Relatório de situação da área de Tecnologia da Informação do Tribunal de Contas do Estado de Goiás – TCEGO

Mauricio Barros de Jesus
Analista de Controle Externo
Agosto de 2015

Sumário

1. Descrição do objeto de trabalho

O estudo em tela trata da análise do ambiente de TI do Tribunal de Contas do Estado de Goiás - TCEGO, através do levantamento de potenciais falhas ou impropriedades que afetam a governança de TI e, direta ou indiretamente, a qualidade dos serviços prestados por essa área estratégica da Corte de Contas.

Foi utilizada a metodologia de entrevistas com os servidores e etnografia para levantamento de informações. Foram utilizados como referência diversos Acórdãos do TCU, principalmente o de número 866/2011, relatório de auditória que avaliou controles gerais de tecnologia da informação no Departamento Nacional de Infraestrutura de Transportes – DNIT.

Ressalta-se que as falhas e impropriedades identificadas devem ser vistas pela alta administração como oportunidade de melhoria, na qual os benefícios advindos constituem-se em fortalecimento dos controles internos do Tribunal e da Governança de TI, com consequente melhoria da qualidade dos serviços prestados pela TI para o TCEGO e para a sociedade.

Os pontos a serem tratados abordam problemas de planejamento estratégico da TI, ausência de processos, padrões e políticas, que colocam o TCEGO em risco quanto à proficiência da tecnologia no âmbito interno.

Além disso, ressaltou-se a ausência de estruturas normativas sobre contratações de bens e serviços de TI e de gestão de segurança da informação, específicas em TI, com escopo estadual, abrangendo inclusive os jurisdicionados. Por falta dessas normas, não existe em Goiás uma padronização das contratações de TI e da gestão de segurança da informação, culminado em deficiências na gestão de recursos e em riscos de perda de dados e exposição de informações importantes. A falta de normas com abrangência estadual provoca ineficiência das Auditorias de Sistemas nos jurisdicionados.

As principais falhas ou inconsistências identificadas foram:

a) Falhas no processo de planejamento de TI
b) Inexistência de Comitê de TI
c) Inexistência de um Comitê de Segurança da Informação e Comunicação
d) Inexistência de Gestor de Segurança da Informação e Comunicações
e) Quadro insuficiente de profissionais de TI

f) Processo de software inexistente ou pouco efetivo
g) Inexistência do processo de gestão de incidentes
h) Inexistência de inventário dos ativos de informação
i) Dificuldade na gestão contratual
j) Ausência de orçamento específico de TI
k) Ausência de planejamento de investimentos em TI
l) Ausência de normas estaduais que disponham especificamente de contratação bens e serviços de TI
m) Ausência de normas estaduais que disponham especificamente de segurança da informação e comunicação.
n) Inexistência do processo de gestão de configuração
o) Inexistência do processo de gestão de mudanças
p) Inexistência de plano de capacitação de TI

Para cada falha ou inconsistência foi relatada:

a) Situação encontra no ambiente de TI.
b) Consequência potencial para o negócio do TCEGO.
c) Critério utilizado que demonstra a não conformidade com norma ou melhores práticas.
d) Proposta de melhoria com base no critério utilizado.

Em um ambiente tão complexo como o da auditoria, missão institucional do TCEGO, é necessário buscar excelência na gestão de TI e qualidade dos produtos e serviços, como forma de tornar-se exemplo para os jurisdicionados. Importante também ressaltar que é fundamental o comprometimento da alta administração na solução dos problemas elencados.

Por fim, reforça-se a proposta de buscar melhoria da TI do TCEGO como um todo, levantando os pontos críticos de gestão que comprometem a qualidade dos serviços oferecidos. A partir dai, faz necessário traçar planejamento de curto, médio e longo prazo, que priorize cada item e que trate da resolução de cada um deles levando em consideração a força laboral do Tribunal.

2. Do alinhamento estratégico

Através da Secretaria de Planejamento e Desenvolvimento Institucional foi estabelecido o Planejamento Estratégico Institucional para os anos de 2014 a 2020. A partir dai planos de ações estão sendo pensados para os próximos anos. Percebe-se especial atenção á aplicação da TI como parceira estratégica das ações de Controle Externo.

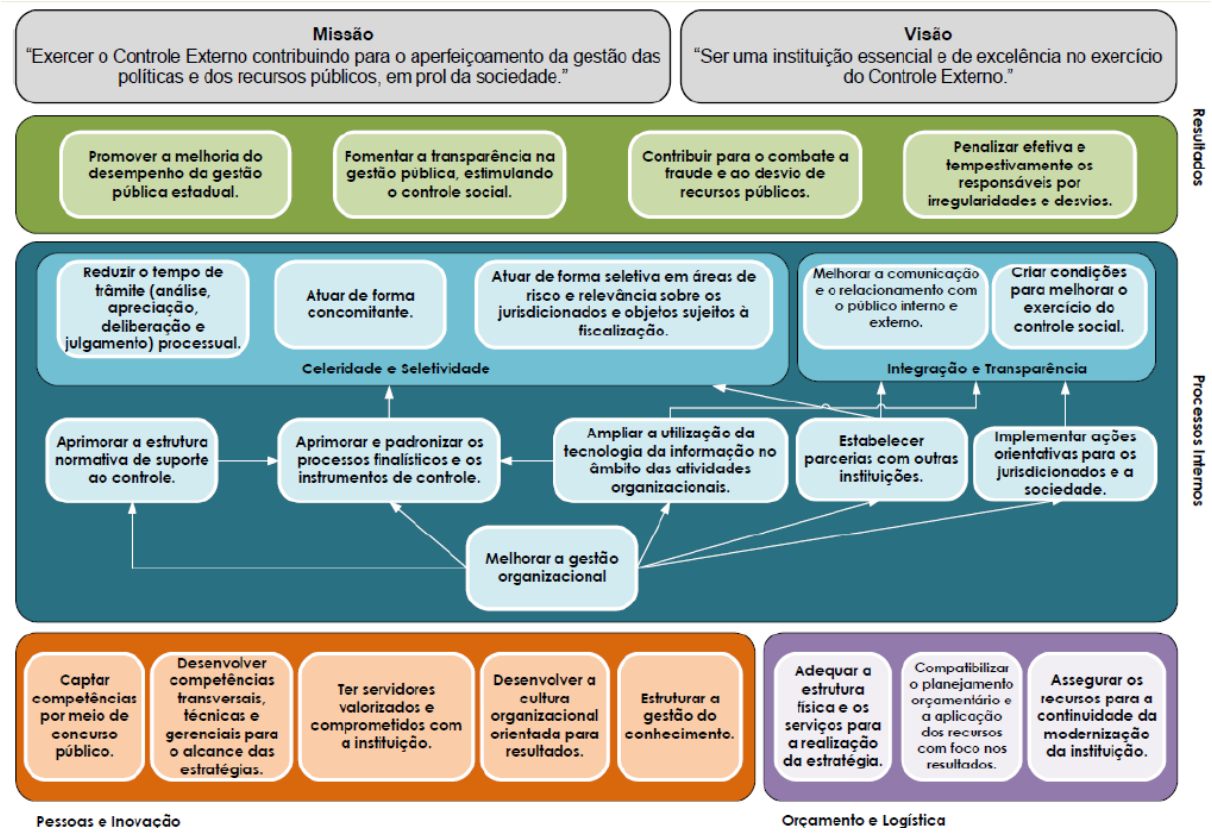

Figura 1: mapa estratégico

Apesar da necessidade de tecnologia na área fim do TCEGO, entendemos que a TI possui problemas internos graves que comprometem sua atuação efetiva em todas as áreas de negócio. Dessa forma, as ações propostas nesse documento têm como foco organizar internamente a TI, buscando fortalecimento da gestão e melhoria dos processos internos.

O quadro abaixo demostra o alinhamento das ações de melhoria propostas com os objetivos estratégicos do Plano Estratégico Institucional:

Perspectiva Pessoas e inovação		
Objetivo Estratégico	**Falha ou inconsistência**	**Proposta de melhoria**
Captar Competências por meio de concurso público. Ter servidores valorizados e comprometidos com a instituição	3.5. Quadro insuficiente de profissionais de TI	3.5.4.1. Realizar estudo técnico de avaliação do quadro de TI como base para pleitear realização de concurso público ou contratação de mão de obra terceirizada, para ampliação do quadro de TI, em conformidade com a Lei 15.222/2005, observando também as melhores práticas estabelecidas no Cobit 4.1 – PO4.12 – Pessoal de TI.

Desenvolver competências transversais e gerenciais para alcance das estratégias Ter servidores valorizados e comprometidos com a instituição	3.16. Inexistência de plano de capacitação de TI.	3.16.4.1. Elaborar um plano de capacitação anual, com estratégia de capacitação e atualização de conhecimento que leve em conta as necessidades de competências de TI, utilizando como referência as melhores práticas do Cobit 4.1, PO7.2 – Competências Pessoais e Cobit 4.1, PO7.4 – Treinamento do Pessoal.

Perspectiva Orçamento e Logística		
Objetivo Estratégico	**Falha ou inconsistência**	**Proposta de melhoria**
Compatibilizar o planejamento orçamentário e a aplicação de recursos com foco nos resultados	3.11 Ausências de planejamento de investimentos em TI	3.11.4.1. Realizar estudo sistemático de aquisições de TI de curto, médio e longo prazo, observando as necessidades estratégicas do TCE e o alinhamento ao planejamento estratégico institucional e ao planejamento estratégico de TI.
Assegurar os recursos para continuidade da modernização da instituição	3.10 Ausências de orçamento específico de TI	3.10.4.1. Propor criação de orçamento específico de TI no TCE

	3.9 Dificuldades na gestão contratual	3.9.4.1. Adequar a métrica homem/hora com base em estimativas de demandas bem definidas para os contratos atuais. 3.9.4.2. Institucionalizar métricas de software com base no resultado esperado, de acordo com as melhores práticas de mercado.

Perspectiva Processos Internos		
Objetivo Estratégico	**Falha ou inconsistência**	**Proposta de melhoria**
Melhorar a gestão organizacional	3.1. Falhas no processo de planejamento de TI	3.1.4.1. Estabelecer PETI observando as práticas contidas no Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.
		3.1.4.2. Estabelecer PDTI observando as práticas contidas no Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.
	3.2. Inexistência de Comitê de TI	3.2.4.1. Estabelecer Comitê de TI conforme melhores práticas estabelecidas no Cobit 4.1 – PO4.3 – Comitê diretor de TI e Cobit 4.1- PO4.2 – Comitê Estratégico de TI.
	3.3. Inexistência de um Comitê de Segurança da Informação e Comunicação	3.3.4.1. Estabelecer Comitê de Segurança da Informação e Comunicação.
	3.4. Inexistência de Gestor de Segurança da Informação e Comunicações	3.4.4.1. Estabelecer Gestor de Segurança da Informação.
	3.14. Inexistência do processo de gestão de configuração	3.14.4.1. Implementar gestão de configuração conforme orientações do Cobit 4.1 – DS9 – Gerenciar Configuração.
	3.15. Inexistência do processo de gestão de mudanças	3.15.4.1. Estabelecer procedimentos formais de gestão de mudanças, de acordo com a NBR ISO/IEC 27002, item 12.5.1 – Procedimentos para controle de mudanças, e observando as melhores práticas estabelecidas no Cobit 4.1 – AI6 – Gerenciar Mudanças.

	3.7. Inexistência do processo de gestão de incidentes	3.7.4.1. Implementar a gestão de incidentes com base Cobit 4.1 DS8 – Gerenciar a central de serviços e incidentes, aproveitando a atual estrutura de Central de Serviços atualmente implantada.
	3.8. Inexistência de inventário dos ativos de informação	3.8.5.1. Estabelecer inventário de ativos de informação, de forma que todos ativos sejam catalogados e tenham um responsável, conforme melhores práticas presentes na NBR ISO/IEC 27002, item 7.1.1 – Inventário de ativos.
	3.6. Processo de software inexistente ou pouco efetivo	3.6.4.1. Desenvolver um processo de software do TCE – PDSTCE - que subsidie o desenvolvimento, manutenção ou aquisição de software, em conformidade com as melhores práticas do Cobit 4.1 – PO8.3 – Padrões de Desenvolvimento e de aquisições.

Estabelecer parcerias com outas instituições Aprimorar a estrutura normativa de suporte ao controle Aprimorar e padronizar os processos finalísticos e os instrumentos de controle	3.13. Ausência de normas estaduais que disponham especificamente de segurança da informação e comunicação.	3.12.4.1. Instituir grupos de trabalho para estabelecimento de norma sobre o processo de contratação de soluções de TI no âmbito do TCE. 3.12.4.2. Utilizar de maneira subsidiária a Instrução Normativa Nº 4 - MP/SLTI/MPOG/2014 nos casos de ausência de legislação estadual específica. 3.12.4.3. Estabelecer parceria com a Secretaria de Estado de Gestão e Planejamento-SEGPLAN, para elaboração de norma específica sobre o processo de contratação de soluções de TI no âmbito do Estado de Goiás.
Implementar ações orientativas e educativas para os jurisdicionados e a sociedade.	3.13. Ausência de normas estaduais que disponham especificamente de segurança da informação e comunicação.	3.13.5.1. Instituir grupos de trabalho para estabelecimento de normas de segurança da informação no âmbito do TCE. 3.13.5.2. Utilizar de maneira subsidiária a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e suas normas decorrentes, nos casos de ausência de legislação específica Estadual.

		3.13.5.3. Estabelecer parceria com a Secretaria de Estado de Gestão e Planejamento-SEGPLAN, para elaboração de normas específicas sobre segurança da informação no âmbito do Estado de Goiás.

Planilha 1: alinhamento estratégico das propostas de melhoria

3. Da definição da maturidade institucional

Modelos de maturidade são importantes ferramentas para definir a qualidade e a confiabilidade dos produtos e dos processos de uma organização. A definição de níveis de maturidade não é requisito obrigatório para a maioria das instituições, mas é importante para definição de metas do planejamento da TI.

Não foram encontradas iniciativas de definição de nível de maturidade para Governança de TI no TCEGO. Tampouco existe definição de maturidade para os serviços de TI. Todavia, para desenvolvimento de software, foi utilizado o modelo MPS.BR como referência e definido o grau de Maturidade “F” para esse Tribunal.

Em relação à definição de nível de maturidade para Governança de TI, o COBIT 4.1 pode ser utilizado para avaliar o desempenho dos processos do TCEGO. Quanto á avaliação do nível de maturidade dos serviços de TI, o ITIL 2011 pode ser utilizado como ferramenta de diagnóstico.

Em relação à avaliação da maturidade dos processos de desenvolvimento de software segundo o MPS.BR, o Nível F – Gerenciado, requer primeiramente o cumprimento do Nível G – Parcialmente Gerenciado. Entretanto existe dificuldade de avaliar a atual aderência do processo de desenvolvimento empregado com o modelo de referência adotado. Nesse caso é importante realizar o levantamento de conformidade do processo de desenvolvimento de software de acordo com o resultado esperado.

Como sugestão, as planilhas abaixo podem ser utilizadas para avaliação da aderência ao MPS.BR. Para cada Atributo/Processo, considerando o resultado esperado por processo, bastaria preencher as planilhas com as entradas:

- “Realizado”: quando o processo atender completamente a todos os resultados esperados.
- “Parcialmente Realizado”: quando o processo atender a mais de 50% dos resultados esperados.

- "Não realizado": quando o processo atender a menos de 50% dos resultados esperados.

NÍVEL G – PARCIALMENTE GERENCIADO		
Atributo/Processo	**Gerência de Projetos – GPR**	**Gerência de Requisitos**
AP 1.1 - Processo é Executado		
AP 2.1 - Processo é Gerenciado		

Planilha 2: avaliação do MPS.BR Nível G – Parcialmente Gerenciado

NÍVEL F – GERENCIADO				
Atributo/Processo	**Aquisição – AQU**	**Gerência de Configuração – GCO**	**Garantia da Qualidade – GQA**	**Gerência de Portfólio de Projetos – GPP**
AP 1.1 - Processo é Executado				
AP 2.1 - Processo é Gerenciado				
AP 2.2 - Produto de processo é gerenciado				

Planilha 3: avaliação do MPS.BR Nível F –Gerenciado

De acordo com a resposta das planilhas de avaliação de conformidade, caso exista alguma entrada diferente de "Realizado", ações de correção podem ser adotadas.

4. Detalhamento das falhas e inconsistências

4.1. **Falhas no processo de planejamento de TI**

4.1.1. Situação

4.1.1.1. Falta do Plano Estratégico de TI - PETI

4.1.1.2. Falta do Plano Diretor de TI - PDTI

4.1.2. Consequência

4.1.2.1. Risco das ações de TI não estarem alinhadas ao negócio.

4.1.3. Critério

4.1.3.1. Cobit 4.1, PO1 – Planejamento Estratégico de TI.

4.1.4. Proposta

4.1.4.1. Estabelecer PETI observando as práticas contidas no Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.

4.1.4.2. Estabelecer PDTI observando as práticas contidas no Cobit 4.1, processo PO1 – Planejamento Estratégico de TI; e melhores práticas do Guia de Elaboração do PDTI, elaborado pelo Ministério do Planejamento, Orçamento e Gestão do Governo Federal.

4.2. **Inexistência de Comitê de TI**

4.2.1. Situação

4.2.1.1. O TCE não designou formalmente um Comitê de TI para auxilio nas decisões de gestão e uso de TI.

4.2.2. Consequência

4.2.2.1. Priorização inadequada de projetos e ações de TI devido à ausência de participação de áreas de negócio.

4.2.2.2. Sobreposição de ações de TI por parte das áreas de negócio.

4.2.2.3. Desconhecimento das necessidades de negócio por parte da TI.

4.2.2.4. Não alinhamento de investimentos de TI com os objetivos institucionais.

4.2.3. Critério

4.2.3.1. Constituição Federal, art. 37, caput.

4.2.3.2. Cobit 4.1 – PO4.3 – Comitê diretor de TI.

4.2.3.3. Cobit 4.1- PO4.2 – Comitê Estratégico de TI;

4.2.4. Proposta

4.2.4.1. Estabelecer Comitê de TI conforme melhores práticas estabelecidas no Cobit 4.1 – PO4.3 – Comitê diretor de TI e Cobit 4.1- PO4.2 – Comitê Estratégico de TI.

4.3. **Inexistência de um Comitê de Segurança da Informação e Comunicação**

4.3.1. Situação

4.3.1.1. O TCE não designou formalmente um Comitê de Segurança da Informação para auxilio nas decisões relativas à segurança da informação;

4.3.2. Consequência

4.3.2.1. Ações de segurança da informação não são otimizadas.

4.3.2.2. Desinformação quanto às normas de segurança da informação,

4.3.2.3. Falta de apoio da alta administração nas ações de segurança da informação.

4.3.3. Critérios

4.3.3.1. NBR ISO/IEC 27002, item 6.1.2 – Coordenação de segurança da informação.

4.3.4. Proposta

4.3.4.1. Estabelecer Comitê de Segurança da Informação e Comunicação.

4.3.4.1.1. Como o Estado de Goiás não possui normas específicas para segurança da informação que tratem do Comitê de Segurança da Informação e Comunicação, utilizar de forma subsidiária até que se estabeleça norma semelhante no Tribunal, a IN – GSI/PR 1/2008, art. 5º, inciso VI; e a Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.3; para instituir o Comitê de Segurança da Informação e Comunicação no âmbito do TCEGO, em conformidade com as melhores práticas da NBR ISO/IEC 27002, item 6.1.2 – Coordenação de segurança da informação.

4.4. **Inexistência de Gestor de Segurança da Informação e Comunicações**

4.4.1. Situação

4.4.1.1. O TCE não designou formalmente um Gestor de Segurança da Informação para auxilio nas decisões relativas à segurança da informação;

4.4.2. Consequência

4.4.2.1. Ações de segurança da informação não são otimizadas.

4.4.3. Critérios

4.4.3.1. NBR ISO/IEC 27002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação.

4.4.4. Proposta

4.4.4.1. Estabelecer Gestor de Segurança da Informação.

4.4.4.1.1. Como o Estado de Goiás não possui normas específicas para segurança da informação que tratem do papel do Gestor de Segurança da Informação, utilizar de forma subsidiária até que se estabeleça norma semelhante no Tribunal, a IN – GSI/PR 1/2008, art. 5º, inciso VI e art. 7º; e a Norma Complementar 03/IN01/DSIC/GSIPR, item 5.3.7.2; para instituir o Gestor de Segurança da Informação, em conformidade com as melhores práticas da NBR ISO/IEC 27002 item 6.1.3 – Atribuição de responsabilidade para segurança da informação.

4.5. **Quadro insuficiente de profissionais de TI**

4.5.1. Situação

4.5.1.1. Apenas quatro servidores efetivos lotados na Gerência de TI;

4.5.1.2. Não há um estudo com critérios objetivos que identifique com clareza o quantitativo necessário de pessoal de TI.

4.5.1.3. Empregados terceirizados com vínculo com duração de mais de dez anos, realizando atividades inerentes ao cargo de Analista de Controle Externo, Especialidade Tecnologia da Informação, previstas no Plano de Carreira e Quadro Permanente dos Servidores do Tribunal de Contas, conforme Lei 15.122/2005.

4.5.2. Consequência

4.5.2.1. Dependência de serviço de empresas terceirizadas.

4.5.2.2. Recursos humanos de TI insuficientes para atender às necessidades do negócio.

4.5.2.3. Falta de competências apropriadas na área de TI.

4.5.3. Critérios

4.5.3.1. Cobit 4.1 – PO4.12 – Pessoal de TI.

4.5.3.2. Lei 15.222/2005 - Plano de Carreira e Quadro Permanente dos Servidores do Tribunal de Contas do Estado de Goiás.

4.5.4. Proposta

4.5.4.1. Realizar estudo técnico de avaliação do quadro de TI como base para pleitear realização de concurso público ou contratação de mão de obra terceirizada, para ampliação do quadro de TI, em conformidade com a Lei 15.122/2005, observando também as melhores práticas estabelecidas no Cobit 4.1 – PO4.12 – Pessoal de TI.

4.6. **Processo de software inexistente ou pouco efetivo**

4.6.1. Situação encontrada

4.6.1.1. Foi elaborado um processo de software específico baseado no MPS-BR. Todavia na prática é utilizada de maneira informal a o Scrum.

4.6.2. Consequência

4.6.2.1. Inexistência de parâmetros para avaliação da qualidade de software.

4.6.2.2. Ineficiência no processo de desenvolvimento, manutenção ou aquisição de software.

4.6.3. Critérios

4.6.3.1. Lei 8.666/1993, art. 6º, inciso IX;

4.6.3.2. Cobit 4.1 – PO8.3 – Padrões de Desenvolvimento e de aquisições.

4.6.3.3. NBR ISO/IEC 12207 – Estabelece uma estrutura para processos de ciclo de vida de software.

4.6.3.4. NBR/IEC 15504 – Avaliação de processo de software

4.6.4. Proposta

4.6.4.1. Desenvolver um processo de software do TCE – PDS.TCE - que subsidie o desenvolvimento, manutenção ou aquisição de software, em conformidade

com as melhores práticas do Cobit 4.1 – PO8.3 – Padrões de Desenvolvimento e de aquisições.

4.6.4.1.1. Toda e qualquer contratação serviço de desenvolvimento, manutenção ou aquisição de software futura deve estar vinculada ao processo de software dessa Corte de Contas.

4.7. **Inexistência do processo de gestão de incidentes**

4.7.1. Situação encontrada

4.7.1.1. O TCE possui um sistema da Central de Serviços (Service Desk) consolidada, que tua na resolução de qualquer evento, ou seja, na restauração imediata dos serviços. Todavia a gestão de incidentes não é realizada, a priorização é feita sem critérios objetivos, não se diferencia evento, incidente, problema, erro conhecido.

4.7.2. Consequência

4.7.2.1. Incidentes sem o devido gerenciamento;

4.7.2.2. Possível paralização de serviços de TI

4.7.2.3. Possível paralização das atividades do TCE;

4.7.3. Critérios

4.7.3.1. Constituição Federal, art. 37, caput;

4.7.3.2. Cobit 4.1 DS8 – Gerenciar a central de serviços e incidentes

4.7.3.3. ITIL V3 – Operação de serviço – Gerenciamento de incidentes

4.7.3.4. NBR ISO/IEC 27002, item 13 – Gestão de incidentes de segurança da informação.

4.7.4. Proposta

4.7.4.1. Implementar a gestão de incidentes com base Cobit 4.1 DS8 – Gerenciar a central de serviços e incidentes, aproveitando a atual estrutura de Central de Serviços implantada, observando melhores práticas do ITIL V3 – Operação de serviço – Gerenciamento de incidentes; e controles da NBR ISO/IEC 27002, item 13 – Gestão de incidentes de segurança da informação.

4.8. **Inexistência de inventário dos ativos de informação**

4.8.1. Situação

4.8.1.1. Não foi encontrado inventário consolidado de ativos de informação.

4.8.2. Consequência

4.8.2.1. Informações sobre ativos dispersas em diversos documentos.

4.8.2.2. Informação críticas sobre ativos de conhecimento apenas de empregados terceirizados.

4.8.2.3. Dificuldade de recuperação de ativo de informação.

4.8.3. Critério

4.8.3.1. NBR ISO/IEC 27002, item 7.1.1 – Inventário de ativos.

4.8.4. Proposta

4.8.4.1. Estabelecer inventário de ativos de informação, de forma que todos ativos sejam catalogados e tenham um responsável, conforme melhores práticas presentes na NBR ISO/IEC 27002, item 7.1.1 – Inventário de ativos.

4.9. **Dificuldade na gestão contratual**

4.9.1. Situação

4.9.1.1. Na gestão do contrato não há avaliação da qualidade dos produtos adquiridos. Não é avaliado o cumprimento dos acordos de níveis de serviço.

4.9.1.2. A forma de pagamento no contrato não é vinculada a resultados obtidos. A métrica utilizada para o desenvolvimento de sistemas é homem/hora, o que não pode ser associada ao resultado esperado, pois não vincula o pagamento aos resultados obtidos, com tendência a remunerar todas as horas de disponibilidade dos empregados da empresa, ainda que não produtivas, conforme versa o Acórdão TCU nº 786/2006 – Plenário.

4.9.1.3. Não há uma estimativa em análise prévia do volume de serviços por demanda. Por isso, não há uma medida direta de produtividade, pois não há comparativo entre a quantidade de homem/hora prevista e a quantidade efetivamente utilizada por demanda de trabalho.

4.9.2. Consequência

4.9.2.1. Risco de ocorrer aquisição que não atenda à necessidade do órgão.

4.9.2.2. Impossibilidade de estabelecer o valor agregado pela TI ao negócio;

4.9.2.3. Impossibilidade de estabelecer o retorno sobre investimento (ROI) para os produtos de TI.

4.9.3. Critério

4.9.3.1. Acórdão 2.471/2008-Plenário.

4.9.3.2. Cobit 4.1, ME3.3 – Avaliar a conformidade com requisitos externos.

4.9.3.3. Cobit 4.1, AI5.2 – Gerir contratos com fornecedores.

4.9.3.4. Cobit 4.1, DS2.4 – Monitorar o desempenho do fornecedor.

4.9.4. Proposta

4.9.4.1. Adequar a métrica homem/hora com base em estimativas de demandas bem definidas para os contratos atuais, de forma a atrelar o resultado esperado ao pagamento efetuado.

4.9.4.1.1. Sabe-se que o contrato atual de desenvolvimento de sistemas expira em julho de 2016. Diante dessa situação, manter a atual forma de pagamento com a métrica homem/hora. Todavia, definir processo de gestão de demandas para área terceirizada, com estimativa de esforço baseado em homem/hora definida e com prazos de entregas semanal e mensal.

4.9.4.2. Institucionalizar métricas de software com base no resultado esperado, de acordo com as melhores práticas de mercado.

4.9.4.2.1. Para as próximas contratações de aquisição, desenvolvimento ou manutenção de software, utilizar as melhores práticas de métricas de software voltadas para resultado, como a estimativa por portos de função do IFPUG.

4.10. **Ausência de orçamento específico de TI**

4.10.1. Situação

4.10.1.1. Não foi encontrado orçamento de específico para TI.

4.10.2. Consequência

4.10.2.1. Recursos insuficientes para TI

4.10.2.2. Interrupção de serviços de TI por falta de recursos necessários;

4.10.2.3. Não alcance de metas organizacionais por falta de suporte da área de TI.

4.10.3. Critério

4.10.3.1. Cobit 4.1 – PO5.3 – Processo de Orçamento de TI.

4.10.4. Proposta

4.10.4.1. Propor criação de orçamento específico de TI no TCEGO, de forma que sustente as ações estratégicas organizacionais, observando as melhores práticas do Cobit 4.1 – PO5.3 – Processo de Orçamento de TI.

4.11. **Ausência de planejamento de investimentos em TI**

4.11.1. Situação

4.11.1.1. Não foi encontrado um planejamento de investimentos em TI.

4.11.2. Consequência

4.11.2.1. Recursos insuficientes para TI

4.11.2.2. Interrupção de serviços de TI por falta de recursos necessários;

4.11.2.3. Não alcance de metas organizacionais por falta de suporte da área de TI.

4.11.3. Critério

4.11.3.1. Cobit 4.1 – PO5.3 – Processo de Orçamento de TI.

4.11.4. Proposta

4.11.4.1. Realizar estudo sistemático de aquisições de TI de curto, médio e longo prazo, observando as necessidades estratégicas do TCE e o alinhamento ao planejamento estratégico institucional e ao planejamento estratégico de TI, de acordo com as melhores práticas do Cobit 4.1 – PO5.3 – Processo de Orçamento de TI.

4.12. **Ausência de normas estaduais que disponham especificamente de contratação bens e serviços de TI**

4.12.1. Situação

4.12.1.1. Não foram encontradas normas estaduais que tratem especificamente de aquisição de bens e serviços de TI.

4.12.2. Consequência

4.12.2.1. Dificuldade de padronização de aquisições de TI;

4.12.2.2. Dificuldade de realização de auditorias específicas de aquisições de TI nos jurisdicionados;

4.12.3. Critério

4.12.3.1. Lei 8666/1993;

4.12.3.2. Decreto Estadual Nº 7.468, DE 20 DE OUTUBRO DE 2011 - Aprova o regulamento da modalidade de licitação denominada pregão, para a aquisição de bens e serviços comuns, no âmbito do Estado de Goiás.

4.12.3.3. Instrução Normativa Nº 4 - MP/SLTI/MPOG, de 11 de setembro de 2014.

4.12.4. Proposta

4.12.4.1. Instituir grupos de trabalho para estabelecimento de norma sobre o processo de contratação de soluções de TI no âmbito do TCEGO.

4.12.4.2. Utilizar de maneira subsidiária a Instrução Normativa Nº 4 - MP/SLTI/MPOG/2014 nos casos de ausência de legislação estadual específica.

4.12.4.3. Estabelecer parceria com a Secretaria de Estado de Gestão e Planejamento-SEGPLAN, para elaboração de norma específica sobre o processo de contratação de soluções de TI no âmbito do Estado de Goiás.

4.13. **Ausência de normas estaduais que disponham especificamente de segurança da informação e comunicação.**

4.13.1. Situação

4.13.1.1. Não foram encontradas normas estaduais que tratem especificamente de segurança da informação e comunicação.

4.13.2. Consequência

4.13.2.1. Ausência de padronização de estruturas gerenciais mínimas voltadas para a segurança da informação;

4.13.2.2. Dificuldade de realização de auditorias específicas em segurança da informação e comunicação nos jurisdicionados;

4.13.2.3. Dificuldade de responsabilização em casos de perdas causadas pela má administração da segurança da informação.

4.13.3. Critério

4.13.3.1. Rol de normas complementares do Gabinete de Segurança Institucional da Presidência da República (http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/52-instrucoes-normativas).

4.13.3.2. NBR ISO/IEC 27001 e NBR ISO/IEC 27002.

4.13.4. Proposta

4.13.4.1. Instituir grupos de trabalho para estabelecimento de normas de segurança da informação no âmbito do TCE.

4.13.4.2. Utilizar de maneira subsidiária a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e suas normas decorrentes, nos casos de ausência de legislação estadual específica.

4.13.4.3. Estabelecer parceria com a Secretaria de Estado de Gestão e Planejamento-SEGPLAN, para elaboração de normas específicas sobre segurança da informação no âmbito do Estado de Goiás.

4.14. **Inexistência do processo de gestão de configuração**

4.14.1. Situação

4.14.1.1. Não foi encontrado processo de gestão de configuração. Para software é feito versionamento de artefatos com Team Foundation Server.

4.14.2. Consequência

4.14.2.1. Deficiência ou desatualização da configuração de TI

4.14.3. Critério

4.14.3.1. Cobit 4.1 DS9 – Gerenciar Configuração

4.14.4. Proposta

4.14.4.1. Implementar gestão de configuração conforme orientações do Cobit 4.1 – DS9 – Gerenciar Configuração.

4.15. **Inexistência do processo de gestão de mudanças**

4.15.1. Situação

4.15.1.1. Não foi encontrado processo de gestão de mudanças.

4.15.2. Consequência

4.15.2.1. Mudanças não controladas em ativos de TI.

4.15.2.2. Não avaliação do impacto de eventuais mudanças;

4.15.2.3. Risco de uma mudança de ativo de TI causar prejuízo ao negócio do TCEGO.

4.15.3. Critério

4.15.3.1. Cobit 4.1 – AI6 – Gerenciar Mudanças.

4.15.3.2. NBR ISO/IEC 27002, item 12.5.1 – Procedimentos para controle de mudanças.

4.15.4. Proposta

4.15.4.1. Estabelecer procedimentos formais de gestão de mudanças, de acordo com a NBR ISO/IEC 27002, item 12.5.1 – Procedimentos para controle de mudanças, e observando as melhores práticas estabelecidas no Cobit 4.1 – AI6 – Gerenciar Mudanças.

4.16. **Inexistência de plano de capacitação de TI**

4.16.1. Situação

4.16.1.1. Não foi encontrado um plano de capacitação específico de TI.

4.16.2. Consequência

4.16.2.1. Desatualização de competências no quadro de pessoal do TCEGO

4.16.3. Critério

4.16.3.1. Cobit 4.1, PO7.2 – Competências Pessoais

4.16.3.2. Cobit 4.1, PO7.4 – Treinamento do Pessoal.

4.16.4. Proposta

4.16.4.1. Elaborar um plano de capacitação anual, com estratégia de capacitação e atualização de conhecimento que leve em conta as necessidades de competências de TI, utilizando como referência as melhores práticas do Cobit 4.1, PO7.2 – Competências Pessoais e Cobit 4.1, PO7.4 – Treinamento do Pessoal.

5. Conclusão

Após análise crítica do ambiente e levantamento da situação da TI do TCEGO, foram observadas falhas principalmente no planejamento das ações de TI.

Por outro lado existe o sentimento no corpo técnico do Tribunal de que mudanças são necessárias e diversas ações estão sendo planejadas para os próximos anos. Através da Secretaria de Planejamento e Desenvolvimento Organizacional foi estabelecido o Planejamento estratégico Institucional de 2015 a 2020. Esse documento deve ser a base para o planejamento das ações de TI nos próximos anos.

Em relação às falhas elencadas no corpo desse documento, cabe ao Gestor de TI a tomada de decisões e priorização de ações. Ressalta-se o caráter informativo desse documento com o apontamento de proposta de melhoria da TI do TCEGO como um todo. Além disso, as falhas aqui elencadas são aquelas encaradas como mais graves considerando aspectos de Gestão e Governança de TI.

Espera-se que essas informações sejam úteis na tomada de decisão por parte da alta direção do TCEGO e que ações de melhoria sejam tomadas. Entende-se que é preciso organizar a TI do TCEGO de maneira profissional, considerando as melhores práticas de mercado, para tornar esse Tribunal referencia no Estado de Goiás.