TRIBUNAL DE CONTAS DA UNIÃO

Auditoria de Tecnologia da Informação e a Experiência do TCU

Ministro Substituto Augusto Sherman

Fortaleza, abril de 2011

Agenda

- ✓ Introdução
- ✓ Histórico
- ✓ Estratégia de Atuação da Sefti
- ✓ Planejamento da Auditoria
- ✓ Avaliação de Governança de TI
- ✓ Resultados
- ✓ Conclusão

Introdução

Tecnologia da Informação (TI)

- Os recursos necessários para adquirir, processar, armazenar e disseminar **informações**. (NBR ISO/IEC 38500:2009)

Importância da TI na APF

- ✓ Materialidade:
  - A União programou gastar **R$ 18 bilhões** em 2011 com TI
- ✓ Criticidade:
  - Todas as áreas críticas da Administração Pública **dependem** de TI

Importância da TI na APF

"A tecnologia da informação é o '**coração**' da administração pública, podendo fazê-la parar ou avançar".

Histórico

Antes da Sefti

Fiscalizações de TI (1994 - 2006)

- ✓ 29 fiscalizações de TI
- ✓ Foco: auditorias de **sistemas** e **dados**
- ✓ Alguns exemplos:
  - Sistemas de Arrecadação Federal
  - Sistemas do Bacen e Caixa
  - Siape, Siafi e Sipia
  - Sistemas da Previdência Social
  - Programa E-Gov
  - Governança no MTE
  - Governança na Infraero

Antes da Sefti

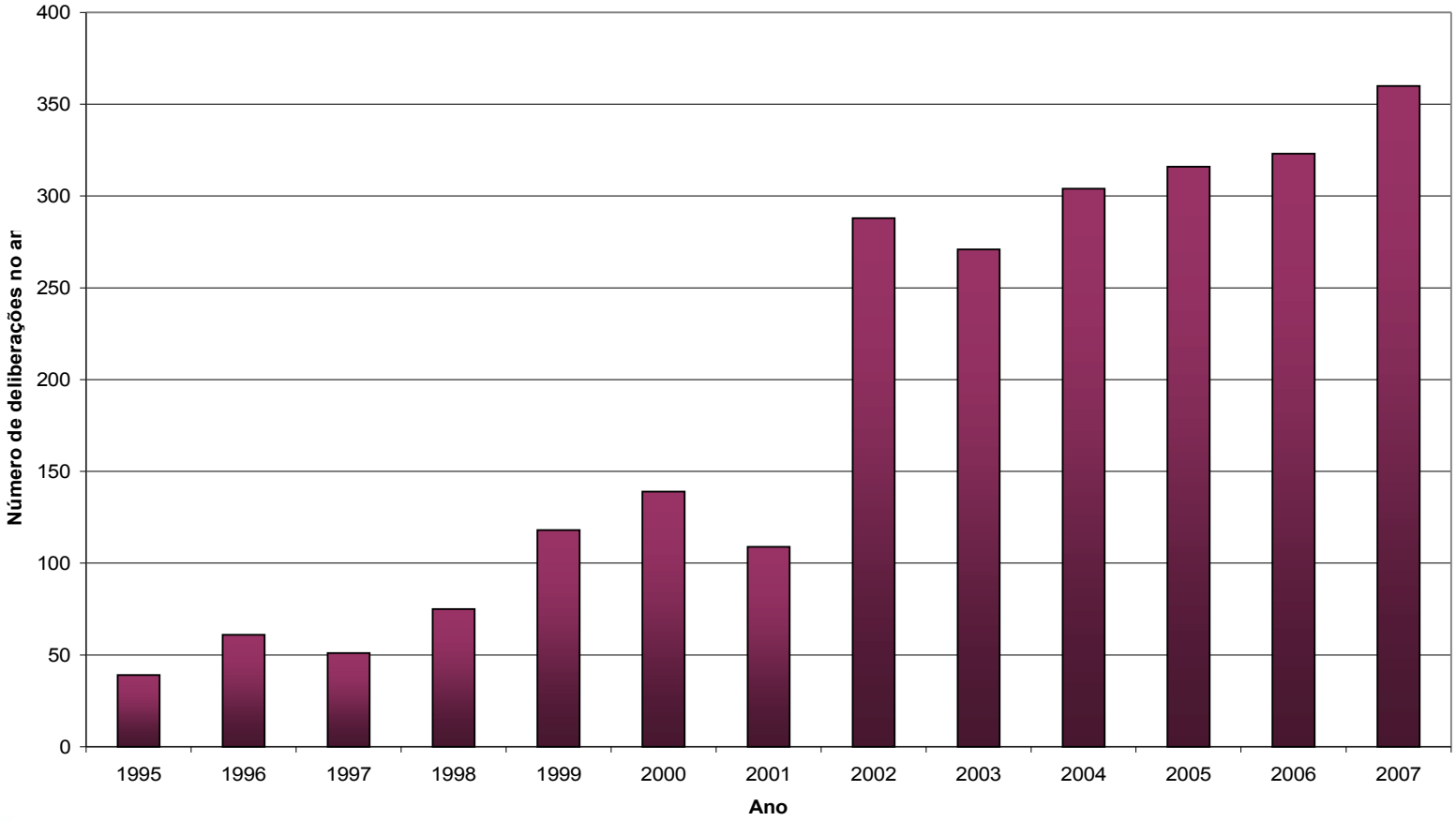
- ✓ Normatização (1997-1998)
  - Manual e procedimentos de auditoria de sistemas
- ✓ Orientações aos gestores (2003)
  - Cartilha “Boas práticas em segurança da informação”
- ✓ Cursos de auditoria de TI (1998 - 2006)
- ✓ Participação em comitês internacionais

Antes da Sefti

Fiscalizações de **Contratações de TI** (2003 - 2006)

- ✓ Foco: modalidade das licitações, planejamento da contratação, quantitativo e qualificação da equipe de TI
- ✓ Principais Acórdãos:
  - Acórdão 1.521/2003-TCU-Plenário (necessidade de se especificar a quantidade dos produtos a serem adquiridos);
  - Acórdão 1.558/2003-TCU-Plenário (necessidade de planejamento das contratações de TI);
  - Acórdão 2.094/2004-TCU-Plenário (alinhamento entre planejamento da contratação e planejamento estratégico do órgão/entidade);
  - Acórdão 140/2005-TCU-Plenário (necessidade de quadro com quantidade e qualificação adequadas de servidores de TI nos órgãos/entidades);
  - Acórdão 2.138/2005-TCU-Plenário (o uso do pregão na contratação de bens e serviços de TI);

Acórdãos TCU relacionados com Contratações de TI



Evolução da quantidade de acórdãos do TCU relacionados com contratações de TI (fonte: TC-019.230/2007-2)

Estratégia de Atuação da Sefti

Criação da Sefti

- Criada em **agosto de 2006** (Resolução TCU nº 193/2006)
  - "A Secretaria de Fiscalização de Tecnologia da Informação tem por finalidade **fiscalizar a gestão e o uso** de recursos de tecnologia da informação pela Administração Pública Federal."

Negócio

Controle externo da **governança de tecnologia da informação** na Administração Pública Federal

Missão

Assegurar que a tecnologia da informação **agregue valor ao negócio** da Administração Pública Federal em benefício da sociedade

Visão

Ser unidade de excelência no controle e **no aperfeiçoamento da governança de tecnologia da informação**

Áreas de atuação

- ✓ Governança
- ✓ Programas e políticas
- ✓ Segurança
- ✓ Sistemas
- ✓ Dados
- ✓ Infraestrutura
- ✓ Contratações de TI

Fiscalização operacional e/ou conformidade

Estrutura da Sefti

- ✓ 3 divisões de fiscalização de governança de TI, 2 assessores e serviço de administração

- ✓ 30 servidores: 27 auditores e 3 técnicos

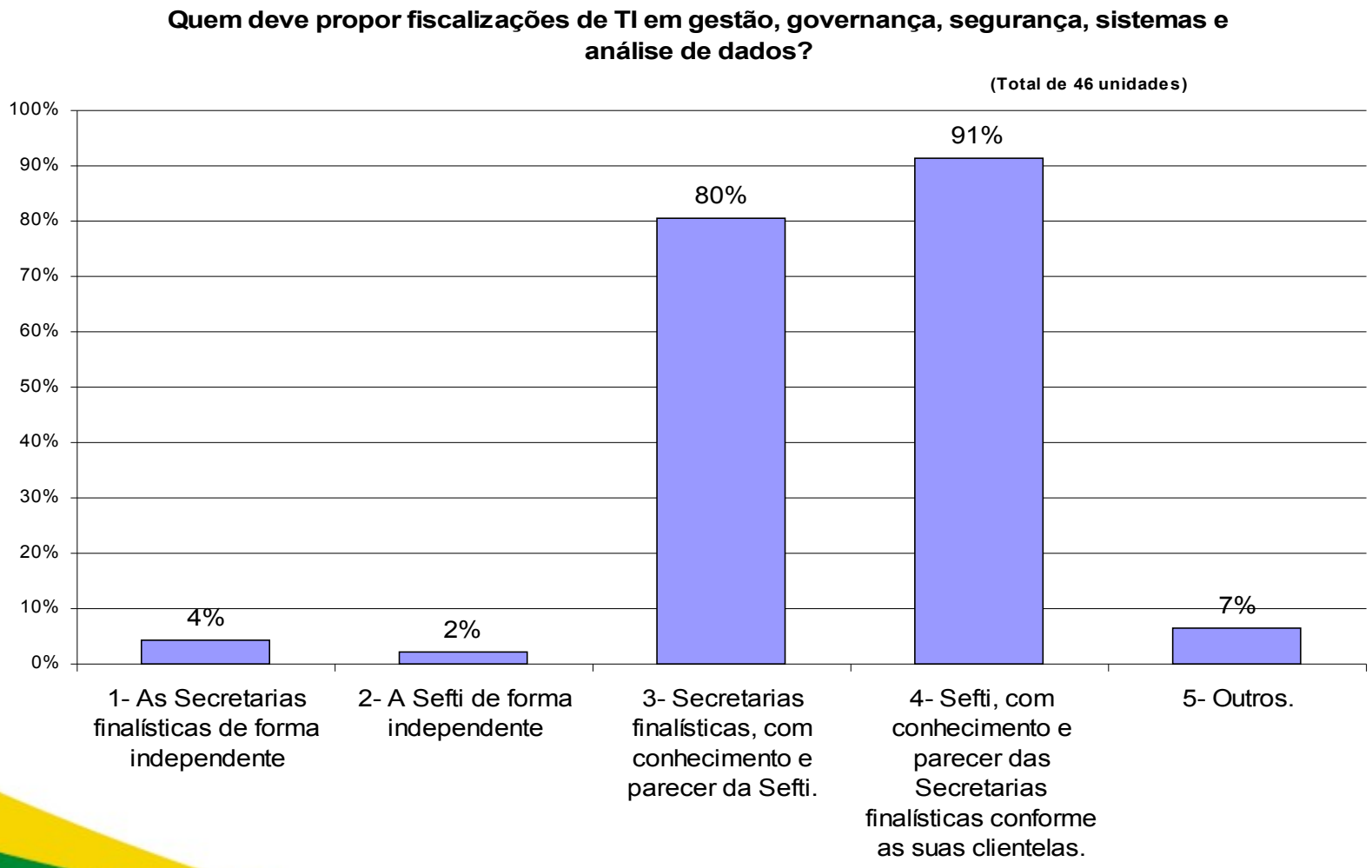
Competência Profissional

- ✓ Formação em áreas de tecnologia
  - Ciência da Computação, Engenharia e afins
- ✓ Certificações
  - 12 auditores CISA (*Certified Information Systems Auditor*)
  - 2 auditores CGEIT (*Certified in the Governance of Enterprise*)
  - 2 auditores CGAP (*Certified Government Auditor Professional*)
  - 1 auditor CISSP (*Certified Information Systems Security Professional*)
- ✓ Mestrados – 3 servidores
- ✓ MBA – 8 servidores

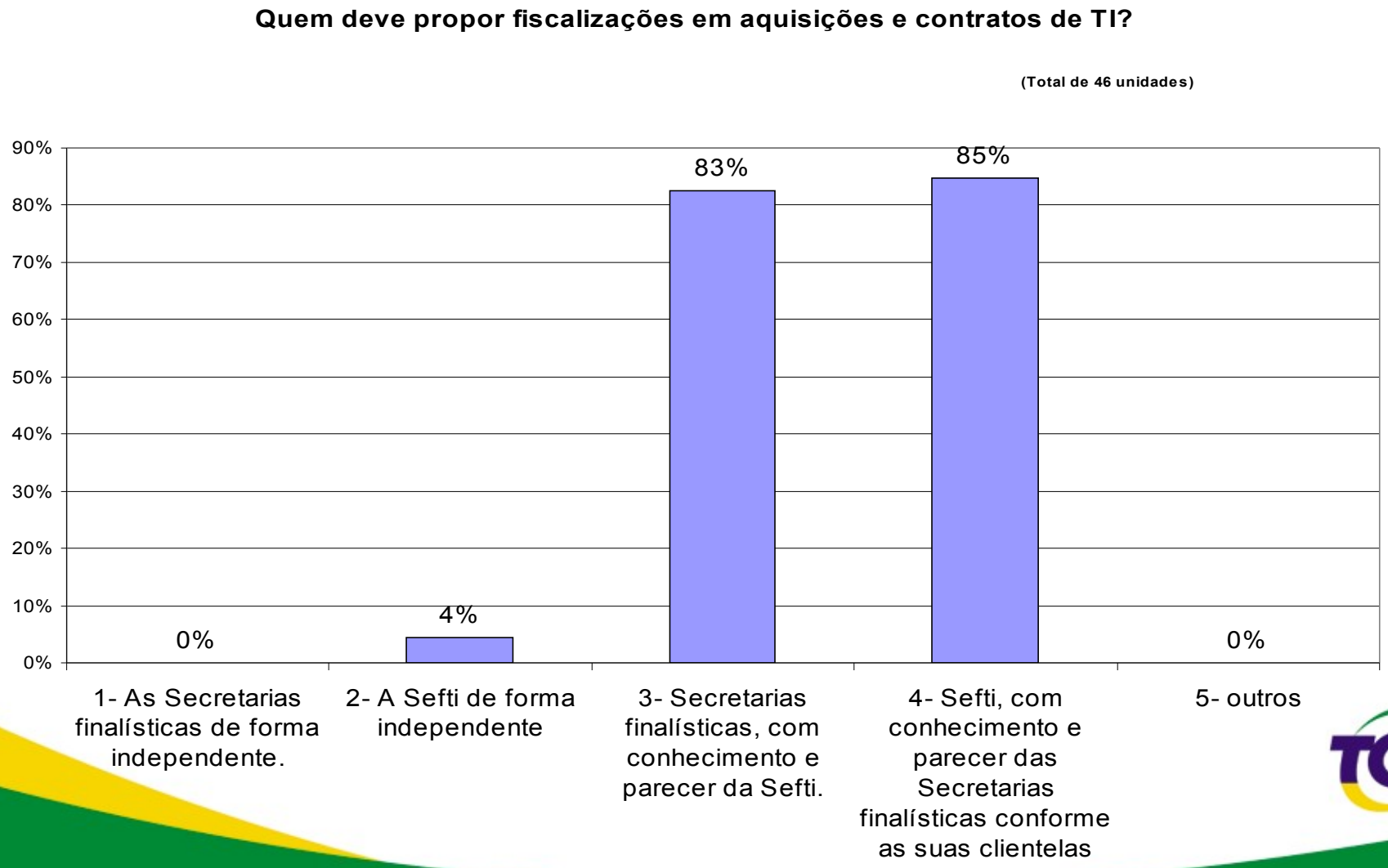
Referencial Estratégico

- **Levantamento** realizado em 2007 que visava, entre outros assuntos:
  - a construção do referencial estratégico da Sefti
  - o conhecimento de boas práticas de fiscalização utilizadas por seus pares internos e externos
- Foram entrevistados internamente
  - 46 unidades, sendo 20 da sede e 26 nos estados
  - 8 gabinetes de ministro

Referencial estratégico



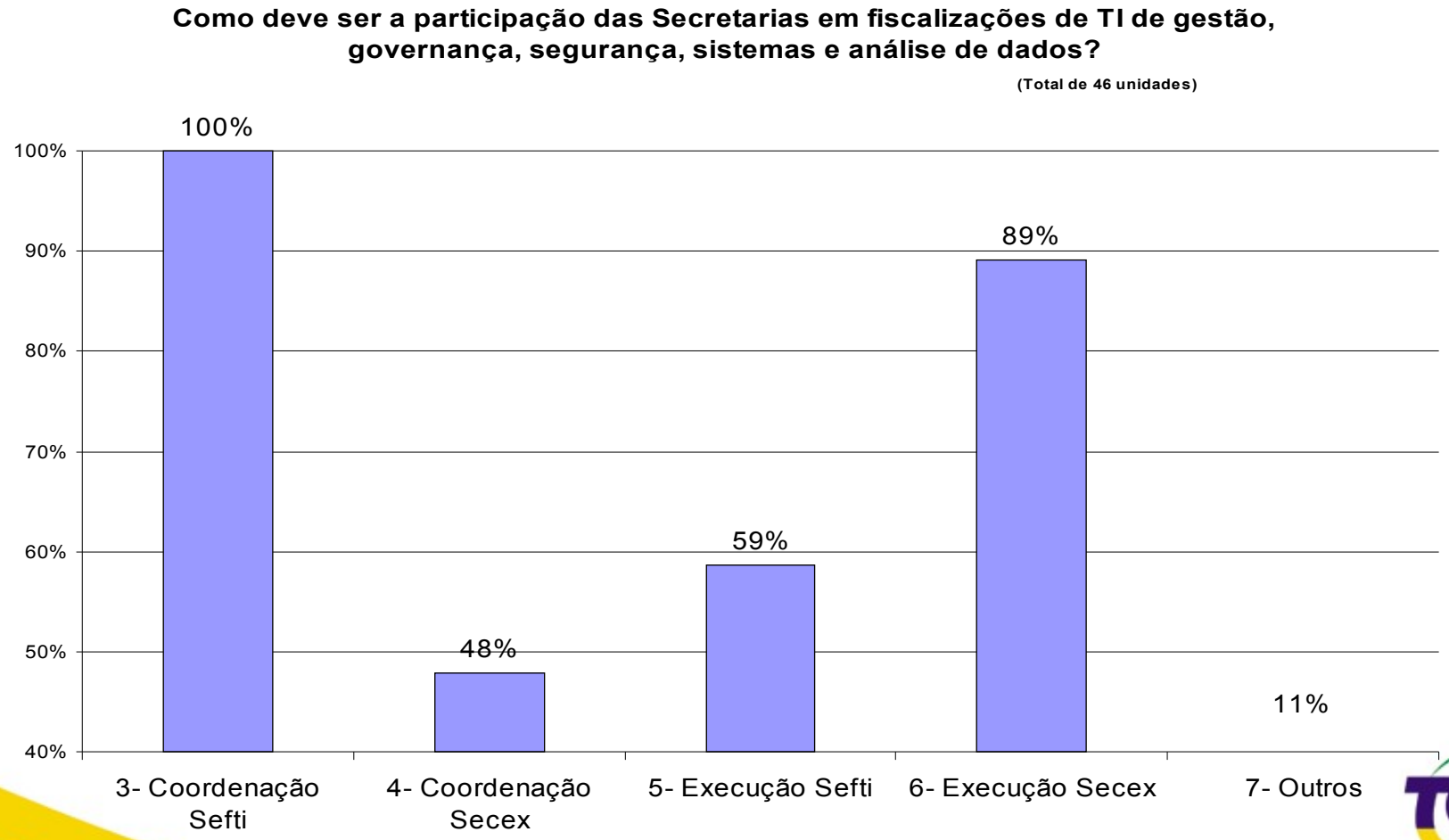
Referencial estratégico



Referencial Estratégico

- ✓ No geral, a opinião dos gabinetes e das unidades técnicas coincidem
- ✓ A **iniciativa para proposição de fiscalizações** de TI deve ser a mais **ampla** possível e negociada caso a caso
- ✓ A Sefti deve **centralizar as informações** dos trabalhos executados na área de TI
- ✓ As Secretarias devem **ser comunicadas** sobre quaisquer fiscalizações que envolvam as suas clientelas

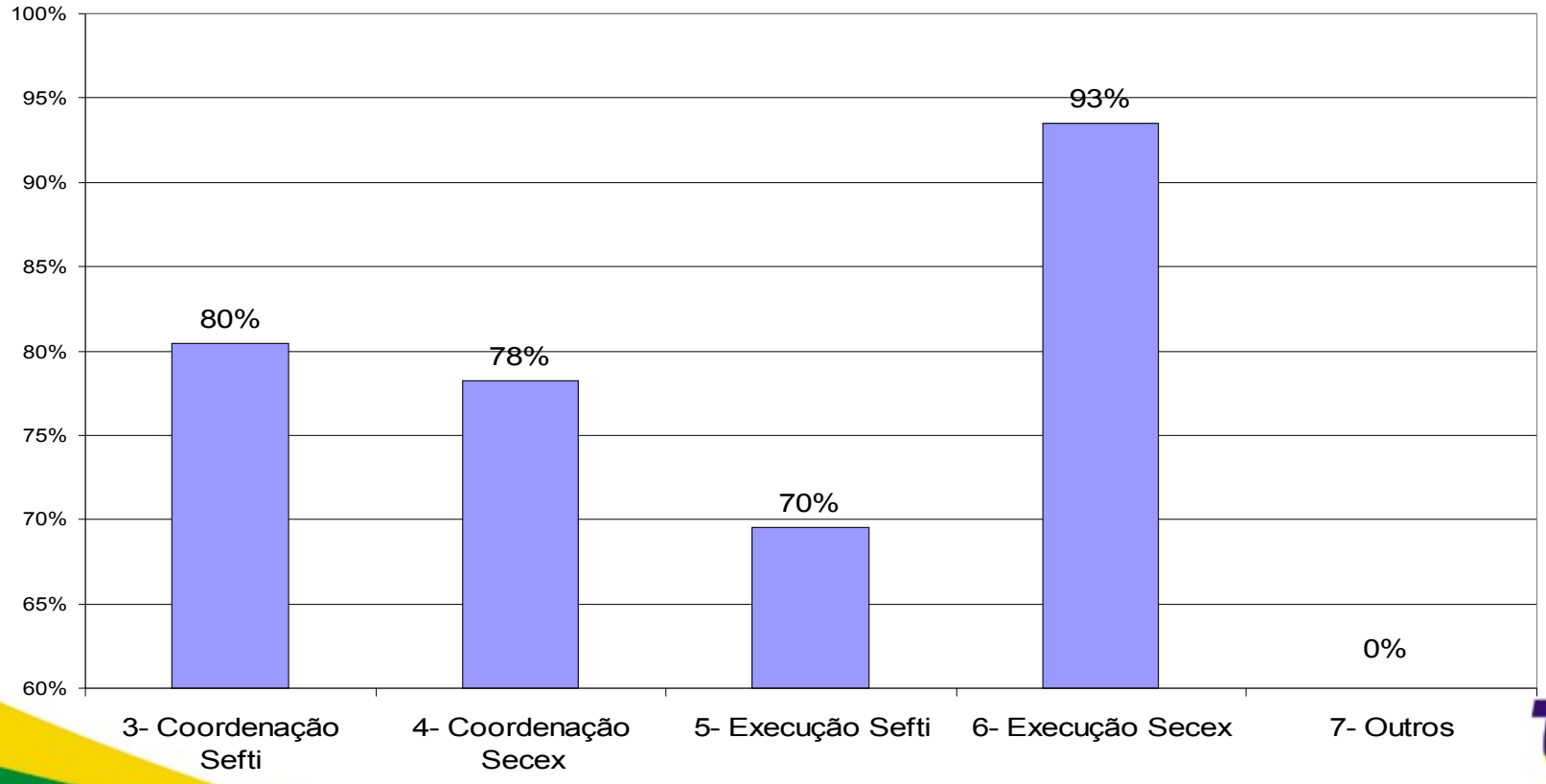
Referencial estratégico



Referencial estratégico

Como deve ser a participação das Secretarias em fiscalizações de aquisições e contratos de TI?

(Total de 46 unidades)



Referencial Estratégico

- Quanto à **instrução inicial** e/ou à análise de mérito de processos que envolvam **contratações de TI**, 41 unidades (89%) concordam que devem ser **feitas na Secretaria de origem**, com **participação formal da Sefti** por meio de pareceres técnicos, quando necessário
- os gabinetes mostraram preocupação com o risco da Secretaria especializar-se apenas na análise de contratações de TI, não sendo capaz de fazer **análise crítica da governança de TI na APF**

Referencial Estratégico

- Quanto à participação da Sefti na instrução de processos:
  - encaminhamento do processo diretamente à Sefti, com **especificação de quesitos** para parecer técnico
  - encaminhamento do processo diretamente à Sefti, **sem quesitos**, em casos de urgência
  - **encaminhamento via relatores** nas situações anteriores, para que possam verificar a necessidade do pedido de encaminhamento e autorizá-lo

Atividades da Sefti 2007-2010

- ✓ Processos (155)
- ✓ Fiscalizações (69)
- ✓ Palestras ministradas (97)
- ✓ Treinamentos ministrados (24)
- ✓ Orientações Formais aos Gestores
  - Cartilha de Boas Práticas em Segurança da Informação - 3ª edição
  - Base de Normas e Jurisprudência de TI www.tcu.gov.br/fiscalizacaoti
  - Notas Técnicas (Termo de Referência e Uso do Pregão)

Principais Atividades em Desenvolvimento na Sefti

- ✓ Guia de Contratação de Soluções de TI
- ✓ Manual de Fiscalização de TI
- ✓ TMS em Sistemas de Gestão das Empresas Estatais
- ✓ Cursos a serem ministrados:
  - Introdução à Auditoria de TI
  - Contratações de TI
  - Controles Gerais de TI
  - Auditoria de Dados

Oportunidades para Sefti

- ✓ Forte necessidade de melhoria da Governança de TI na APF
- ✓ Grande dependência da TI pela APF
- ✓ Materialidade das despesas com TI
- ✓ Critérios para gestão e fiscalização já bem estabelecidos
- ✓ Método de fiscalização testado e aprovado
- ✓ Boa repercussão na APF e sociedade

Riscos para a Sefti

- ✓ Eventual falta de determinado conhecimento específico em assunto tão amplo e complexo
- ✓ Desatualização dos auditores quanto à capacitação técnica
- ✓ Grande quantidade de processos para elaboração de parecer ou instrução de mérito (denúncias, representações)
- ✓ Não incremento proporcional da força de trabalho

Planejamento da Auditoria

Processo de Auditoria

Método de Auditoria do TCU

- ✓ Fases (Levantamento, Planejamento, Execução, Elaboração do Relatório e Monitoramento)
- ✓ Matrizes (Planejamento, Procedimentos e Achados)
- ✓ Técnicas de Auditoria de Conformidade
- ✓ Técnicas de Auditoria Operacional

Matriz de Planejamento

Objetivo: Enunciar de forma clara e resumida o aspecto a ser enfocado pela auditoria, de acordo com o levantamento de auditoria previamente realizado.

Questões de Auditoria	Informações Requeridas	Fontes de Informação	Procedimentos	Detalhamento do Procedimento	Objetos	Membro Responsável	Período	Possíveis Achados
Apresentar, em forma de perguntas, os diferentes aspectos que compõem o escopo da fiscalização e que devem ser investigados com vistas à satisfação do objetivo	Identificar as informações necessárias para responder a questão de auditoria	Identificar as fontes de cada item de informação requerida da coluna anterior. Estas fontes estão relacionadas com as técnicas empregadas	Código ou enunciado do procedimento	Descrever as tarefas que serão realizadas, de forma clara, esclarecendo os aspectos a serem abordados (itens de verificação ou *check list*)	Indicar o documento, o projeto, o programa, o processo, ou o sistema no qual o procedimento será aplicado. Exemplos: contrato, folha de pagamento, base de dados, ata, edital, ficha financeira, processo licitatório, orçamento	Pessoa(s) da equipe encarregada (s) da execução de cada procedimento	Dia(s) em que o Procedimento será executado	Esclarecer precisamente que conclusões ou resultados podem ser alcançados

Questões de Auditoria – Exemplo TMS Gestão e Uso de TI

1. O órgão/entidade executa o **processo de planejamento estratégico institucional** de acordo com as boas práticas?
2. O órgão/entidade executa o **processo de planejamento estratégico de TI** de acordo com as boas práticas?
3. A **organização de TI** do órgão/entidade **é adequada** às atividades a que ele deve dar suporte?

Questões de Auditoria – Exemplo TMS Gestão e Uso de TI

4. O órgão/entidade executa o **processo orçamentário de TI** segundo a legislação e as boas práticas?
5. Há **processo de software estabelecido** no órgão/entidade?
6. Há **processo de gerenciamento de projetos de TI** estabelecido no órgão/entidade?

Questões de Auditoria – Exemplo TMS Gestão e Uso de TI

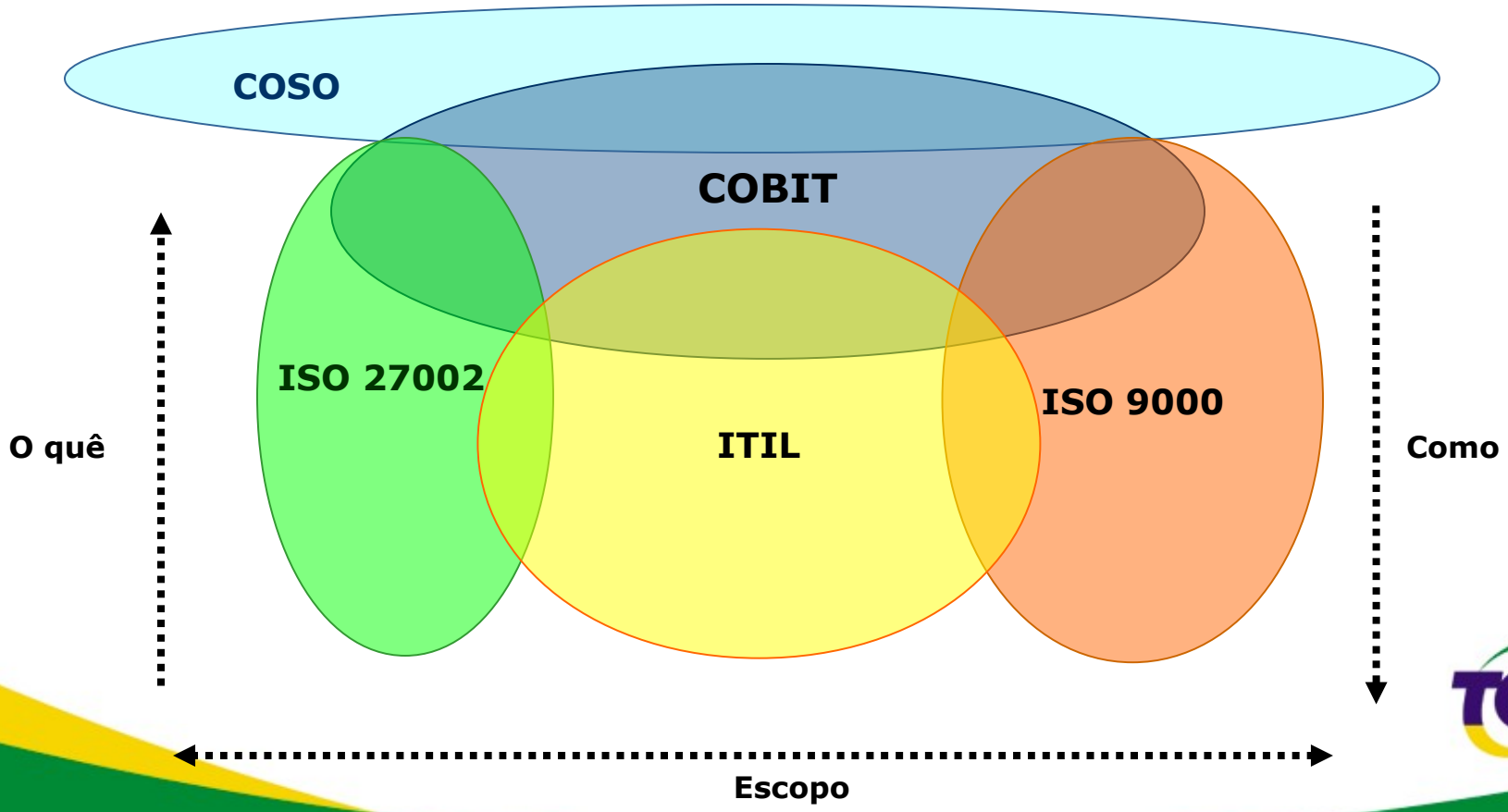
7. Há **processos de gestão de serviços de TI** que apóiem o órgão/entidade na administração da qualidade dos serviços de TI?
8. O órgão/entidade executa os **processos corporativos de segurança da informação** segundo a legislação e as boas práticas?
9. Há **plano de capacitação de profissionais de TI** que auxilie no desenvolvimento das competências necessárias para a boa execução dos trabalhos?

Questões de Auditoria – Exemplo TMS Gestão e Uso de TI

10. O órgão/entidade realiza **monitoração do desempenho da gestão e uso da TI**?
11. O órgão/entidade realiza o **processo de contratação de bens e serviços de TI** segundo as normas vigentes?
12. O órgão/entidade realiza o **processo de gestão de contratos de bens e serviços de TI** segundo as normas vigentes?

Avaliação da Governança de TI

Governança Corporativa e de TI



Avaliação de Governança de TI

- ✓ **Levantar** informações para elaboração de mapa com a **situação da Governança de TI** na Administração Pública Federal com vistas a subsidiar o planejamento das fiscalizações da Sefti
- ✓ Verificar onde a **situação** da Governança de TI está mais **crítica**
- ✓ Identificar as áreas **onde o TCU pode atuar como indutor** do processo de aperfeiçoamento da **Governança de TI**
- ✓ Identificar os **principais sistemas e bases de dados** da Administração Pública Federal

Levantamento de Governança de TI em 2007

- ✓ Questionário de **39 questões**
- ✓ **255 órgãos/entidades** da APF
- ✓ **respostas declarativas, com anexação de evidências**
- ✓ Acórdão nº 1.603/2008 – Plenário

Acórdão nº 1.603/2008-Plenário

- ✓ Recomendações ao:
- ✓ CNJ
- ✓ CNMP
- ✓ Senado Federal
- ✓ Câmara dos Deputados
- ✓ TCU
- ✓ MP (especialmente SLTI)
- ✓ GSI/PR
- ✓ CGU

Acórdão nº 1.603/2008-Plenário

- ✓ promovam ações com o objetivo de **disseminar a importância do planejamento estratégico**, procedendo ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, **planejamento estratégico de TI** e comitê diretivo de TI;
- ✓ adotem providências com vistas a garantir que as **propostas orçamentárias** para a área de TI sejam elaboradas com base nas atividades que efetivamente pretendam realizar e **alinhadas aos objetivos do negócio**;

Acórdão nº 1.603/2008-Plenário

- ✓ envidem esforços visando à implementação de **processo de trabalho formalizado de contratação de bens e serviços de TI**, bem como de gestão de contratos de TI, buscando a uniformização de procedimentos nos moldes recomendados no item 9.4 do Acórdão 786/2006-TCU-Plenário;
- ✓ atentem para a necessidade de dotar a **estrutura de pessoal de TI** do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor;

Acórdão nº 1.603/2008-Plenário

- ✓ orientem sobre a importância do **gerenciamento da segurança da informação**, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a **gestão da continuidade do negócio**, a gestão de mudanças, a gestão de capacidade, a **classificação da informação**, a gerência de incidentes, a **análise de riscos de TI**, a área específica para gerenciamento da segurança da informação, a **política de segurança da informação** e os procedimentos de controle de acesso;

Acórdão nº 1.603/2008-Plenário

- ✓ estimulem a adoção de **metodologia de desenvolvimento de sistemas**, procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança;
- ✓ promovam ações voltadas à implantação e/ou aperfeiçoamento de **gestão de níveis de serviço de TI**;
- ✓ introduzam práticas voltadas à realização de **auditorias de TI**, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados;

Levantamento de Governança de TI em 2010

- ✓ Acórdão nº 1.603/2008-Plenário
  - *"...determinar à Sefti que ... organize outros levantamentos com o intuito de acompanhar e manter base de dados atualizada com a situação de governança de TI na APF"*

- ✓ TMS Gestão e Uso de TI (2010)

Questionário de 2010

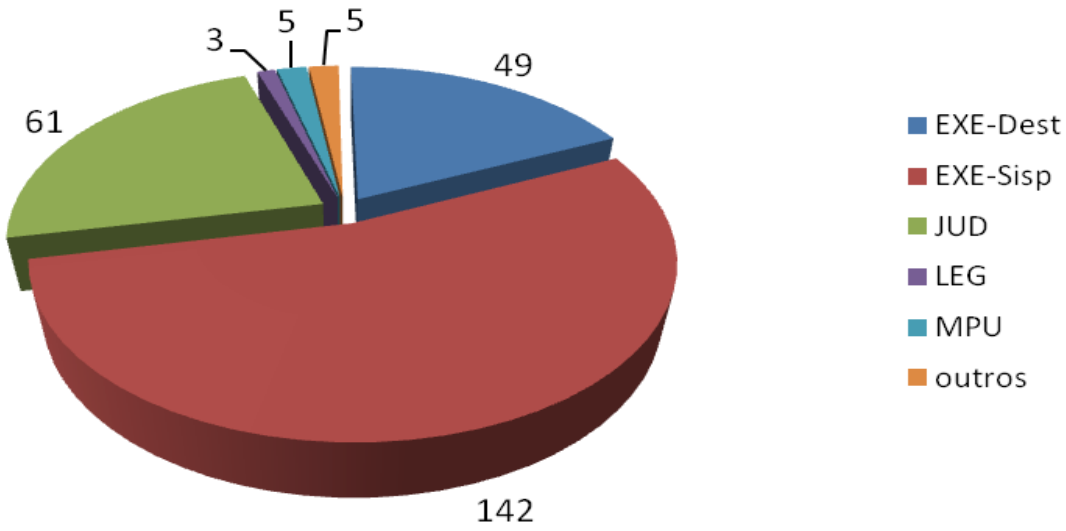
- ✓ 30 questões – 152 itens
- ✓ Dividido segundo 7 dimensões do Gespública
  - Liderança
  - Estratégias e planos
  - Cidadãos
  - Sociedade
  - Informações e conhecimento
  - Pessoas
  - Processos

Critérios Utilizados

- ✓ Acórdão nº 1.603/2008-TCU-Plenário
- ✓ Legislação
- ✓ Códigos de melhores práticas internacionais
  - ◆ Cobit, ITIL
- ✓ Normas ABNT
  - ◆ ABNT NBR ISO/IEC 20.000
  - ◆ ABNT NBR ISO/IEC 27.002
  - ◆ ABNT NBR ISO/IEC 38.500

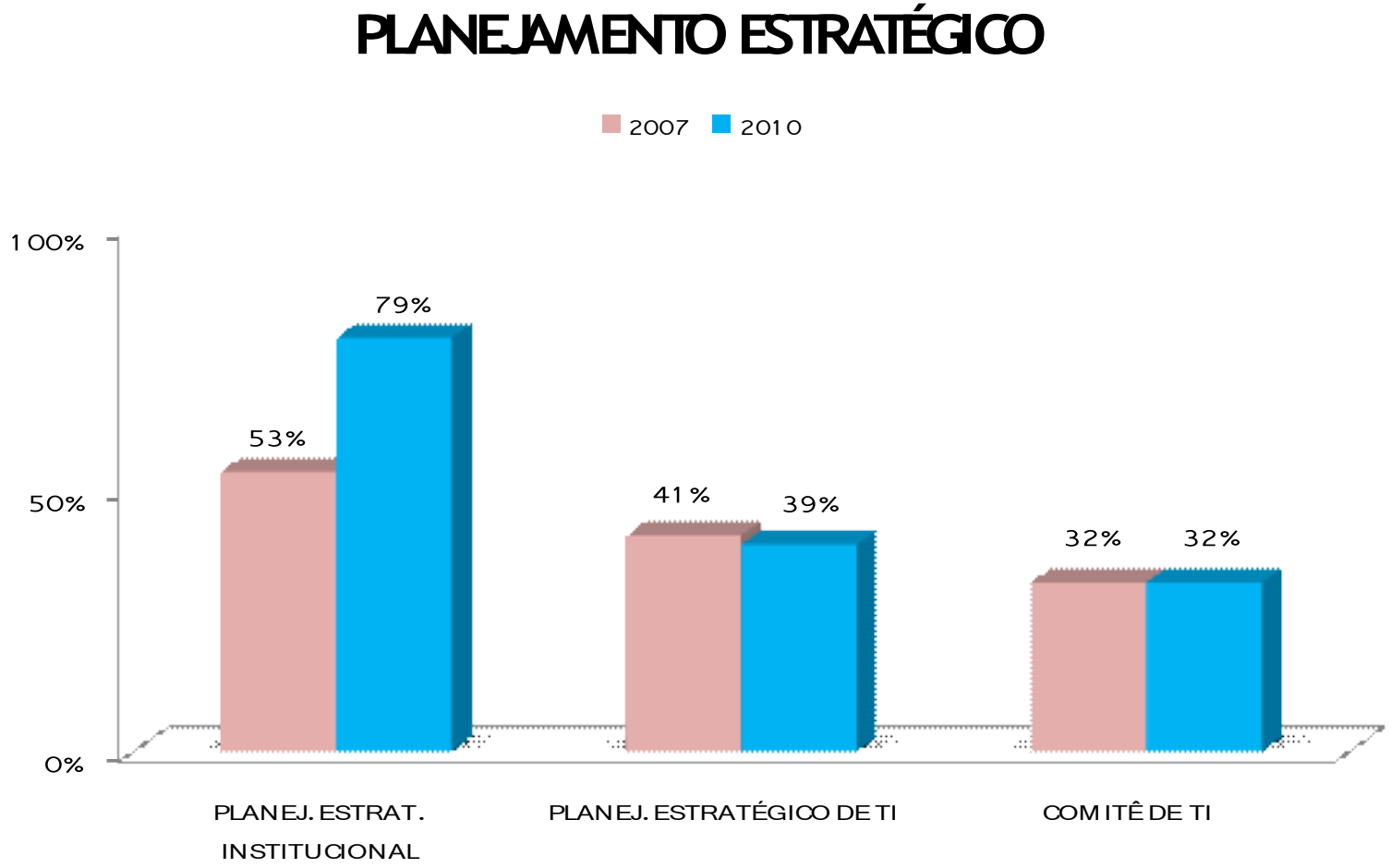
Público alvo

- ✓ 265 de 315 instituições responderam (84%)
- ✓ Respondentes por segmento:

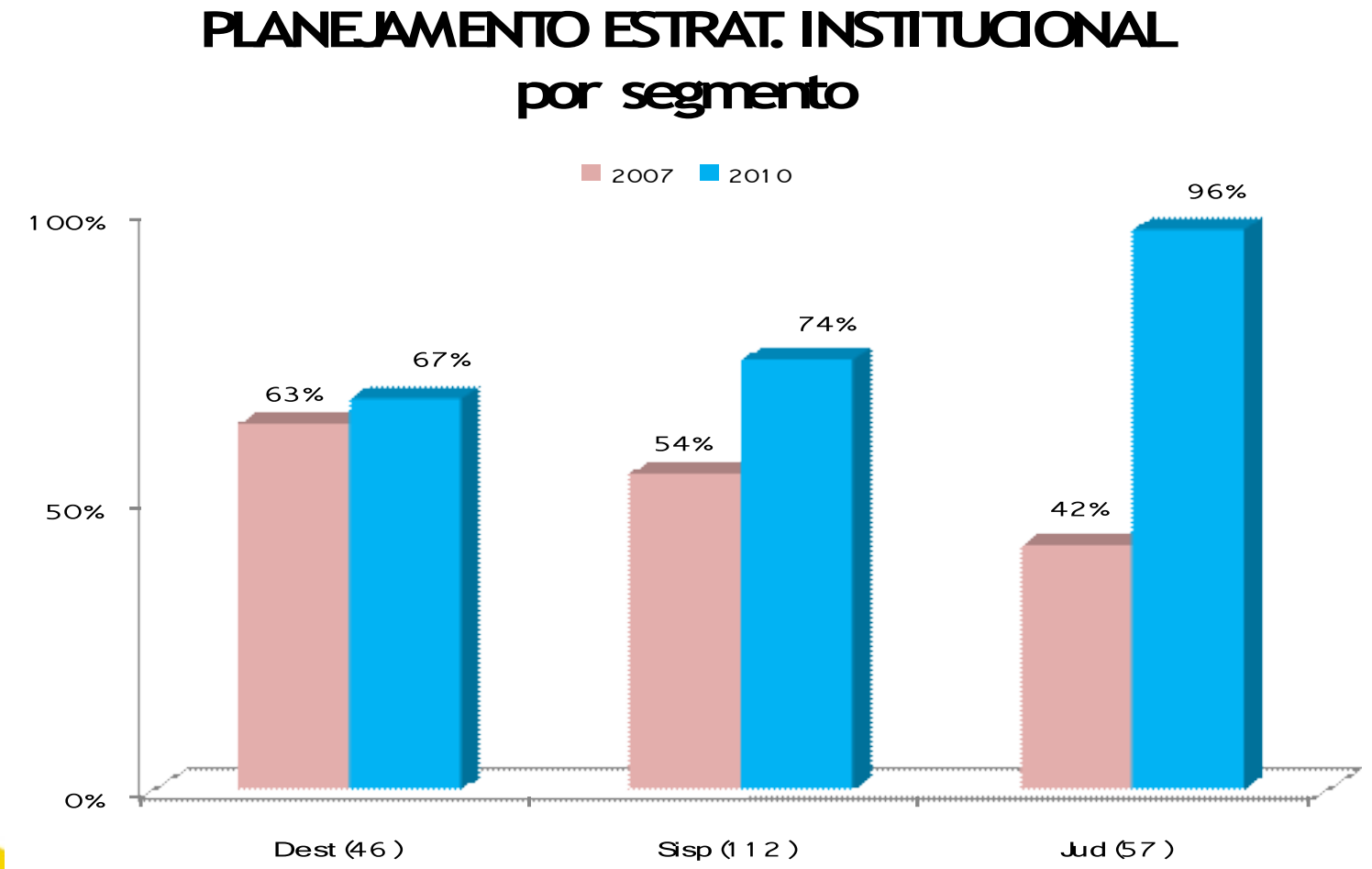


- ✓ 223 responderam os dois levantamentos (de 2007 e de 2010)

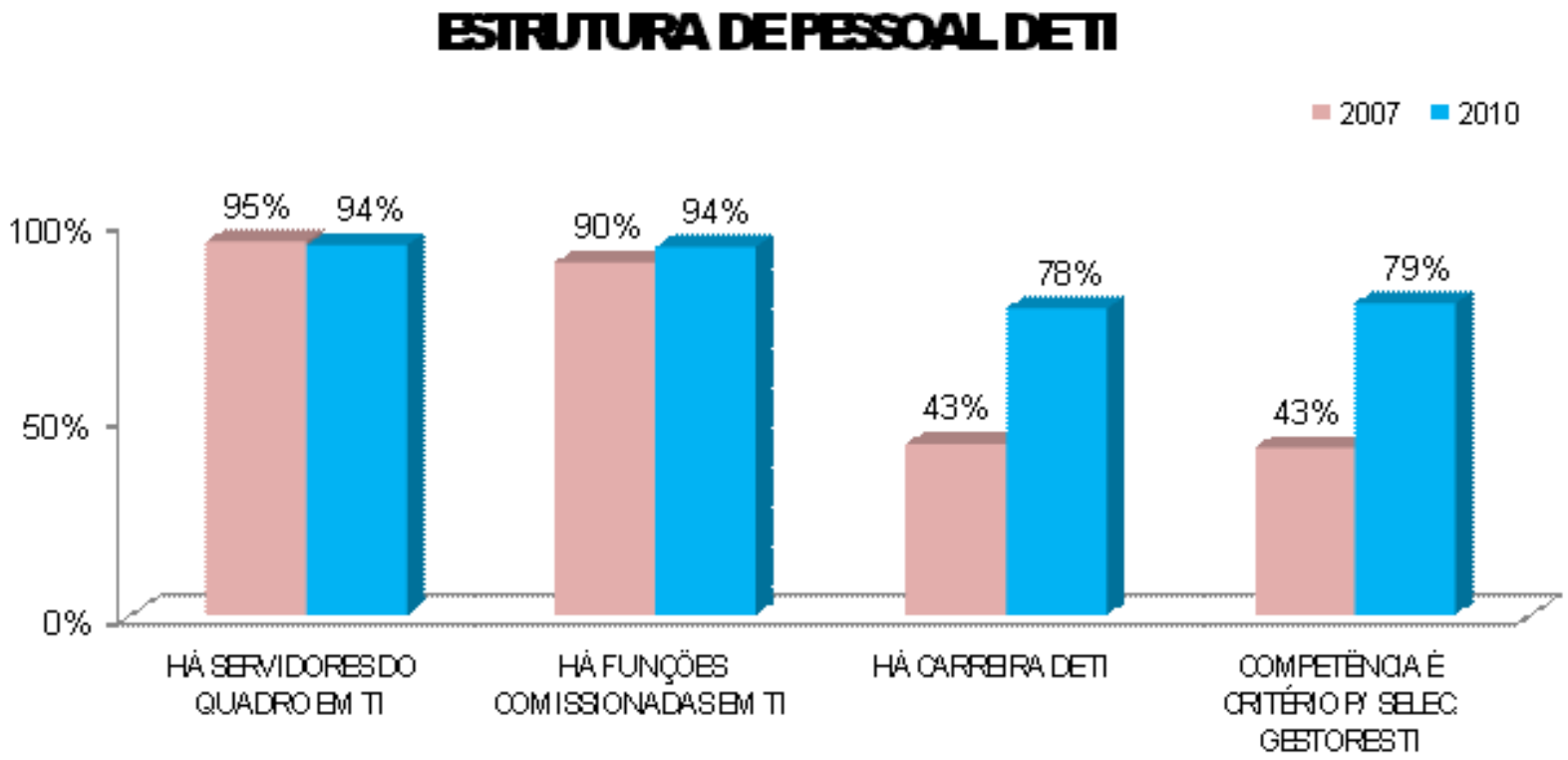
Comparação 2007 x 2010



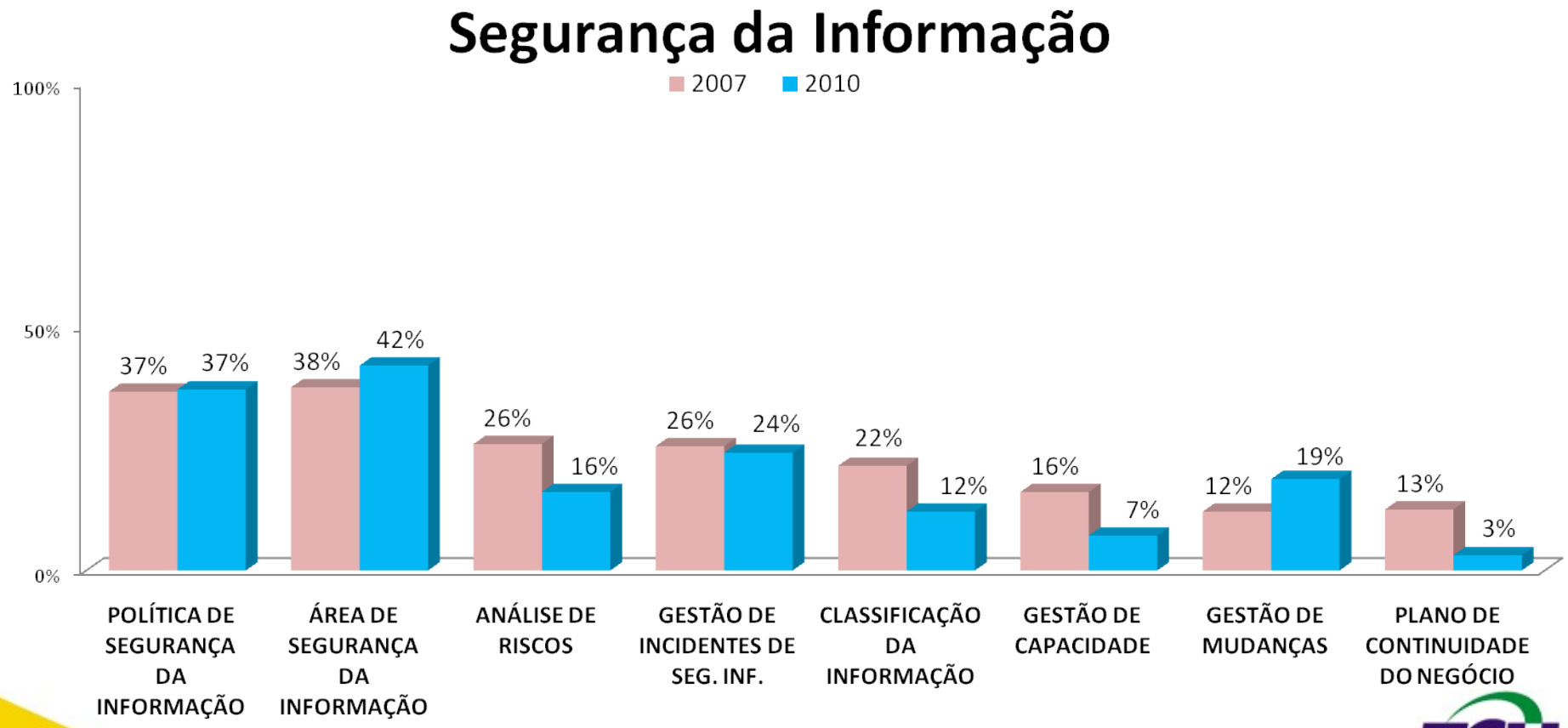
Comparação 2007 x 2010



Comparação 2007 x 2010

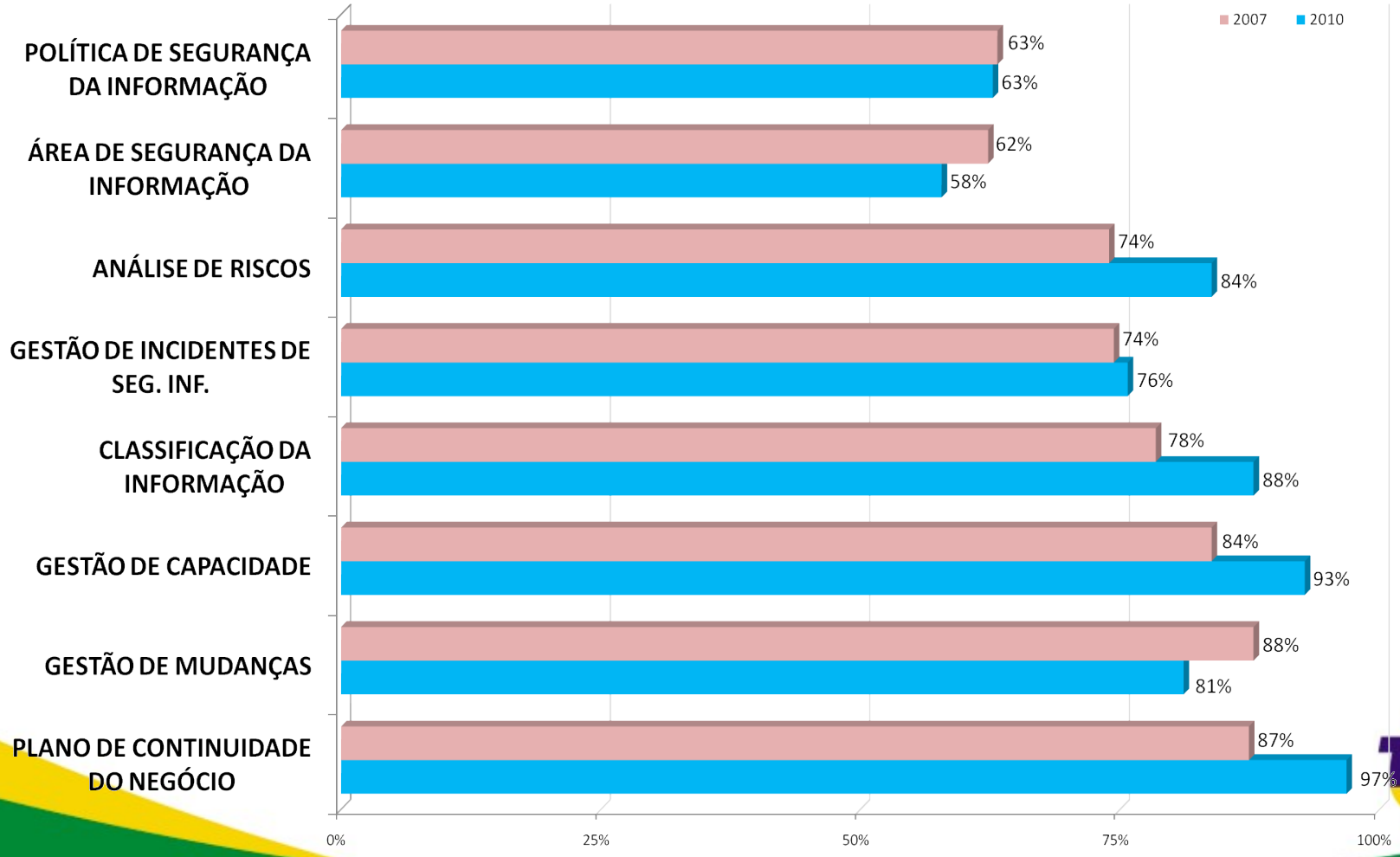


Comparação 2007 x 2010

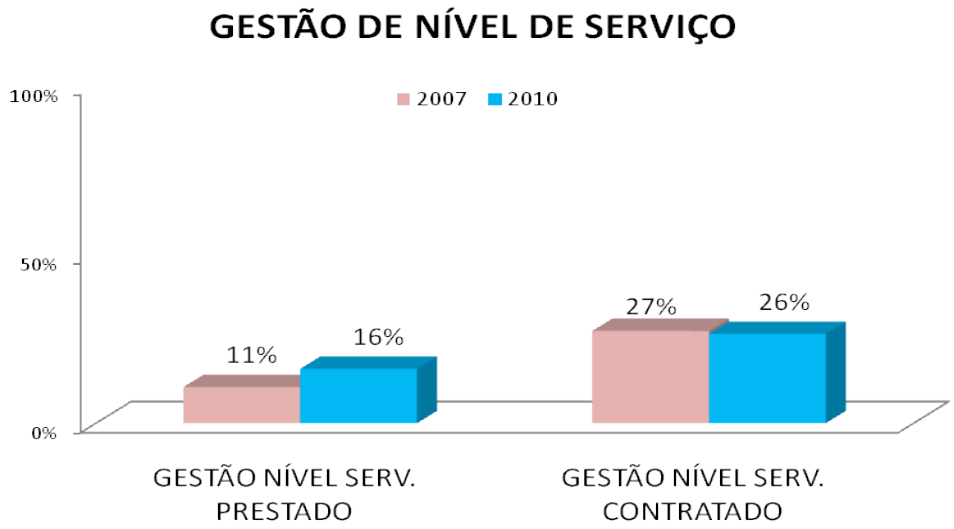


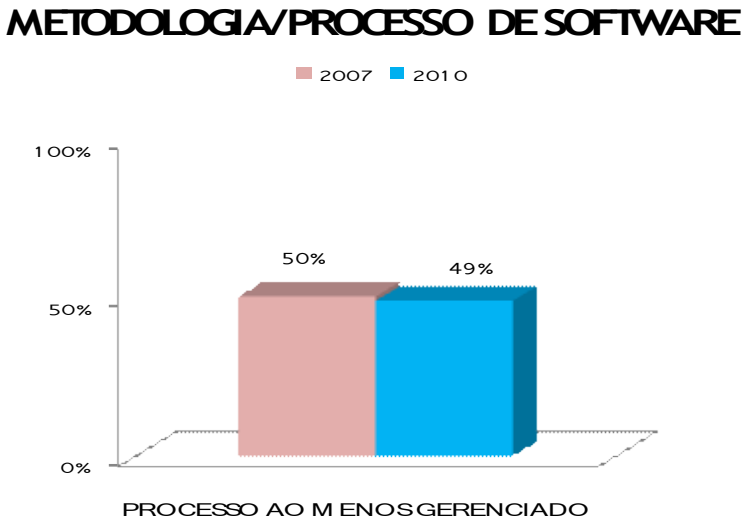
Comparação 2007 x 2010

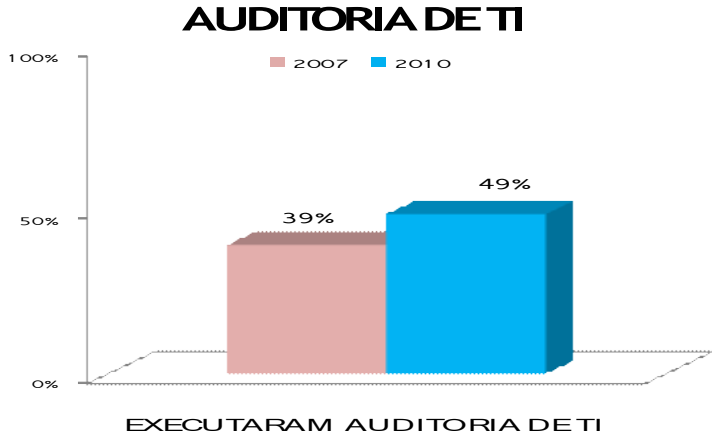
DEFICIÊNCIAS EM SEGURANÇA DA INFORMAÇÃO



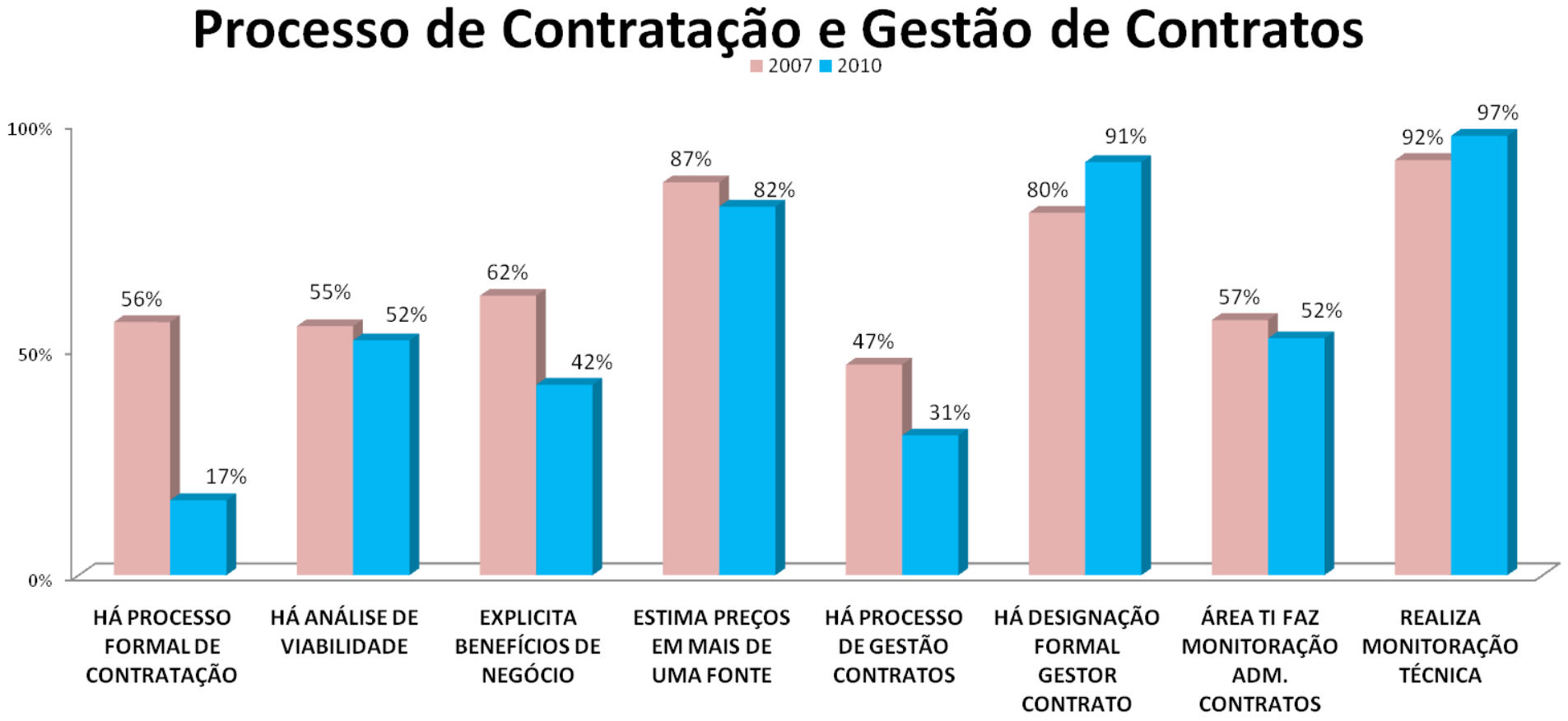
Comparação 2007 x 2010



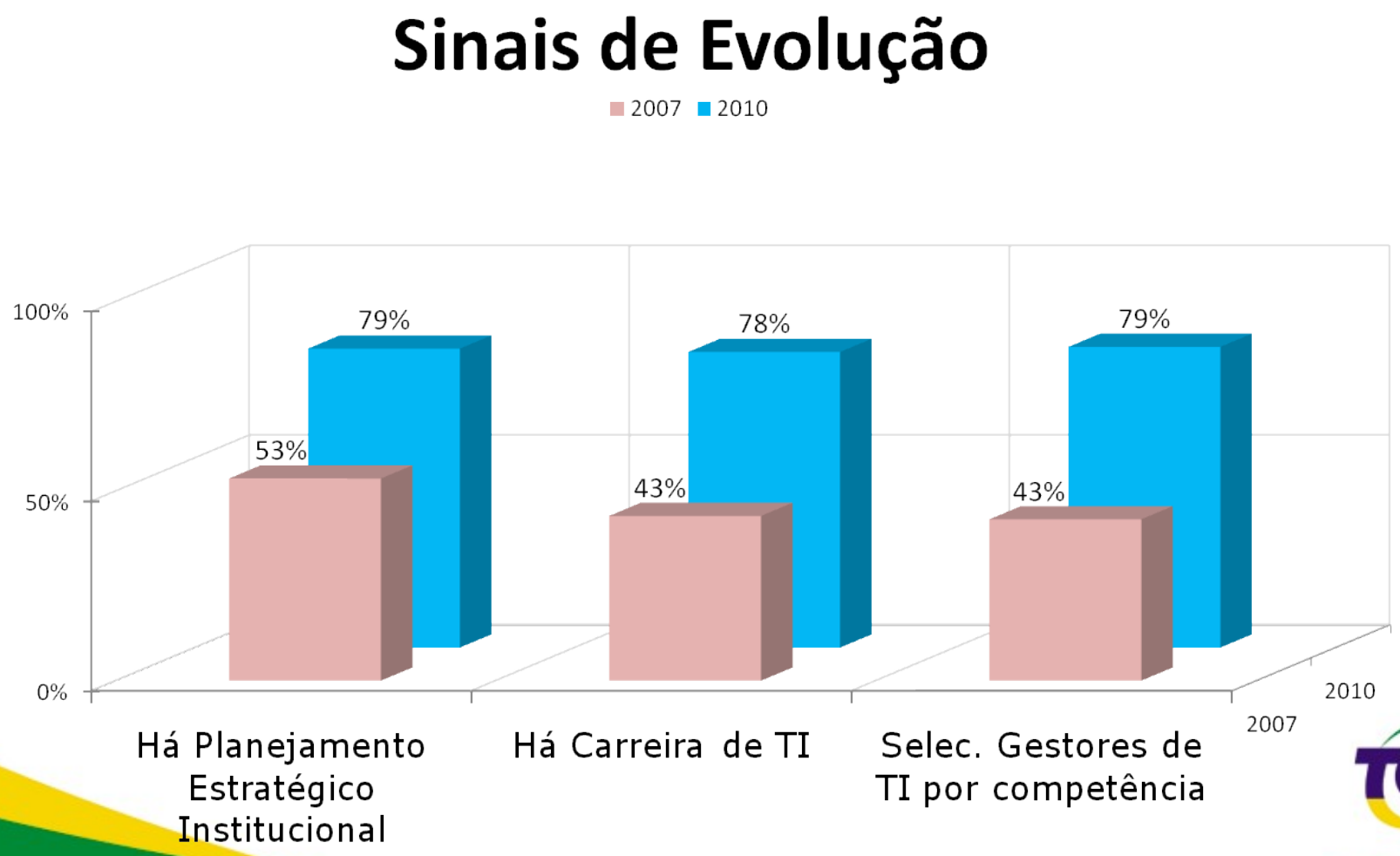




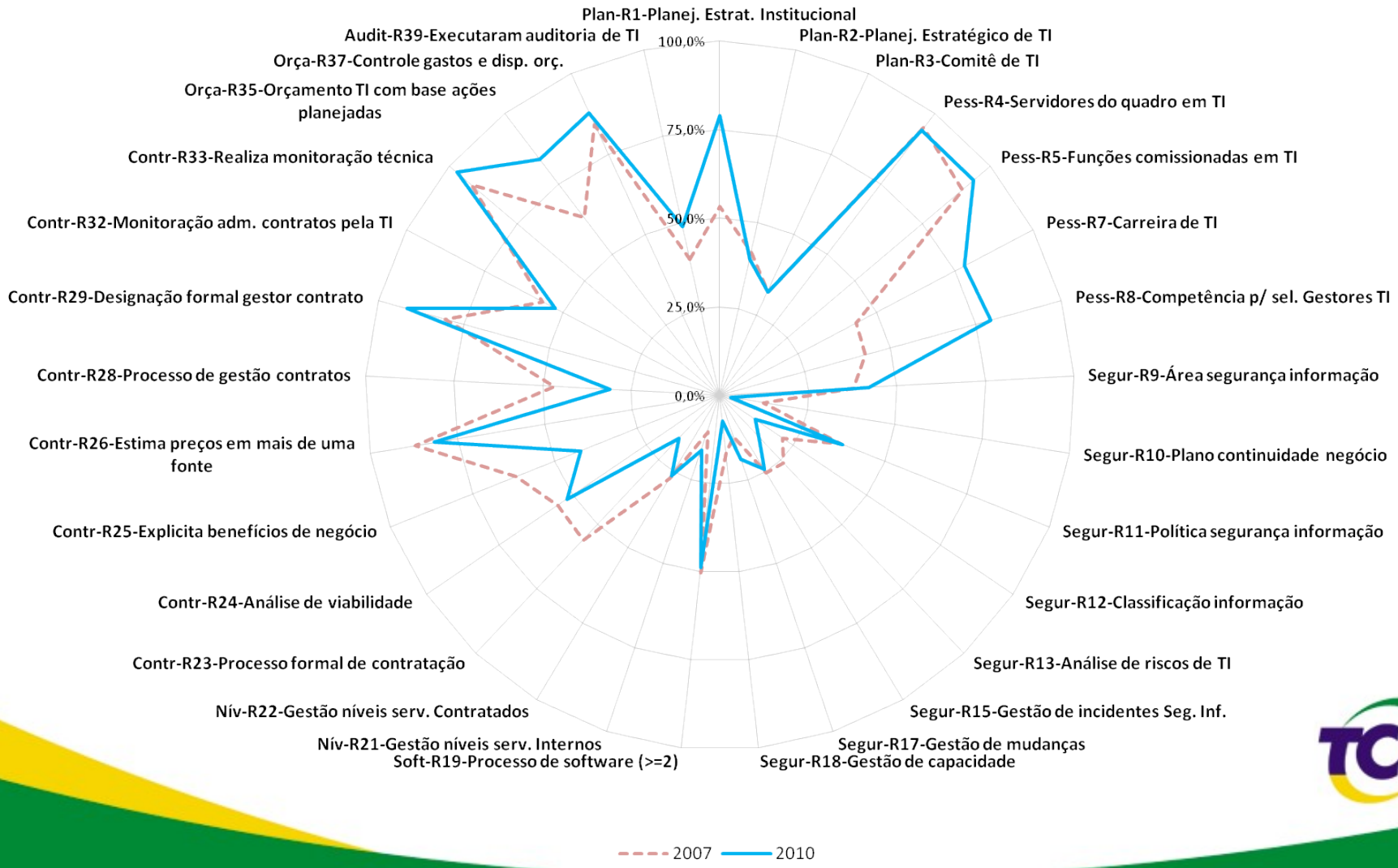
Comparação 2007 x 2010



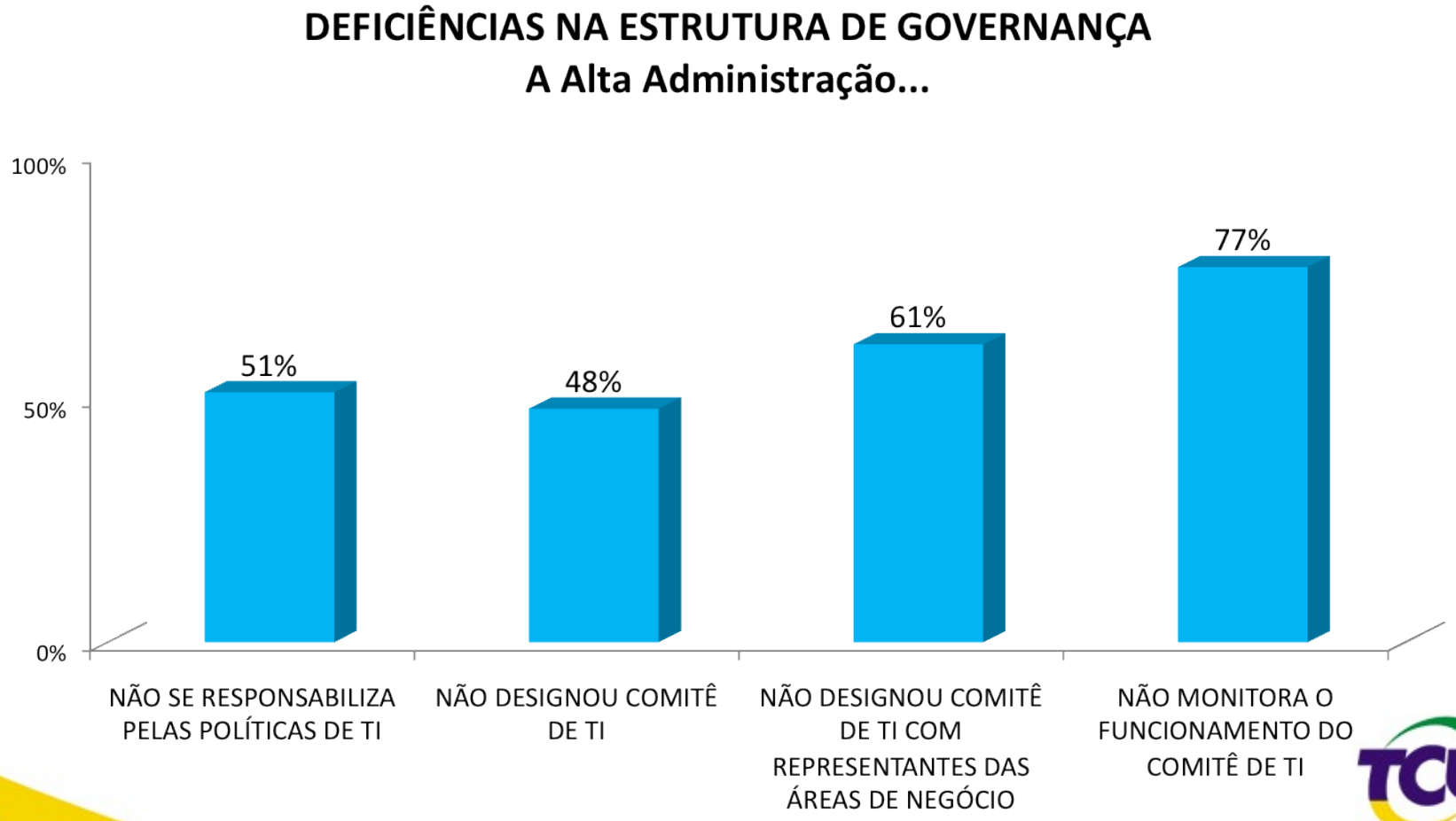
Comparação 2007 x 2010



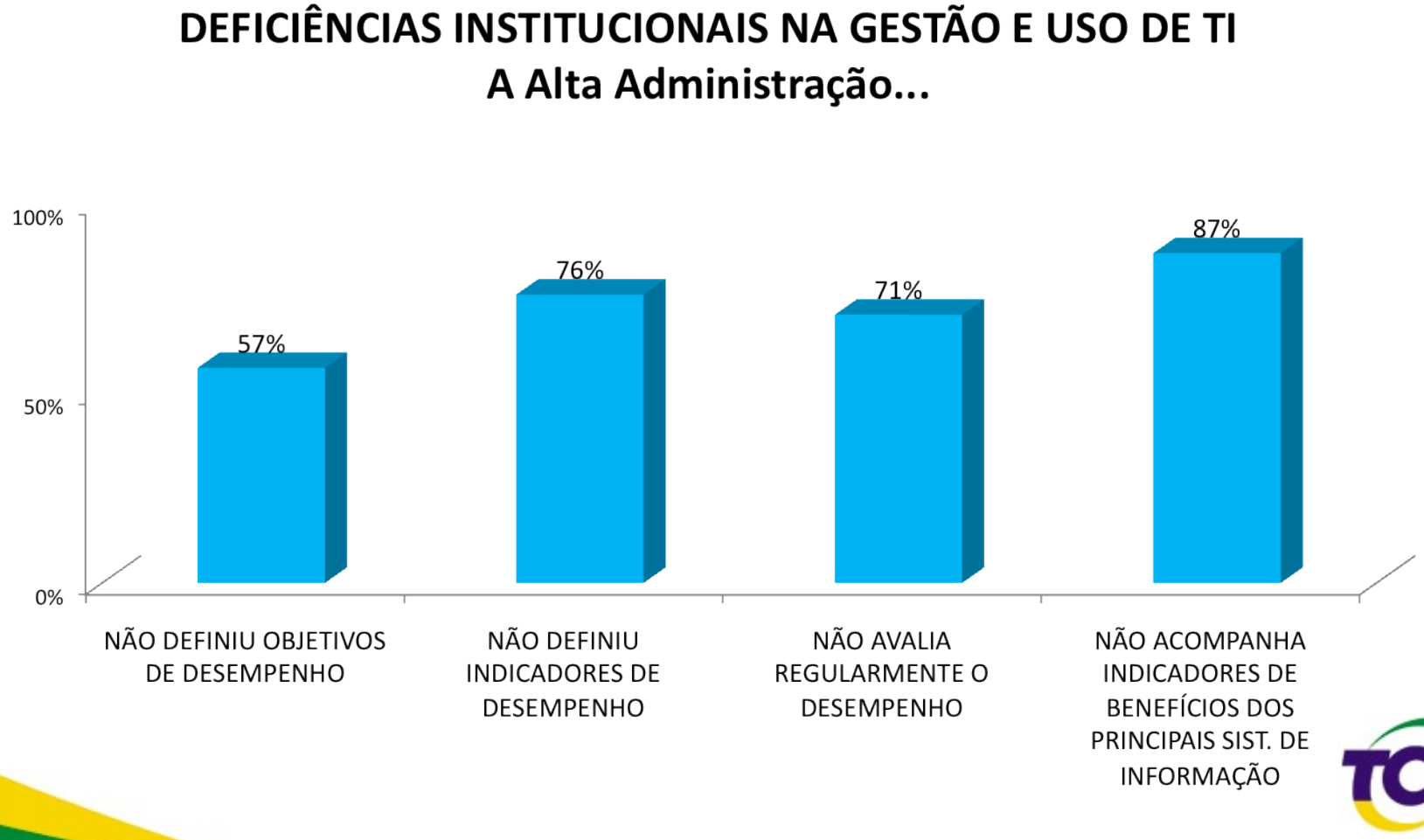
Radar - Comparativo 2007/2010



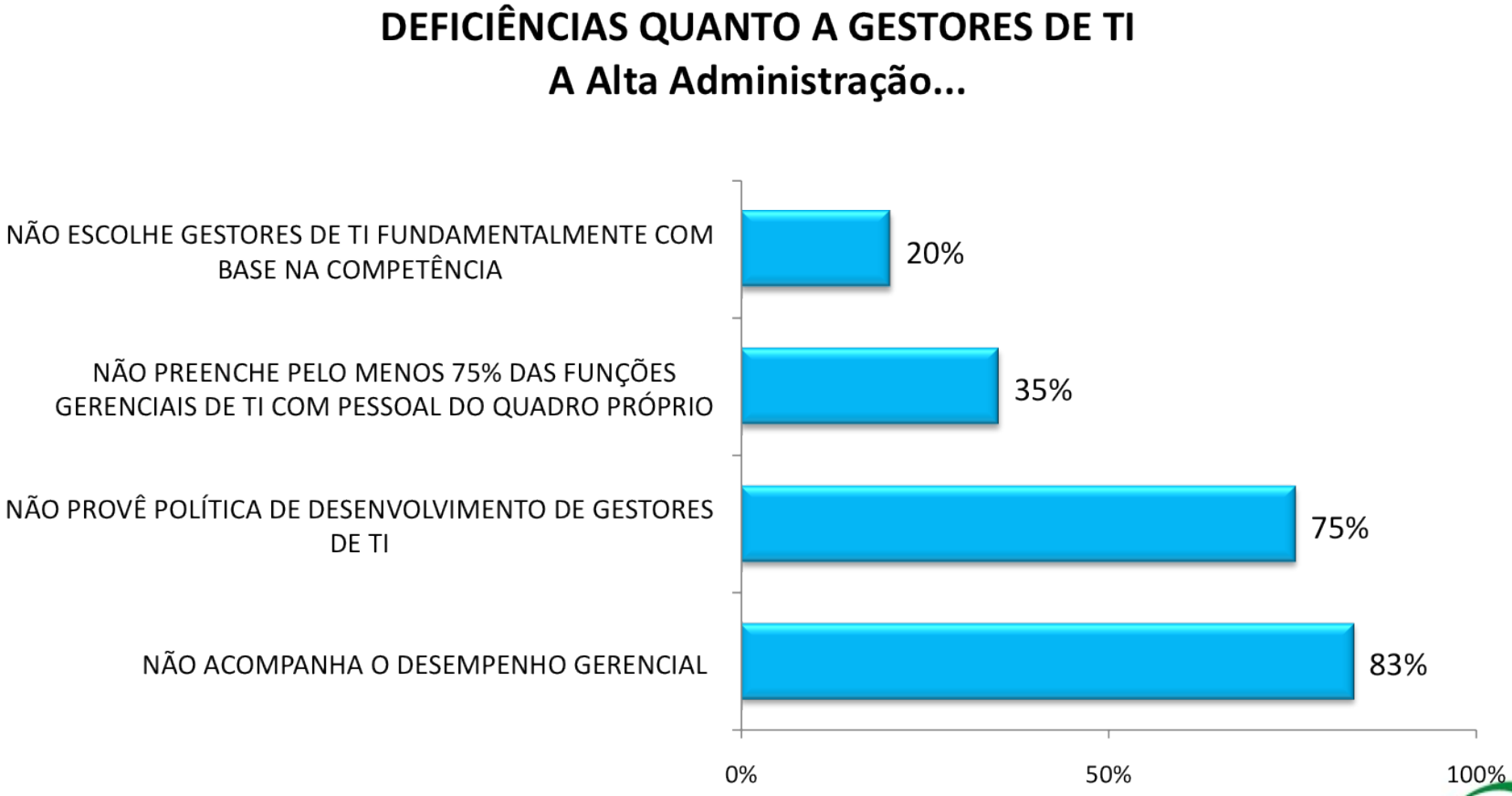
Principais Achados



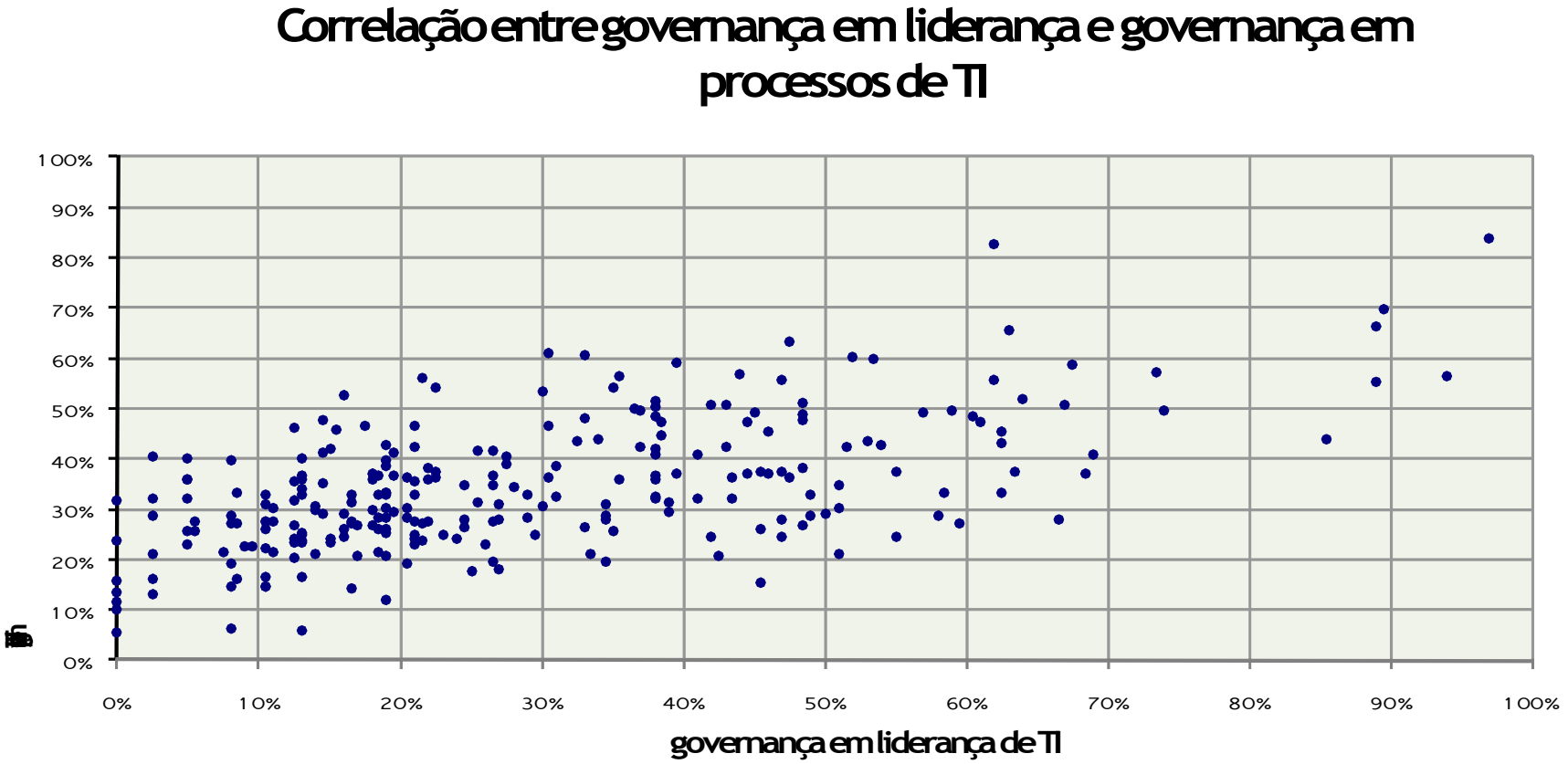
Principais Achados



Principais Achados



Principais Achados



Índice de Governança de TI iGovTI 2010

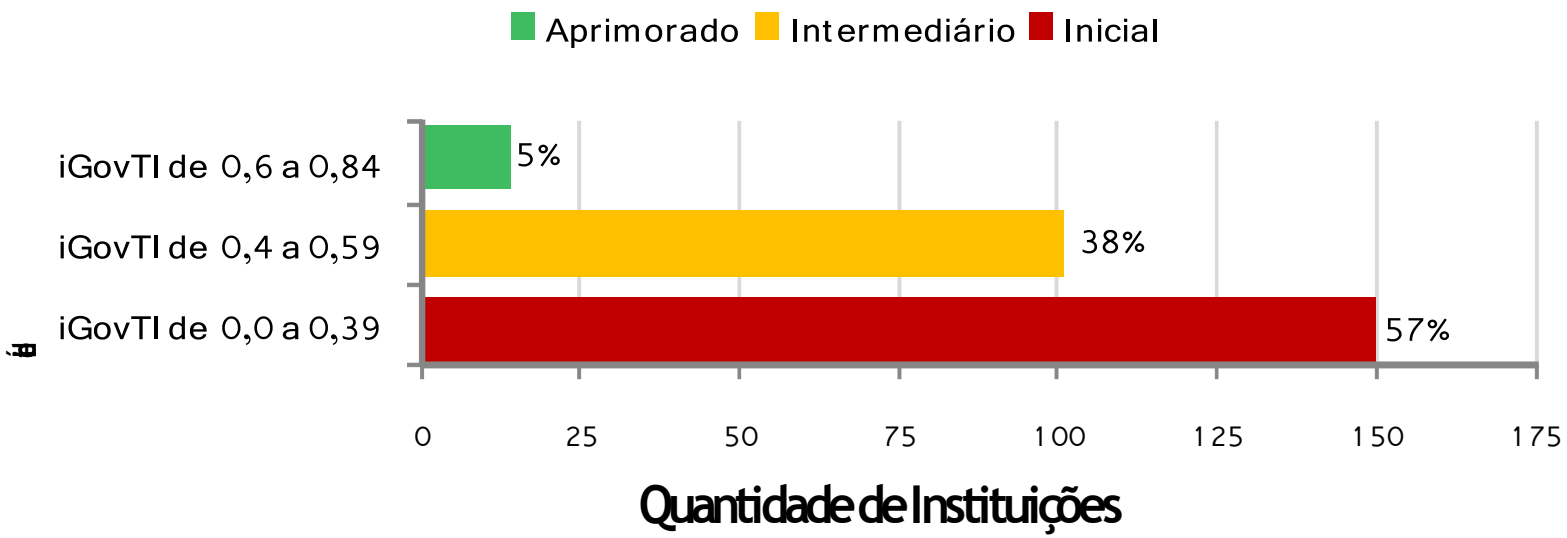
- ✓ iGovTI
  - Métrica de governança de TI criada pela Sefti
  - Calculado sobre as respostas 2010
- ✓ Critérios
  - Cobit 4.1
  - Gespública
  - Acórdão nº 1.603/2008-TCU-Plenário

Índice de Governança de TI iGovTI 2010

- iGovTI – Estágios
  - Inicial = índice abaixo de 40%
  - Intermediário = índice de 40 a 59%
  - Aprimorado = índice a partir de 60%

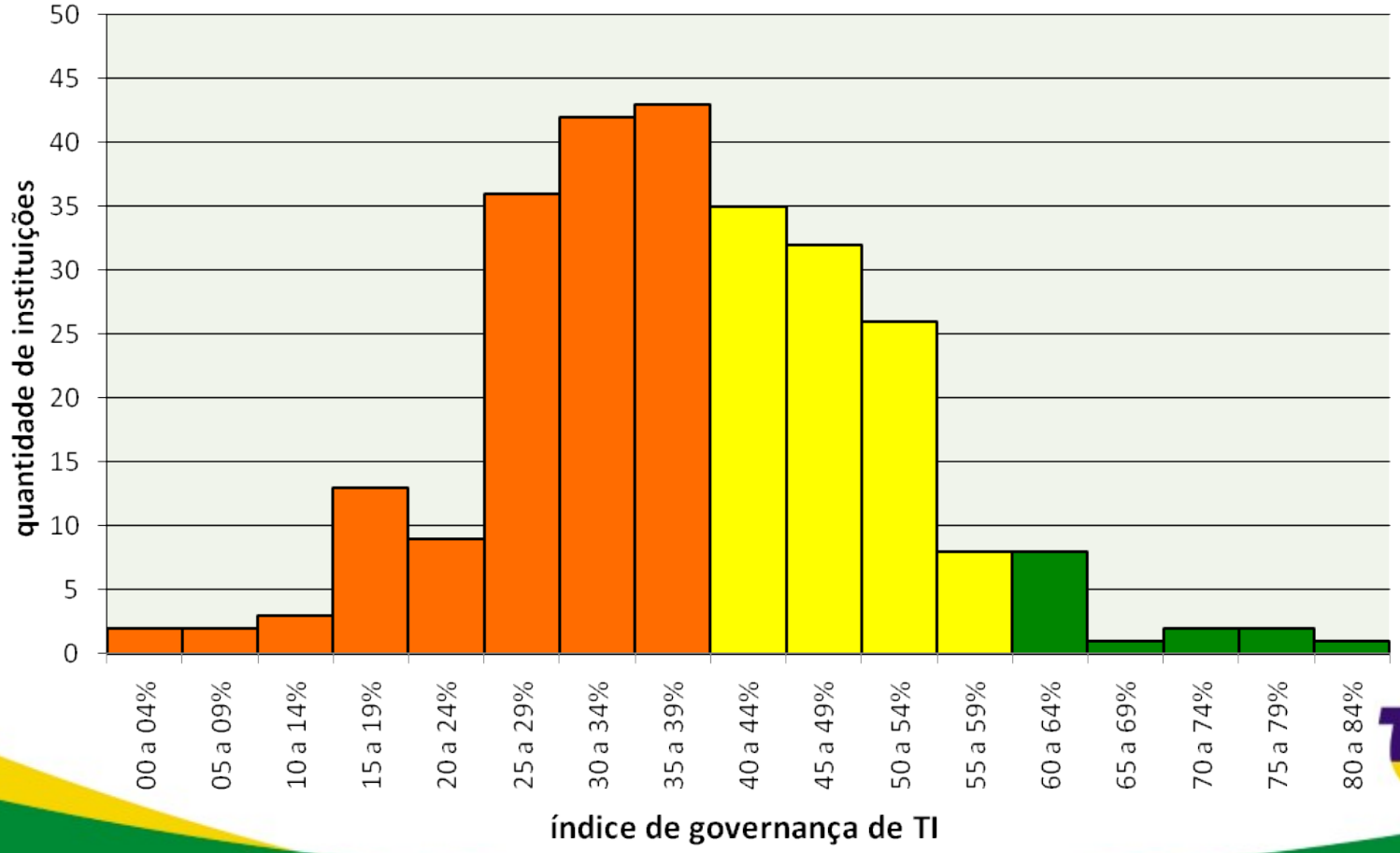
Índice de Governança de TI iGovTI 2010

Instituições x Estágios do iGovTI

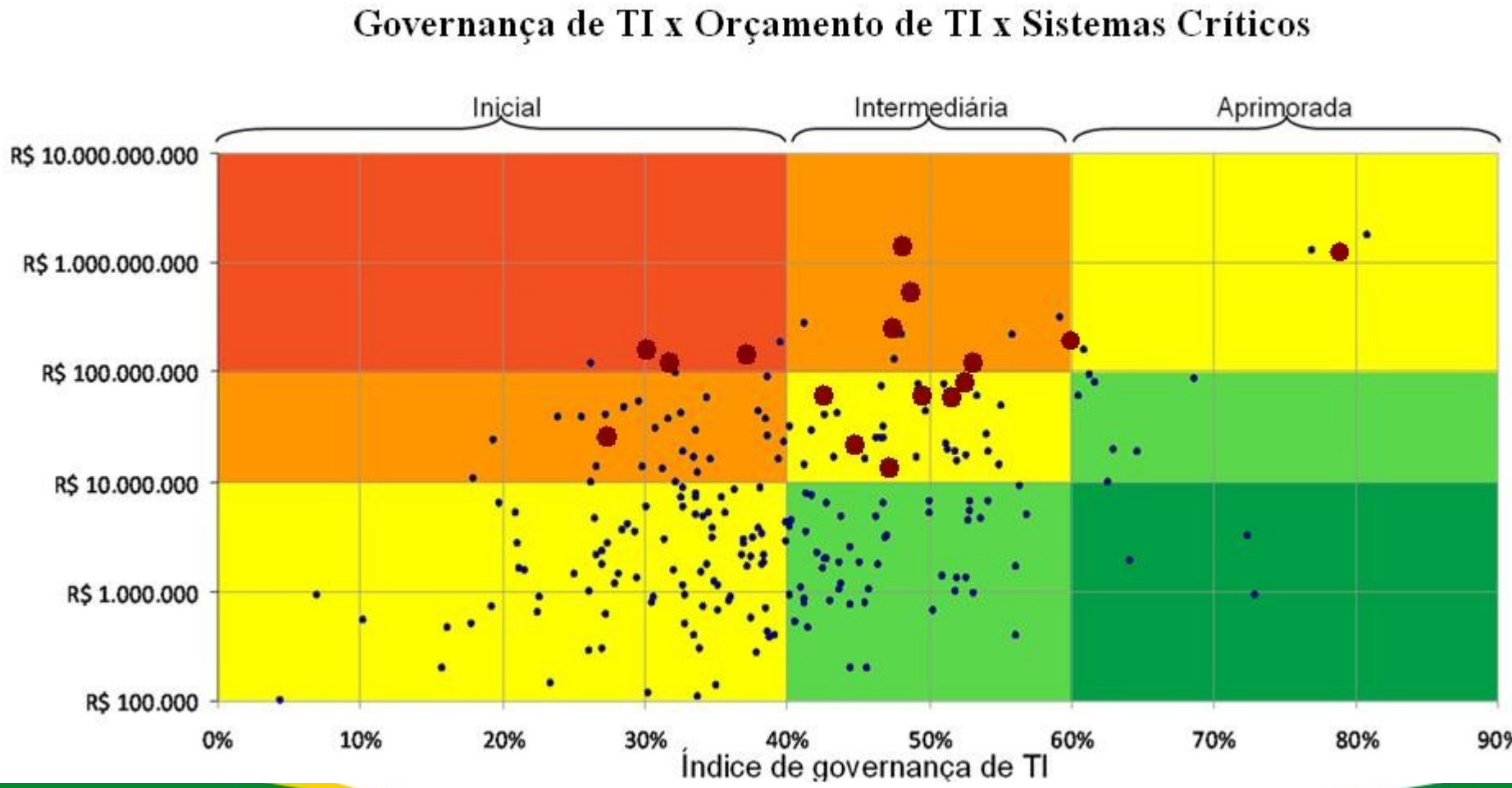


Índice de Governança de TI iGovTI 2010

Distribuição das Instituições



Índice de Governança de TI iGovTI 2010



Obs: As cores indicam risco

Acórdão nº 2.308/2010-Plenário

Recomendar aos Órgãos Superiores:

a) **orientar** as instituições sob sua jurisdição sobre a necessidade de a respectiva **alta administração** estabelecer formalmente:

   i. objetivos institucionais de TI alinhados às estratégias de negócio
   ii. indicadores para cada objetivo
   iii. metas para cada indicador
   iv. mecanismos que a alta administração adotará para acompanhar o desempenho da TI da instituição

b) promover, mediante **orientação normativa**, a obrigatoriedade de a **alta administração** de cada instituição sob sua jurisdição estabelecer os itens citados

Acórdão nº 2.308/2010-Plenário

Determinar à Sefti:

a) **monitore** a adoção das providências recomendadas;

b) **continue a monitorar** o cumprimento das providências recomendadas no **Acórdão nº 1.603/2008 –TCU–Plenário**;

c) desenvolva ações de **estímulo à conscientização da alta administração** das unidades da APF acerca de conceitos, objetivos, indicadores, ações e estruturas de governança de tecnologia da informação;

Acórdão nº 2.308/2010-Plenário

Determinar à Sefti:

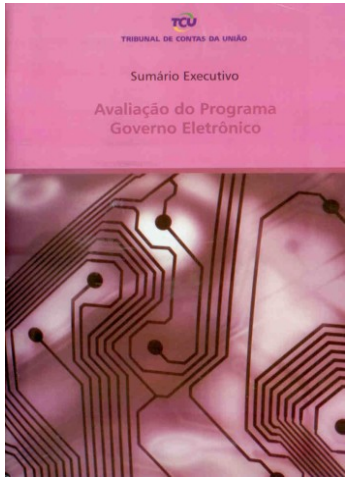
d) defina e mantenha processo de trabalho permanente e sustentável de acompanhamento da governança de TI na APF, com fins de:
   - subsidiar processos de fiscalização do TCU em TI;
   - subsidiar processos de planejamento e controle das unidades jurisdicionadas;

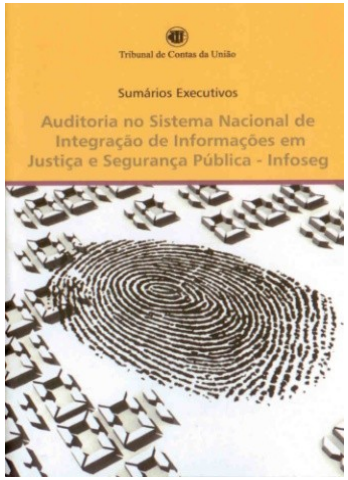
d) realize levantamentos regulares com coleta de evidências;

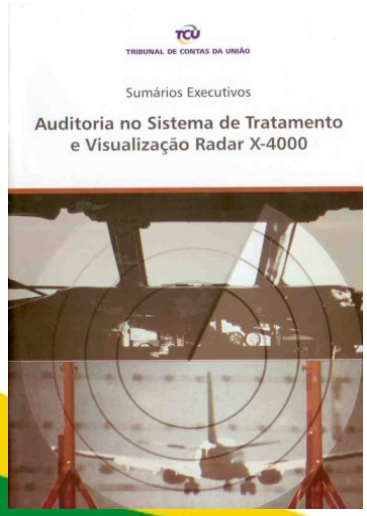
e) dê publicidade ao levantamento:
   - feedback aos participantes;
   - divulgação das informações consolidadas;
   - divulgação **dos dados coletados** sem identificação individual dos respondentes.

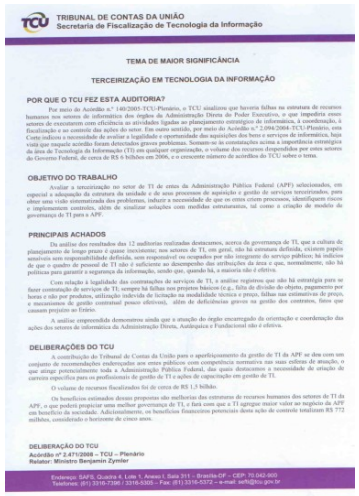
Resultados

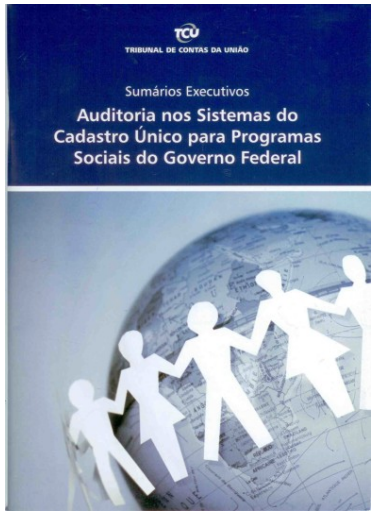
Trabalhos mais relevantes

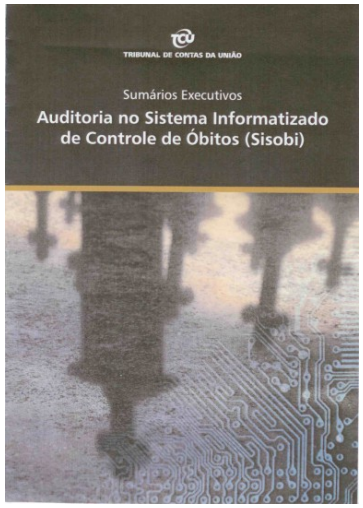


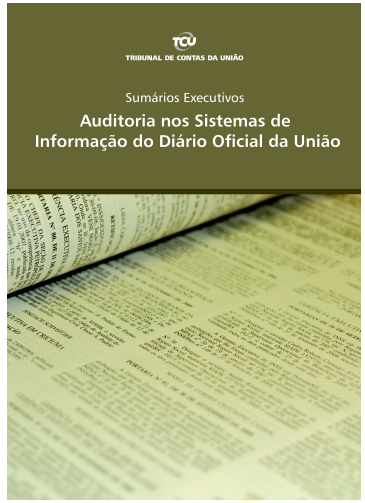












Benefícios das ações de controle

- ✓ Financeiros: R$ 7,5 bilhões (2007-2010)
  - Relação custo benefício: R$ 366,00 para R$ 1,00
  - Débitos, multas, economias e ganhos
- ✓ Benefícios não financeiros
  - melhorias na organização administrativa, nos controles internos e na forma de atuação dos órgãos fiscalizados;
  - fornecimento de subsídios para a atuação do Ministério Público e do Congresso Nacional;
  - recomendações para aprimoramento de normas.

Pesquisa com 14 gestores auditados no TMS Gestão e Uso de TI (2010)

- ✓94% ficaram satisfeitos ou muito satisfeitos com os procedimentos adotados pelas equipes, no início, na execução e no encerramento da auditoria.
- ✓Grande parte apontou estar satisfeita com a relevância dos resultados apresentados para a melhoria dos controles e desempenho do órgão.
- ✓Predominou o elogio acerca do objetivo da fiscalização de adequar a estrutura da administração pública federal às melhores práticas de TI e o caráter pedagógico de orientação aos órgãos e entidades fiscalizados.

Primeiros Resultados

- ✓ Judiciário
  - **CNJ** – Resolução nº 70, de 18.03.2009 – dispõe sobre o **Planejamento** e a Gestão Estratégica no âmbito do Poder Judiciário
  - **CNJ** – Resolução nº 99, de 24.11.2009 – dispõe sobre o Planejamento Estratégico de TI no âmbito do Poder Judiciário
- ✓ Executivo
  - **GSI/PR** – IN GSI/PR nº 01, de 13.06.2008 – disciplina a Gestão de **Segurança da Informação** na Administração Pública Federal
  - **GSI/PR** – 7 Notas Complementares (entre outubro de 2008 e maio de 2010)

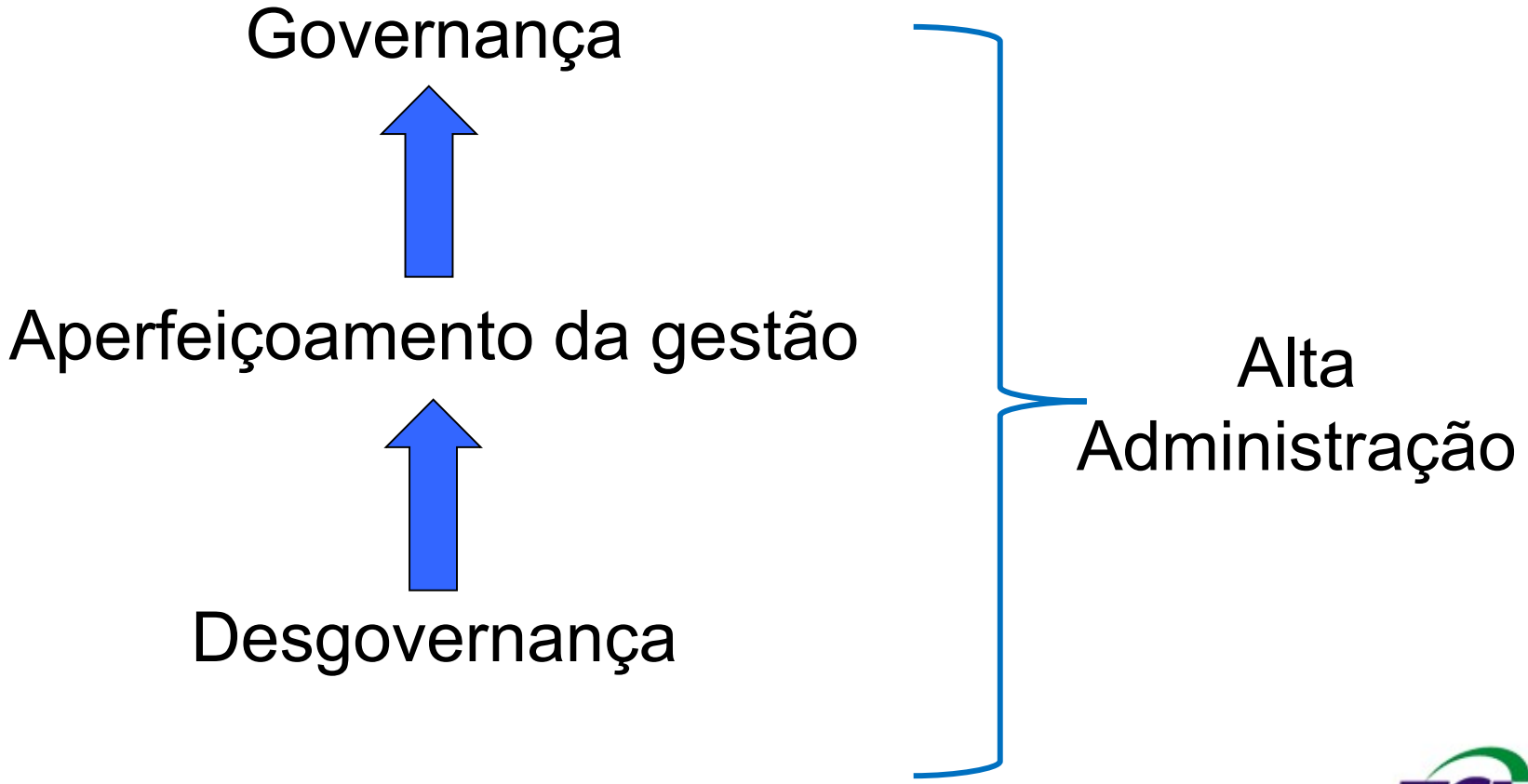
Primeiros Resultados

- ✓ Executivo
  - **MP** – **IN/SLTI nº 04/2008**, de 19.05.2008 – dispõe sobre processo de trabalho para contratações de TI

    (atualizada pela **IN/SLTI nº 04/2010**, de 12.11.2010)
  - **MP** – Portaria nº 63, de 27.03.2009 e Portaria nº 107 de 04.03.2010 – autorizam a realização de concurso público para provimento e a contratação de 230 **Analistas de TI**
  - **MP** – Indução da previsão e execução das despesas de **TI no OGU** (Acórdão nº 371/2008 – Plenário)

Conclusão

Conclusão


Governança
Aperfeiçoamento da gestão
Desgovernança
Alta
Administração

Obrigado

Augusto Sherman Cavalcanti