos – item 3 – termos e definições.

2.3.3. Evidências

a) Respostas ao primeiro questionário de apoio a esta auditoria, mais especificamente, as relativas à seção 2;

b) Respostas ao segundo questionário[18] de apoio à auditoria, enviado ao Cenin após visitas aos Centros de Tecnologia (Cetecs) I e Norte.

2.3.4. Causas

a) Situação retratada no item 2.1: processos de negócios críticos não definidos nem priorizados;

b) Ausência ou ineficiência de diretrizes, indicadores e metas passados pela governança corporativa à gestão da Tecnologia da Informação da Câmara dos Deputados.

2.3.5. Efeitos

a) Resolução dificultada de interrupções não planejadas em processos de negócios críticos da Casa que dependem de recursos de TI (efeito real);

b) Aumento do intervalo de tempo entre interrupção não planejada e volta à normalidade dos processos mencionados no item anterior (efeito potencial de alto impacto);

c) Em decorrência direta do item anterior, prejuízos tangíveis e intangíveis, administrativos e/ou políticos e à imagem da Casa (efeito potencial de alto impacto).

2.3.6. Esclarecimentos do auditado[19]

[18] Enviado por e-mail no dia 14 de outubro de 2013 com o assunto: “Capacidade e continuidade de serviços de TI”.

[19] Não publicados em atendimento ao disposto no Ato da Mesa n. 45/2012, art. 18, VII, b, c e d.

2.3.7. Análise

É forçoso ressaltar que, ainda que a contingência proporcionada pelo Cenin seja em nível suficiente para que muitas falhas passem despercebidas pelo usuário, o que é digno de louvor, as ações de caráter reativo ou os procedimentos de recuperação das informações e de recursos de TI devem ser menos frequentes, catalogados criteriosamente e de fácil acesso por seus responsáveis diretos.

O processo de Gestão da Continuidade DSS04 do Cobit 5 estabelece e mantém um plano que possibilita à organização e à área de Tecnologia da Informação responder a incidentes e a interrupções de tal forma que os processos de negócios críticos e os serviços de TI que os apoiam sejam mantidos, assim como o acesso à informação, todos em um nível aceitável.

Em linhas gerais, o processo DSS04 se destina a:

- Identificar partes interessadas, papéis e responsabilidades principais para a definição e o aceite (acordo) da política e do escopo da continuidade;
- Manter uma estratégia de continuidade;
- Desenvolver e implementar um plano de continuidade de negócio;
- Exercitar, testar e revisar o plano de continuidade de negócio;
- Revisar, manter e aperfeiçoar o plano de continuidade;
- Realizar treinamento no plano de continuidade;
- Gerenciar a política de *backup*;
- Conduzir revisão pós-reinício (pós-retorno à operação normal das atividades).

Cabe trazer à baila algumas definições, todas obtidas da Norma ABNT 22301, que trata dos requisitos de um sistema de gestão de continuidade de negócios:

a) Continuidade de negócios – capacidade da organização de continuar a entrega de produtos e serviços em um nível aceitável previamente definido após incidentes de interrupção;

b) Gestão da continuidade de negócios – processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. **Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado** (grifos nossos);

c) Plano de continuidade de negócios – **procedimentos documentados que orientam a organização a responder, recuperar, retomar e**

restaurar, após a interrupção, para um nível predefinido de operação (grifos nossos);

d) Programa de continuidade de negócios – processo contínuo de gestão e governança suportado pela Alta Direção que recebe apropriadamente os recursos para implementar e manter a gestão de continuidade de negócios.

Mais uma vez observa-se a necessidade imperiosa de uma ação corporativa, ou seja, a formulação de um plano de continuidade de negócios, capaz de prover a sustentação necessária para a efetiva gestão da continuidade de negócios, e, em etapa aprimorada, pavimentar a criação um programa de continuidade de negócios. Nota-se que o cerne de tal estrutura é o plano.

A continuidade de negócios também é endereçada pela segurança da informação, tema para o qual a Câmara dos Deputados possui política institucional, materializada pelo Ato da Mesa nº 47 de 2012. Os aspectos básicos para a gestão da continuidade de negócios que são relacionados à segurança da informação estão descritos sucintamente na seção A.14.1 da norma ABNT 27001, que trata dos requisitos para sistemas de gestão de segurança da informação. Eles são reproduzidos no Quadro 2.

Quadro 2 – Aspectos da gestão da continuidade do negócio relacionados à segurança da informação.

A.14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação *Objetivo:* Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.		
A.14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio	***Controle*** **Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.**
A.14.1.2	Continuidade de negócios e análise/avaliação de risco	***Controle*** **Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as consequências para a segurança de informação.**
A.14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	***Controle*** **Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.**
A.14.1.4	Estrutura do plano de continuidade do negócio	***Controle*** **Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.**

Fonte: Norma ABNT 27001, Seção A.14. Grifos nossos.

Percebe-se a concatenação das etapas a serem desenvolvidas com vistas à implementação de um plano de continuidade de negócios, em uma cadeia de eventos sucessivos e coordenados.

Uma linha sucessiva de eventos também se mostra no tocante à elaboração de tal plano: há que, antes, se elencar os processos de negócio críticos, o que foi objeto da seção 2.1 deste relatório.

O Ato da Mesa nº 47/2012 estabelece em seu art. 14 que as demandas iniciais do Comitê Gestor de Segurança da Informação terão entre suas prioridades o Plano de Continuidade de Negócio (inciso IX). A recomendação que se segue não tem o propósito de ocasionar atropelos na priorização definida pelo Ato, mas sim, à luz das evidências trazidas durante os trabalhos de auditoria, possibilitar o amadurecimento e implementação de um processo que se mostra essencial para uma instituição da envergadura e da relevância da Câmara dos Deputados, dada sua dependência dos recursos de TI.

2.3.8. Proposta de encaminhamento

a) Recomendar ao Comitê de Gestão Estratégica que, de forma coordenada por sua secretaria, representada pela Assessoria de Projetos e Gestão, apresente plano de ação[20], com cronograma, para desenvolver e implantar o Plano de Continuidade de Negócios da Câmara dos Deputados, com base nas boas práticas sobre o tema.

   Prazo: 180 dias, a contar da formulação do plano de ação previsto no item 2.1.8.

3. Conclusões

Esta auditoria teve por objetivo avaliar os seguintes aspectos de governança de TI na Câmara dos Deputados: capacidade, desempenho e continuidade de negócio.

A partir da metodologia aplicada, pode-se afirmar que não se encontrou na Câmara dos Deputados evidência de um processo formal de planejamento de capacidade e desempenho dos recursos e serviços de Tecnologia da Informação. O mesmo se aplica ao planejamento de continuidade de negócios da Casa, ou seja, dos processos de negócio críticos, sejam administrativos, legislativos ou de outra alçada, que dependem de recursos e serviços de TI para funcionarem.

Deve-se observar que o estabelecimento de tais processos de TI é antecedido pela identificação e mapeamento dos citados processos de trabalho da Casa, classificando-os em termos de relevância e criticidade, tarefa de natureza, complexidade e importância tais que sugerem que sejam orquestradas pela alta gestão. Sem essa ótica, corre-se o risco de que não ocorra o perfeito alinhamento entre

[20] Portaria n. 233/2009, art. 6ª, IV.

as perspectivas da alta administração e da gestão de TI sobre esses serviços, o que os tornaria menos efetivos, trazendo menos benefícios e minimizando os resultados obtidos.

Por fim, registre-se o agradecimento aos servidores do Centro de Informática, da Secretaria-Geral da Mesa, do Departamento de Comissões e do Centro de Documentação e Informação que colaboraram com esta auditoria, e sem cuja valiosa ajuda estes trabalhos não teriam sido possíveis.

Síntese

A partir das considerações dispostas no relatório observa-se a relevância dos processos de capacidade, desempenho e continuidade dos serviços de TI para a Casa, ao serem analisados sob o enfoque do modelo de governança apresentado pelo Cobit 5, o qual já se constitui em critério para elaboração de diretrizes para o planejamento de ações de TIC, conforme se constata pelo processo 129.855/2013.

A Câmara dos Deputados vem realizando diversas iniciativas no tocante à governança de TIC, o que se evidencia pelos normativos citados no relatório, tais como o Ato da Mesa nº 47/2012 (Política de Segurança da Informação), a Portaria nº 406/2013/DG (modelo de governança de TIC) e a Decisão nº 1 de 2013 do Comitê Estratégico de TIC (diretrizes de tecnologia da informação e comunicação para o quadriênio de 2014 a 2017). Da mesma forma, são patentes os esforços do Centro de Informática e da Casa em se coadunar com as melhores práticas para gestão dos serviços de TIC a fim de melhor prover os serviços e produtos que dele são esperados. As recomendações que se apresentam no relatório procuram vir, como sempre, ao encontro desses esforços e iniciativas, consolidando ações baseadas em um conjunto coeso de processos, com vistas à otimização de recursos, à minimização de riscos e ao real provimento de benefícios, objetivos basilares de uma boa governança.

Nesse sentido, são apresentadas as recomendações que se repetem a seguir, com o fito de sumarizá-las:

a) Recomendar ao Comitê Estratégico de TIC da Casa que, ouvido o Comitê de Gestão Estratégica, apresente plano de ação, com cronograma, que contemple:

   i. Identificação, mapeamento e ordenação em termos de relevância e criticidade dos processos de negócios da Câmara dos Deputados que dependem de serviços de Tecnologia da Informação para operarem segundo parâmetros e requisitos de qualidade previamente definidos;

   Prazo: 180 dias.

b) Observadas as dependências em relação à recomendação do item anterior, recomendar ao Centro de Informática que apresente plano de ação, com cronograma, para:

i. Implantação de processo de planejamento de capacidade e desempenho dos serviços e recursos de TI, contemplando as informações dos processos de negócios críticos e do BDGC;

ii. Aprimoramento do processo de monitoramento da capacidade e desempenho dos serviços e recursos de TI;

iii. Integração dos processos acima com o processo de gestão de nível de serviços.

Prazo: 180 dias, a contar do recebimento pelo Centro do plano de ação previsto no item 2.1.8.

c) Recomendar ao Comitê de Gestão Estratégica que, de forma coordenada por sua secretaria, representada pela Assessoria de Projetos e Gestão, apresente plano de ação, com cronograma, para desenvolver e implantar o Plano de Continuidade de Negócios da Câmara dos Deputados, com base nas boas práticas sobre o tema.

Prazo: 180 dias, a contar da formulação do plano de ação previsto no item 2.1.8.

Brasília – DF, maio de 2014