



## NOTA TÉCNICA SUTIN 016, de 29 de Outubro de 2010

**ASSUNTO:** Considerações sobre a avaliação da Governança de TI da Conab pelo TCU

### 1. Introdução

Esta Nota Técnica pretende fazer algumas considerações sobre a apuração do indicador de Governança de TI (IGovTI) elaborado pelo Tribunal de Contas da União – TCU, a partir de dados coletados pelo referido Tribunal junto aos diversos órgãos da Administração Pública Federal, com vistas a ter um instrumento de avaliação quanto à Governança de TI. O instrumento é valioso e foi desenvolvido com rigor metodológico e conceitual.

A Conab participou dessa avaliação, tendo o TCU encaminhado à Sutin os seguintes resultados: indicador IgovTi apurado para a Companhia e para os diversos segmentos de atuação de órgãos da Administração Pública, relatório comparativo com a última avaliação da Conab e a metodologia de cálculo do IgovTI, dentre outros dados.

### 2. Sobre o conceito de Governança de TI

Para melhor compreensão do indicador IGovTI, vale a pena retomar o conceito que o origina - Governança de TI -, conforme o ITGI - Information Technology Governance Institute - COBIT - Control Objectives for Information and related Technology<sup>1</sup>

**“Responsabilidade da alta direção, que consiste em liderança, estruturas organizacionais e processos que garantem que a TI corporativa sustenta e estende as estratégias e objetivos da organização”**

Conforme esse conceito, a Governança de TI transcende a esfera de atuação da área de TI, devendo se constituir numa preocupação corporativa, cuja definição e implementação deve estar sob a responsabilidade da alta administração. Também se observam as seguintes premissas:

- ✓ O cerne da boa governança de TI está em assegurar que sejam atribuídas responsabilidades claras para todas as pessoas envolvidas no processo de gestão e uso da TI na organização e que efetivamente todas essas pessoas se comportem como esperado, de modo que os benefícios da TI sejam efetivamente alcançados
- ✓ A responsabilidade pela decisão estratégica de gastos na área de TI deve ser compartilhada pelas unidades de negócio beneficiadas ou demandantes.

---

1 [ITGI. Information Technology Governance Institute COBIT - Control Objectives for Information and related Technology.](#)

•p.5 IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.



### 3. Sobre o índice iGovTI da Conab

O indicador iGovTI preconizado pelo TCU é composto de 4 segmentos, cujas avaliações são utilizadas por meio de ponderações para o cálculo final do indicador. Esses 4 segmentos são consentâneos com a definição de Governança de TI do ITGI, apresentada no item 1, atestando assim a consistência e coerência do indicador iGovTI.

A Conab recebeu as seguintes avaliações:

## Índice de Governança de TI da Instituição (iGovTI)

**Nome Instituição:** COMPANHIA NACIONAL DE ABASTECIMENTO

**Tipo Instituição:** Soc. econ. mista ou empresa pública

**Segmento:** EXE-Dest

I.Liderança	2.Estrat. Planos	6.Pessoas	7.Processos	iGovTI	Estágio de Gov. de TI
0,11	0,41	0,68	0,30	0,35	Inicial

Para a interpretação desses índices, foram definidos pelo TCU os seguintes estágios e respectivos limites:

iGovTI de 0 a 0,39 – considera-se em estágio INICIAL de governança de TI;

iGovTI de 0,40 a 0,59 - considera-se em estágio INTERMEDIÁRIO;

iGovTI a partir de 0,60 - considera-se em estágio APRIMORADO

### 4. Análise dos 4 segmentos do indicador iGovTI da Conab

Para a análise do resultado final do iGovTI da Conab, vale a pena fazer uma análise individual de cada um desses segmentos:

#### 1. Liderança

Esse segmento explora um conjunto de questões relativas a como a alta administração da organização avaliada vem tratando a sua Tecnologia da Informação: estrutura da governança de TI, desempenho organizacional na gestão e uso de TI, desenvolvimento de gestores de TI e auditoria de TI. Assim, trata-se de um vetor de avaliação completamente externo à área de TI.

A avaliação para esse segmento foi baixa: 0,11, o que contribui sobremaneira para puxar o valor final do indicador da Conab para baixo, tanto pela baixa avaliação em si quanto pela alta ponderação do item no cálculo do valor final do indicador.

## **2. Estratégia e Planos**

Para esse segmento, são abordadas questões relativas à estratégia organizacional e as suas interfaces com a área de Tecnologia da Informação, ou dizendo de outro modo, as relações entre o planejamento estratégico institucional e o planejamento estratégico de TI. Também aqui, o foco é mais externo à área de TI.

A avaliação para esse segmento foi razoável - 0,41 - haja vista a boa relação entre planejamento estratégico de TI e suas vinculações com a negócio da Conab, estabelecidas quando do Planejamento Estratégico implantado em 2003/2004. O ponto mais frágil ficou por conta da avaliação do Planejamento Estratégico da Conab, que foi avaliado de forma menos positiva que em 2007, quando este encontrava-se ainda em pleno vigor de sua implementação e utilização como ferramenta de gestão.

## **3. Pessoas**

O segmento compreende a avaliação de como a organização avaliada trata o quesito em tela, dando realce a aspectos como a composição do quadro de pessoal de TI, preocupação da organização em alocar pessoas dos seus quadros a funções de gestão de TI e capacitação oferecida a esses gestores.

A avaliação do segmento foi positiva: 0,68. Entretanto, entendemos que ela não reflete a real situação da Conab, pois, ao privilegiar alguns aspectos em que a Conab está bem posicionada, deixou de apreciar outros como, por exemplo, o aparelhamento de seus quadros funcionais de modo a atender às necessidades da área e conseguir garantir a continuidade do negócio quanto às ações de TI, questões recorrentes e já exaustivamente tratadas/encaminhadas à Dipai.

## **4. Processos**

Esse último segmento privilegia a avaliação de processos ligados à área de segurança da informação (tanto no âmbito da organização quanto no âmbito de TI), processo de software, gerenciamento de projetos, gerenciamento de serviços de TI e contratações de serviços de TI.

O perfil desse segmento é híbrido, focado tanto em processos internos quanto em processos externos à área de TI, como, por exemplo, processos de contratação de serviços de TI que envolvem várias áreas da organização (CPL, Supad e área de TI) e de segurança da informação.

A avaliação desse segmento foi de 0,30, sendo considerada ruim. O Fator teve forte contribuição negativa para a nota final da Conab, principalmente por esse quesito ter alta ponderação no cálculo dessa nota.

## **5. Recomendações**

A questão da Governança de TI na Conab já havia sido levantada pela Auditoria Interna da Companhia, que em seu “Relatório de Auditoria Acompanhamento da Gestão nº 10, de 09/06/2009” veio solicitar posicionamentos da Sutin quanto ao cumprimento de recomendações do TCU no que concerne a esses aspectos.

Conforme demonstrado à época (CI SUTIN 198 de 03/07/2009 endereçada à Audin) e neste documento, acreditamos que a implantação de uma Governança de TI depende de esforços da Conab, devendo contar com o patrocínio da alta administração devido a seu caráter corporativo

e seu foco externo, e que transcende, portanto, à área de Tecnologia da Informação.

Pela sua atualidade e pertinência com os aspectos negativos apontados na avaliação atual do IGOVTI da Conab (vide item 4), vale a pena reproduzir aqui as recomendações feitas pela Sutin à época (Julho/2009). Acrescentamos uma coluna para indicar a situação atual do item.

Acreditamos que tais recomendações, se implementadas, poderão contribuir de forma significativa para a obtenção de um melhor IgovTI para a Conab, nas próximas avaliações:

Recomendação do TCU	Considerações/ Medidas Adotadas e/ou Sugeridas (Julho/2009)	Situação atual (outubro/2010)
Itens 9.4.1 a 9.4.3 – contemplando: Criação de Listas de verificação para Julgamento de Licitação de TI, Elaboração de Normas, Criação de um Plano de Contratação	Trata-se, em essência, da definição de um Processo de Contratação de Serviços de TI, que envolve atores de várias áreas da Companhia (CPL, Proge, Supad/Gecot), além da Sutin. Para tanto, será necessária a criação de um projeto e de um grupo de trabalho com representantes dessas áreas. O assunto deverá ser encaminhado à DIPAI, DIRAD e PRESI para as deliberações cabíveis.	A mesma
Item 9.4.4 – Elaboração e implementação de um Modelo de Governança de TI	<p>Já explicitado no documento.</p> <p>O entendimento é que essa recomendação do TCU deva ser endereçada à DIPAI, para que esta inclua o tema na agenda da alta administração da Conab, de modo a que a matéria seja apropriadamente tratada.</p> <p>Em termos de operacionalização, recomendamos a criação de um Projeto Institucional para tratar a Governança de TI na Conab, de modo a definir o Modelo de Governança e implantá-lo.</p>	A mesma
Item 9.4.5 – Trata da Recomposição do Quadro Permanente de Pessoal de TI e Criação da carreira específica	<p>As questões elencadas no item já vêm sendo exaustivamente tratadas pela Sutin, desde 2003, em diversas notas técnicas e expedientes encaminhados à DIPAI, a exemplo de Notas Técnicas mais recentes como a NT 001/2009. Também foi tratado pelo Relatório preliminar de Recomendações para Melhoria nos Controles e Procedimentos Relativos ao ambiente de Processamento Eletrônico de Dados, elaborado pela empresa BDO Trevisan Auditores Independentes, contratada pela Conab para fins de auditoria das demonstrações contábeis.</p> <p>De forma sintética, a situação atual é a seguinte:</p> <p>A nova estrutura organizacional da Sutin foi recentemente implantada, conforme proposta no PDTI, aprovado em 15/06/2007;</p> <p>A Sutin propôs a criação de uma Gratificação para a área de TI (CI 188 de 25/06/2009), a exemplo da GSIST, proposta pelo SISP, como forma de compensar a defasagem salarial dos técnicos da área de TI da Conab.</p> <p>O PCCS continua em andamento.</p>	<p>O PCCS foi implantado.</p> <p>O restante continua na mesma situação.</p>

Recomendação do TCU	Considerações/ Medidas Adotadas e/ou Sugeridas (Julho/2009)	Situação atual (outubro/2010)
	Como o PCCS não contempla a criação de uma carreira de TI na Conab, recomenda-se o estudo quanto à oportunidade / viabilidade de criação de um Plano de Carreira específico para a área de TI, juntamente com a realização de novo concurso público. Essas matérias já foram objeto de solicitação ao DEST (Ofício Presi 133 de 03/04/2009)	
Item 9.4.7 – Trata de implantação de Processo de Planejamento Institucional	Não se aplica à Sutin.	
Item 9.4.8 – Trata da criação da Estrutura de TI	Vide resposta ao item 9.4.5	
Item 9.6 – Criação de Procedimento para elaboração de Política de segurança da Informação, de controle de acesso, de cópia de segurança, Análise de Risco e Plano de Continuidade de Negócio	<p>A Sutin já havia elaborado um documento contendo as diretrizes de segurança da informação, controle de acesso e cópias de segurança, que foi aprovado pela Diretoria em 16/08/2007, estando o normativo já em vigor desde então, objeto do Capítulo 60.213 da NOC.</p> <p>Entretanto, o Relatório de Recomendações para Melhoria nos Controles e Procedimentos Relativos ao ambiente de Processamento Eletrônico de Dados, elaborado pela empresa BDO Trevisan Auditores Independentes, recomenda <b>ELABORAR, FORMALIZAR E IMPLEMENTAR PROCEDIMENTOS DESCRITOS NO PLANO DA POLÍTICA DE BACKUP PARA CÓPIAS DE SEGURANÇA, TESTES E RESTAURAÇÃO DE DADOS E TRANSPORTE E DESCARTE DE MÍDIAS.</b></p> <p>Os itens Análise de Risco e o Plano de Continuidade de Negócio não estão ainda implementados. Por outro lado, o PMTI prevê a implantação de um Projeto de Segurança da informação e contingência. Segurança da informação é algo que deve ser perseguido diuturnamente, neste sentido a pequena equipe da Geasi vem implementando frequentemente mecanismos de segurança e eventualmente são realizadas análise de vulnerabilidades em pontos de entrada na rede e de maior criticidade. Em 2004, foi realizada pela UnB análise de vulnerabilidades em todo o ambiente de TI da Conab, entretanto, de lá para cá o ambiente foi modificado e é necessário que nova análise completa seja realizada. Neste contexto, também se insere o projeto de segurança da informação, no qual inclui a análise de risco e plano de continuidade de negócio, os quais pretende-se elaborar termo de referência para contratação de terceiros, tão logo haja alguma disponibilidade da equipe, haja vista que o quantitativo de pessoal é muito limitado e está dedicado, principalmente, à manutenção do ambiente operacional</p>	<p>O Projeto de Segurança da Informação encontra-se na fase elaboração .</p> <p>Esse projeto é composto de vários subprojetos. Para maiores detalhes do Projeto, vide Anexo I.</p>
em 9.8 – que trata da formalização do Processo de	Vide resposta aos itens 9.4.1 a 9.4.3	

Recomendação do TCU	Considerações/ Medidas Adotadas e/ou Sugeridas (Julho/2009)	Situação atual (outubro/2010)
Contratação		
Item 9.10 – que trata da capacitação dos Gestores de TI com conteúdo multidisciplinar necessário ao exercício das atribuições inerentes a essas funções, que vão além de conhecimentos de Tecnologia da Informação	<p>A Sutin destacou 2 (dois) analistas de sistemas para participar do Programa de Capacitação dos órgãos Integrantes do Sistema de Administração dos Recursos de Informação e Informática – SISPI, promovido pela MPOG/SLI, curso de Planejamento da Contratação de TI e ministrado pela ENAP.</p> <p>Recomenda-se que a área de Recursos Humanos da Conab inclua em seu Planejamento (LNT) a capacitação de mais gestores de TI da Sutin nas áreas solicitadas pelo Acórdão, por meio da ENAP.</p>	A mesma

Frederico Cabral de Menezes  
Gerência de Administração de Rede e Segurança da Informação  
Gerente

Gustavo Perdigão Meneses Lima  
Gerência de Suporte Técnico  
Gerente

Juliana Dantas da Fonseca  
Gerência de Engenharia de Software  
Gerente

Élcio Umezu  
Gerência de Sistemas de Informação  
Gerente

Benjamin Rodrigues da Silveira  
Superintendência de Gestão da Tecnologia da Informação  
Assistente

Marcelo Lins Faustino  
Superintendência de Gestão da Tecnologia da Informação  
Superintendente



## Anexo I - Projeto de Segurança da Informação

Escopo:

O Projeto abrange segurança da informação e governança de TI, e está estruturado nos seguintes subprojetos:

**METODOLOGIA DE GESTÃO DE RISCOS,**

**GAP ANALYSIS – ANÁLISE DOS PROCESSOS,**

**MODELO DE GESTÃO DE TRATAMENTO E RESPOSTAS A INCIDENTES DE SEGURANÇA,**

**SUBPROJETO ANÁLISE DE CONFORMIDADE - ABNT 15.408,**

**SUBPROJETO DE GESTÃO DE RISCOS, MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO** (definição da forma de atuação e funcionamento do comitê gestor de segurança da informação, que a norma de recursos computacionais da Conab prevê e que a diretoria da Conab ainda não instituiu),

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, quanto à governança de TI,** está dentro do subprojeto Gap Analysis o ambiente computacional será tratado de modo a identificar as medidas, ações e projetos necessários a sua adequação às normas ABNT NBR ISO/IEC 27001 e melhores práticas do Cobit 4.1 e ITIL V3.

**O que já foi feito /Situação Atual:** estudos realizados com vistas a especificação dos serviços a serem contratados. Especificações elaboradas, mas em fase de avaliação final pela equipe da Gerência de Administração de Rede e Segurança da Informação.

Entretanto, convém ressaltar que a execução do projeto retratará o momento, mas precisa permitir a alimentação dinâmica de dados. Se ficar apenas no papel, o trabalho tende a ser perdido com o tempo, pois ocorrem mudanças a todo momento na política e nos processos. Para isso, é importante o uso de software que permita a manutenção viva.

**Pendências/Decisões a serem tomadas:** Finalização das especificações, submetê-las ao mercado com vistas a obtenção de críticas e, posteriormente, propostas comerciais.

Todavia, o modelo proposto depende da tomada decisão quanto à adoção de uma das seguintes opções:

- a) contratação de software proprietário
- b) não utilização de nenhum software
- c) contratação de desenvolvimento do software de código aberto, transformando-o em software público.

Esta decisão decorre da seguinte razão: este tipo de software, comumente, é muito dispendioso, na casa de milhões de reais, e existem poucos que estão em poder de fornecedores especializados. Logo, estamos avaliando se é interessante desenvolver e tornar público ou adquirir a licença de uso sem direito ao código. Entretanto, para o desenvolvimento a equipe é insuficiente para dispor de tempo para especificar, tendo sido muito difícil se chegar até o ponto em que se encontram as especificações preliminares do termo de referência que está em construção.