TRIBUNAL DE CONTAS DA UNIÃO

# Auditoria Interna na Área de Tecnologia da Informação

**André Luiz Furtado Pacheco, CISA**

4º Workshop de Auditoria de TI da Caixa

Brasília, agosto de 2011

# Agenda

- ✓ Introdução
- ✓ Exemplos de Deliberações pelo TCU ao Controle Interno
- ✓ Histórico da Auditoria de TI no TCU
- ✓ Estratégia de Atuação da Sefti
- ✓ Avaliação de Governança de TI
- ✓ 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 Administração Pública Federal

- ✓ 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 Administração Pública Federal

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

(Ministro Augusto Sherman, 30 Anos de TI no TCU)

# Exemplos de Deliberações pelo TCU ao Controle Interno

# Acórdão 2.094/2004-TCU-Plenário

*"9.3. determinar à (...) que, no seu âmbito de atuação, exerça o* ***controle efetivo dos contratos*** *de terceirização de serviços de informática e de desenvolvimento de sistemas* ***fazendo constar nas tomadas e prestações de contas*** *das entidades que realizam tais contratações* ***os exames realizados e os resultados obtidos****;"*

# Acórdão 353/2008-TCU-Plenário

*"9.2. recomendar, com fundamento no art. 27, inciso XVII, alínea g, da Lei 10.683/2003, ao (...) que:*

*9.2.1. oriente os órgãos e entidades do Poder Executivo quanto ao disposto no § 2º do art. 2º da Lei Complementar 110/2001, motivo pelo qual devem:*

*9.2.1.1. em atenção ao § 5º, do art. 65, da Lei 8.666/93, adotar as medidas necessárias, junto aos seus contratados, para* ***revisar para menos os valores previstos nos contratos em vigor, por conta do expurgo do adicional de FGTS eventualmente cobrado****;*

*(...)"*

# Acórdão 353/2008-TCU-Plenário

*"(...)*

*9.2.1.2.* ***buscar o ressarcimento das quantias pagas a maior****, a partir da competência janeiro de 2007, sempre que a relação custo/benefício assim o justificar;*

*9.2.1.3.* ***orientar os entes para os quais transfiram recursos públicos federais para que adotem as mesmas providências****;*

*9.2.1.4.* ***informar, nas contas prestadas anualmente a esta Corte, as medidas adotadas e os resultados alcançados****;"*

# Acórdão 353/2008-TCU-Plenário

*"9.3. determinar à (...) que* ***verifique as providências adotadas e os resultados alcançados*** *pelos entes da Administração Pública Federal, em decorrência das medidas do subitem 9.2 supra por ocasião das* ***contas de 2008****."*

# Acórdão 1603/2008-TCU-Plenário

*"9.3. recomendar à (...)* ***que realize regularmente Auditorias de TI e/ou promova ações para estimular a realização dessas Auditorias nos órgãos/entidades da Administração Pública Federal****;"*

# Acórdão 381/2011-Plenário

*"9.1.11. em face da Resolução CNJ 90/2009, art. 10, **promova ações para que a auditoria interna apoie a avaliação da TI**, observando as orientações contidas na Norma Técnica – **ITGI – Cobit 4.1, ME2 – Monitorar e avaliar os controles internos**, conforme tratado no achado 18 – Auditoria interna não apoia avaliação da TI – do relatório de fiscalização;"*

# Acórdão 757/2011-Plenário

*"9.1.9.* ***estabeleça processo de avaliação da gestão de TI****, à semelhança do Cobit 4.1, itens ME1.4 – Avaliação de desempenho, ME1.5 – Relatórios gerenciais, ME1.6 – Ações corretivas e ME2 – Monitorar e avaliar os controles internos;*

*9.1.10.* ***promova ações para que a auditoria interna apoie a avaliação da TI****, à semelhança das orientações do Cobit 4.1, ME2 – Monitorar e avaliar os controles internos;"*

# Histórico da Auditoria de TI no TCU

# 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

## 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);

# 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

# 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

# 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)

# Oportunidades para Sefti

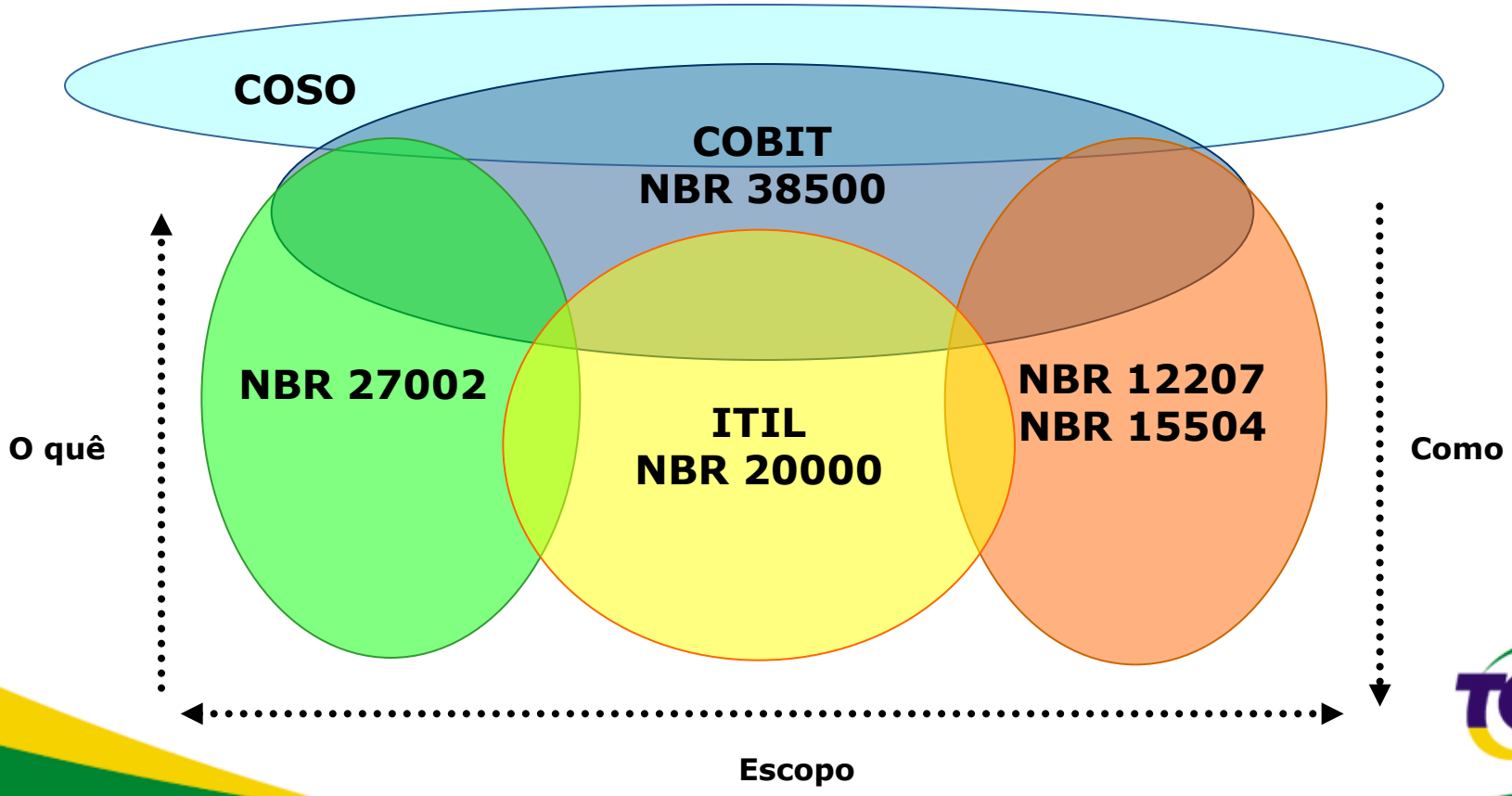
- ✓ Indução da melhoria da Governança de TI na APF
- ✓ Materialidade das despesas com TI
- ✓ Critérios para gestão e fiscalização bem estabelecidos
- ✓ Método de fiscalização testado e aprovado
- ✓ Dependência da TI pela APF
- ✓ Boa repercussão na APF e sociedade

# Riscos para a Sefti

- ✓ Falta de conhecimento específico para assunto complexo ou peculiar
- ✓ Desatualização dos auditores quanto à capacitação técnica
- ✓ Quantidade de processos para elaboração de parecer ou instrução de mérito (denúncias, representações)
- ✓ Não incremento da força de trabalho

# 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

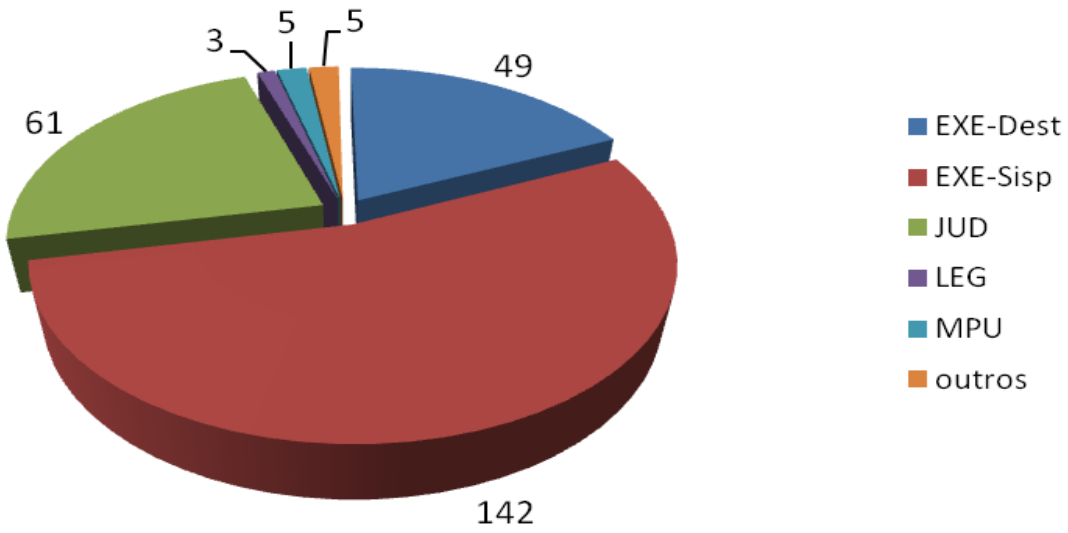
- ✓ 30 questões – 152 itens
- ✓ Dividido segundo 7 dimensões do Gespública
  - Liderança
  - Estratégias e planos
  - Cidadãos
  - Sociedade
  - Informações e conhecimento
  - Pessoas
  - Processos

# 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

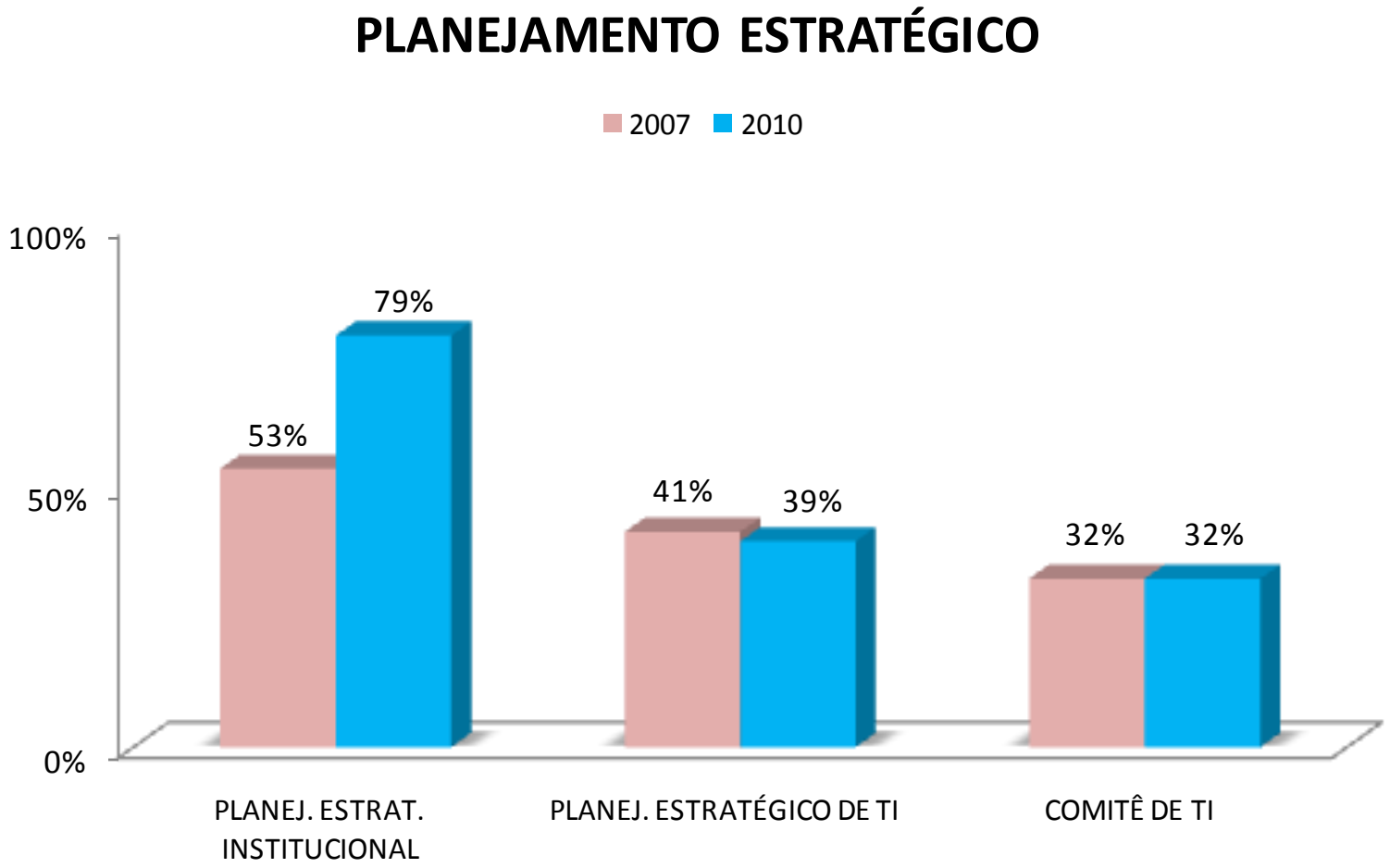
# Público alvo

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

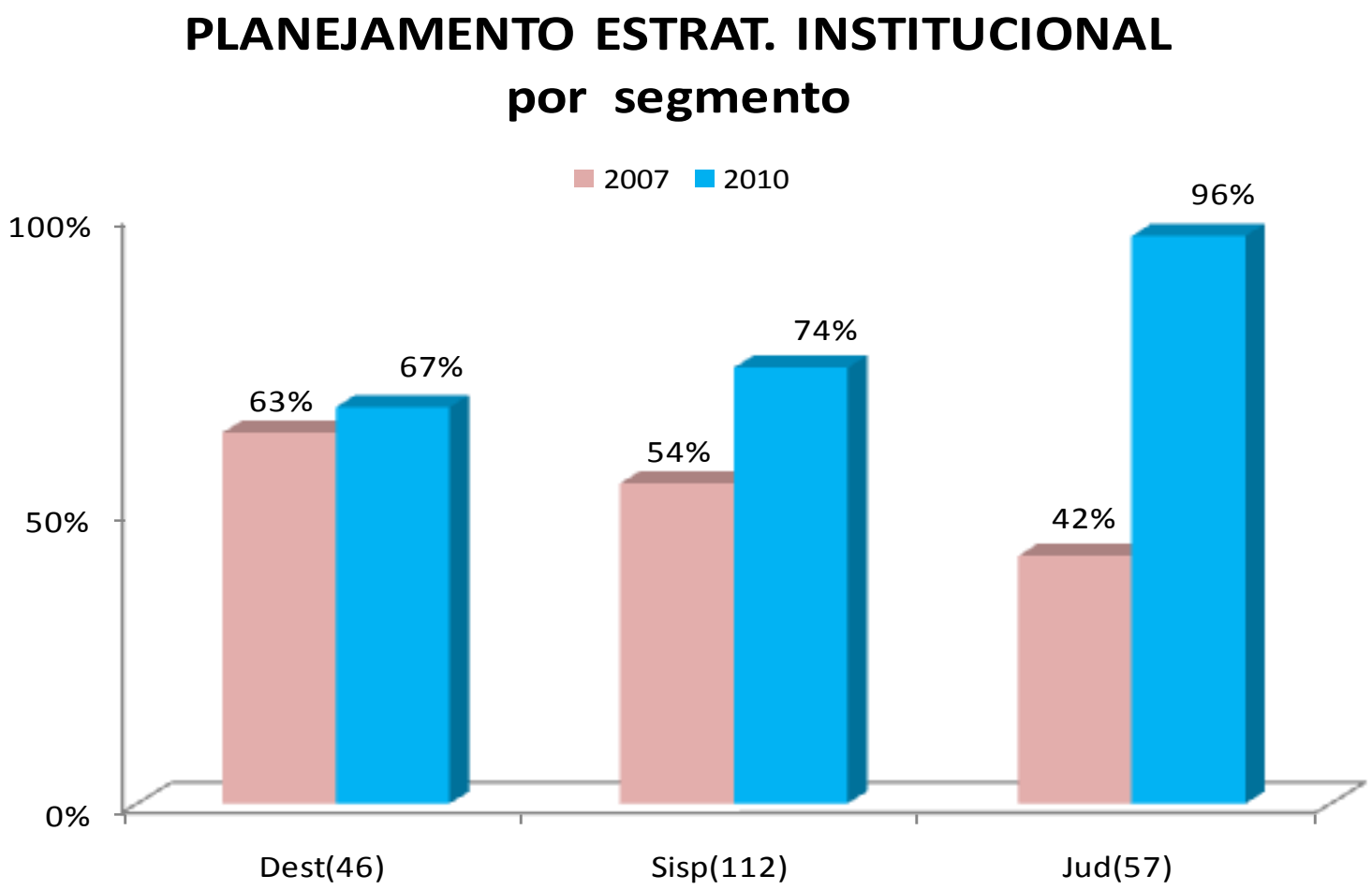



- ✓ 223 responderam os dois levantamentos (de 2007 e de 2010)

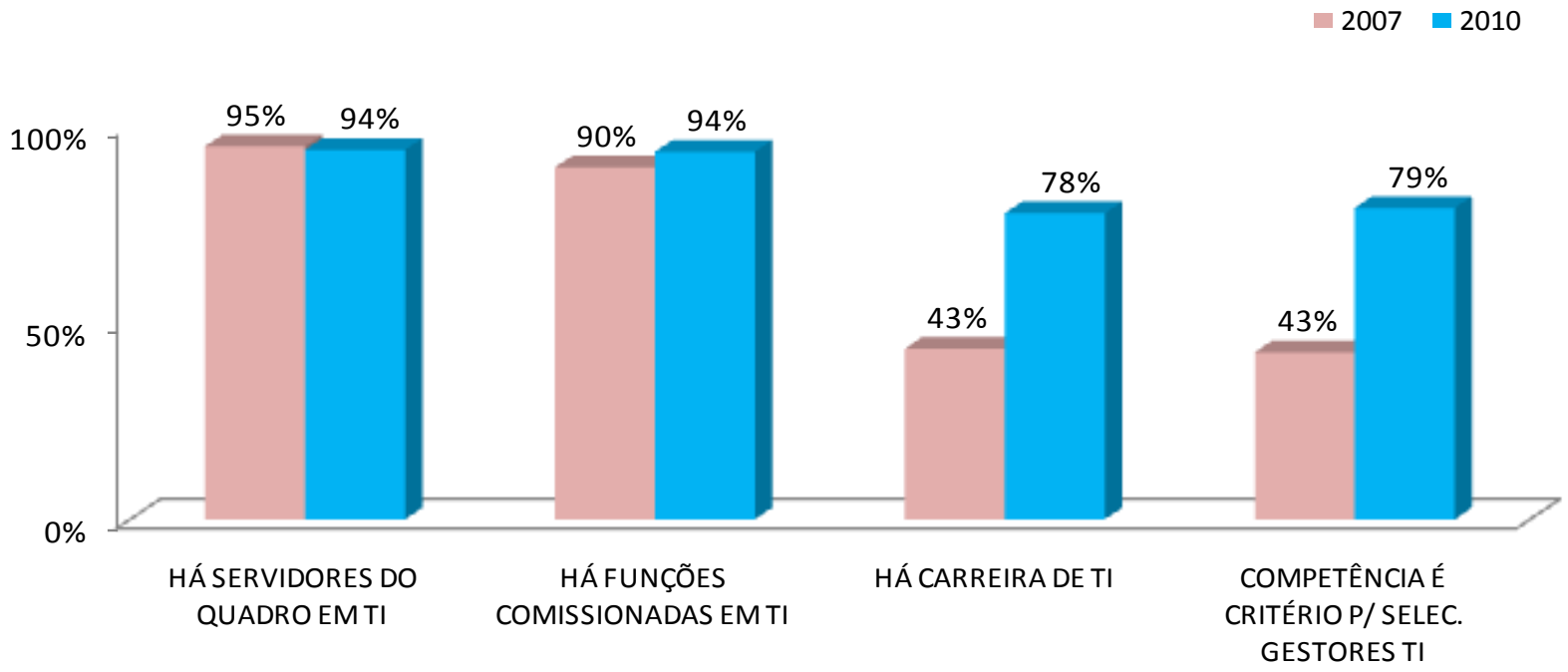
# Comparação 2007 x 2010



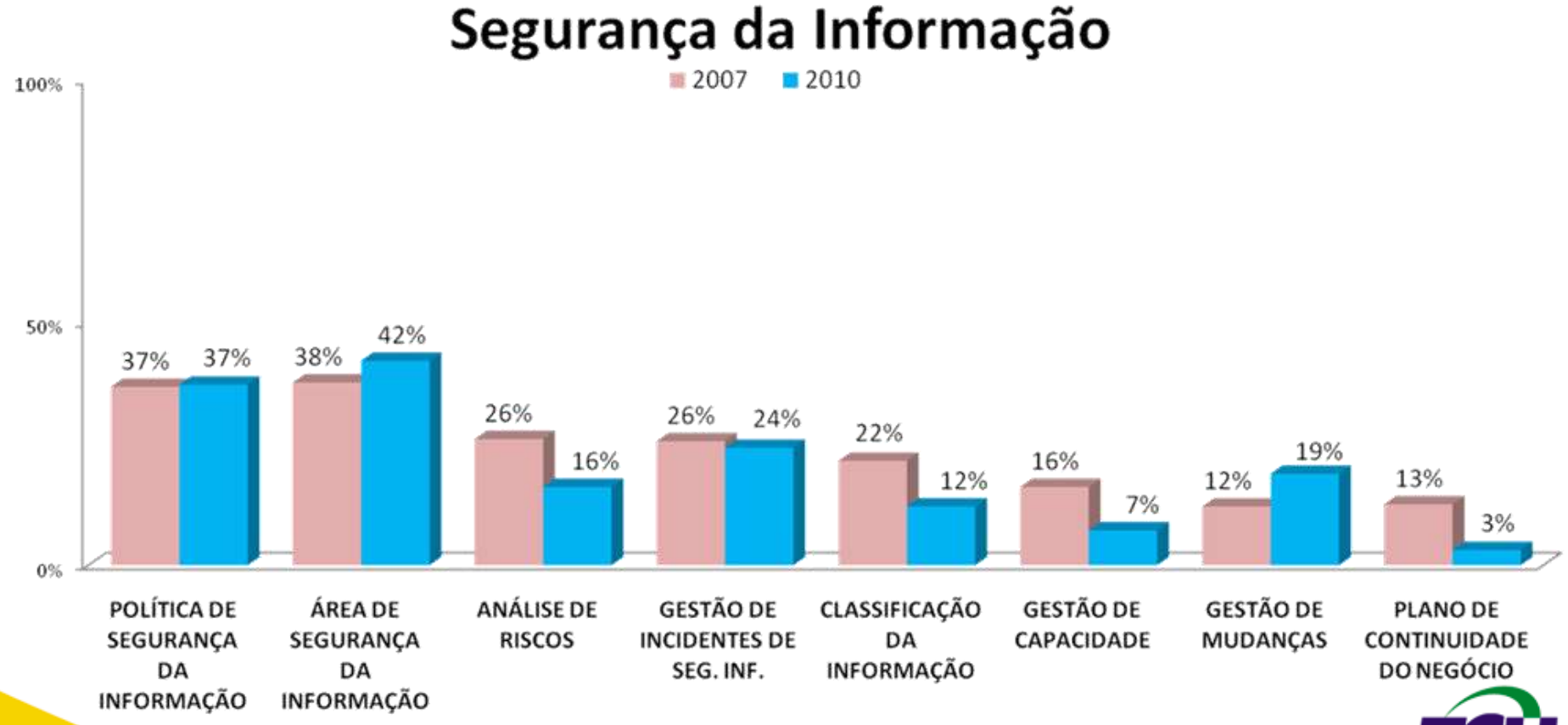
# Comparação 2007 x 2010



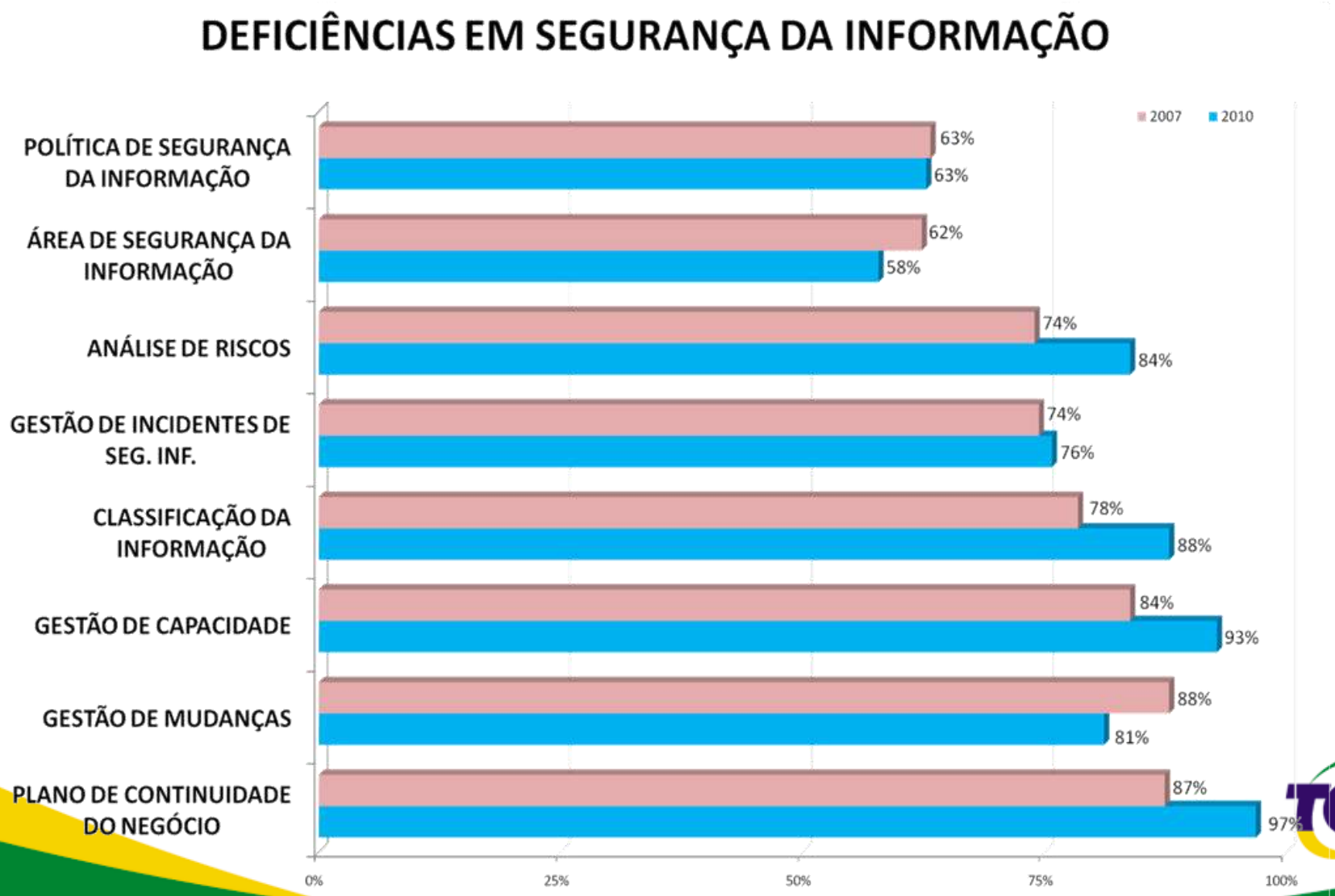
# Comparação 2007 x 2010



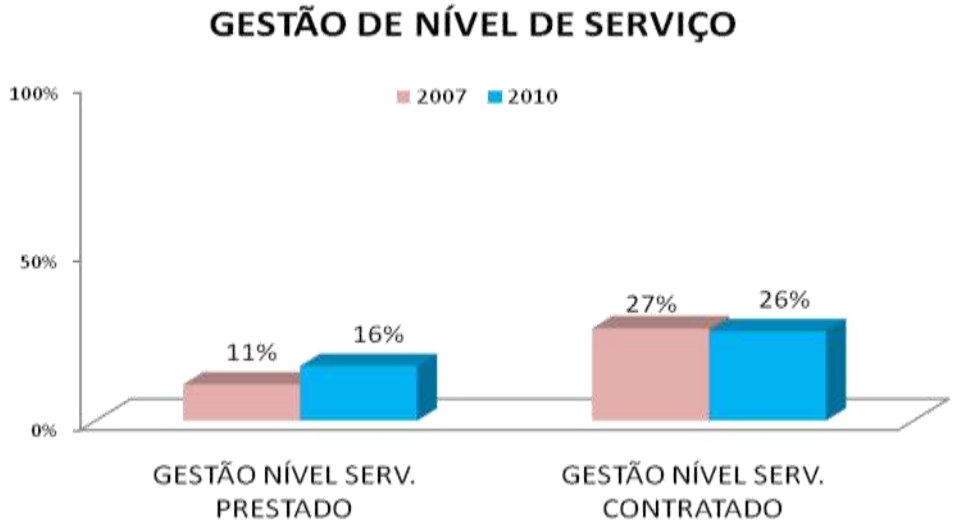
# Comparação 2007 x 2010

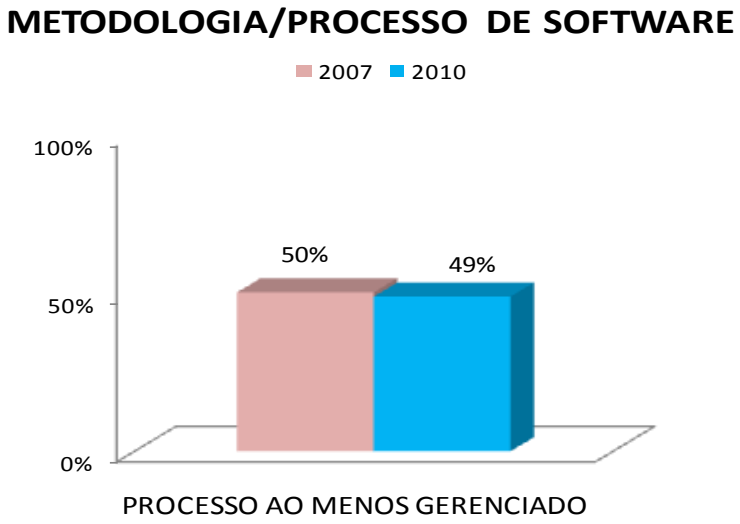


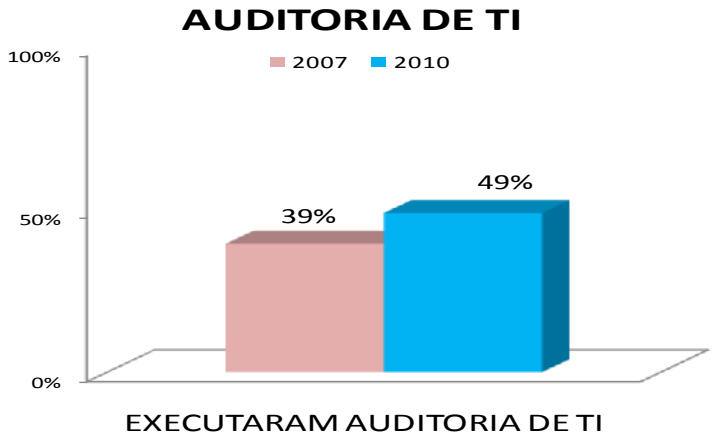
# Comparação 2007 x 2010



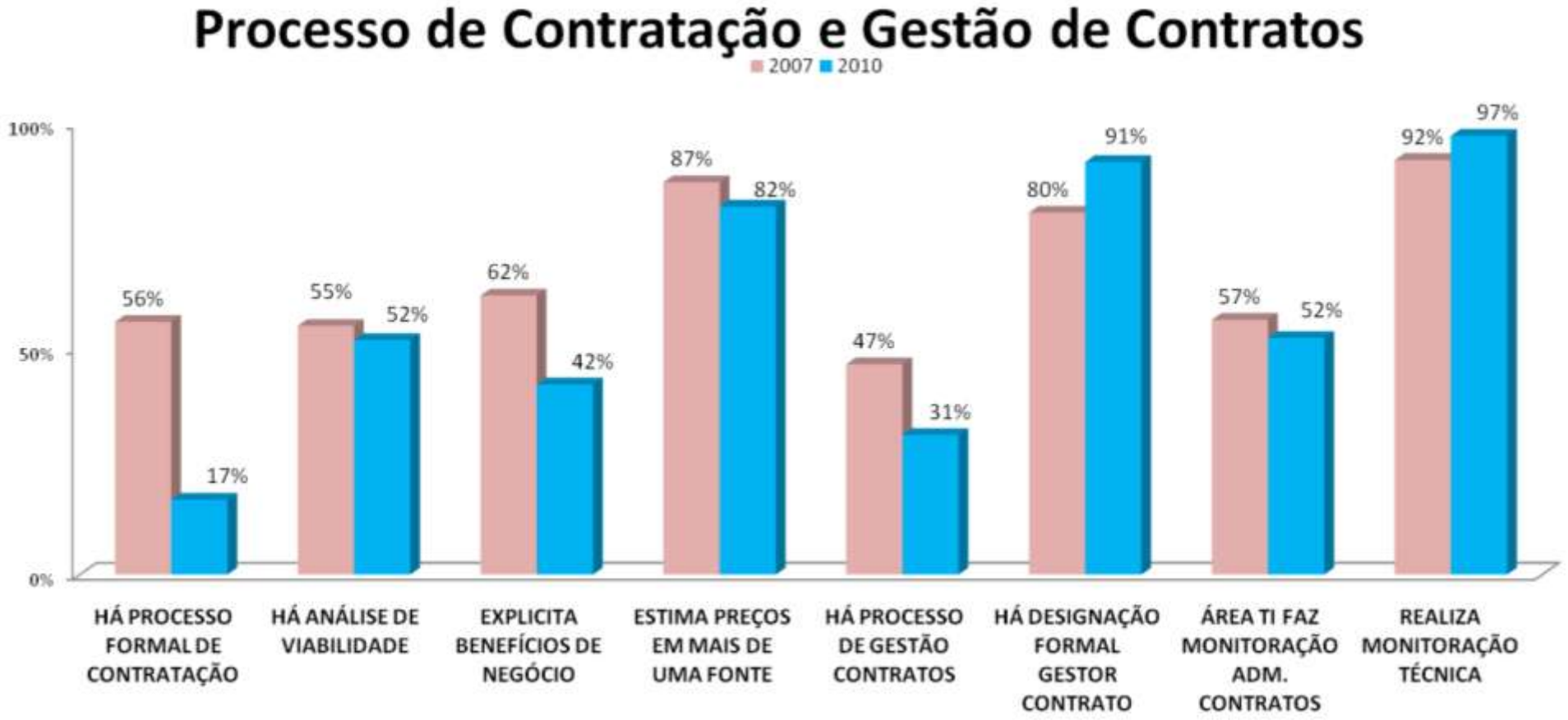
# Comparação 2007 x 2010



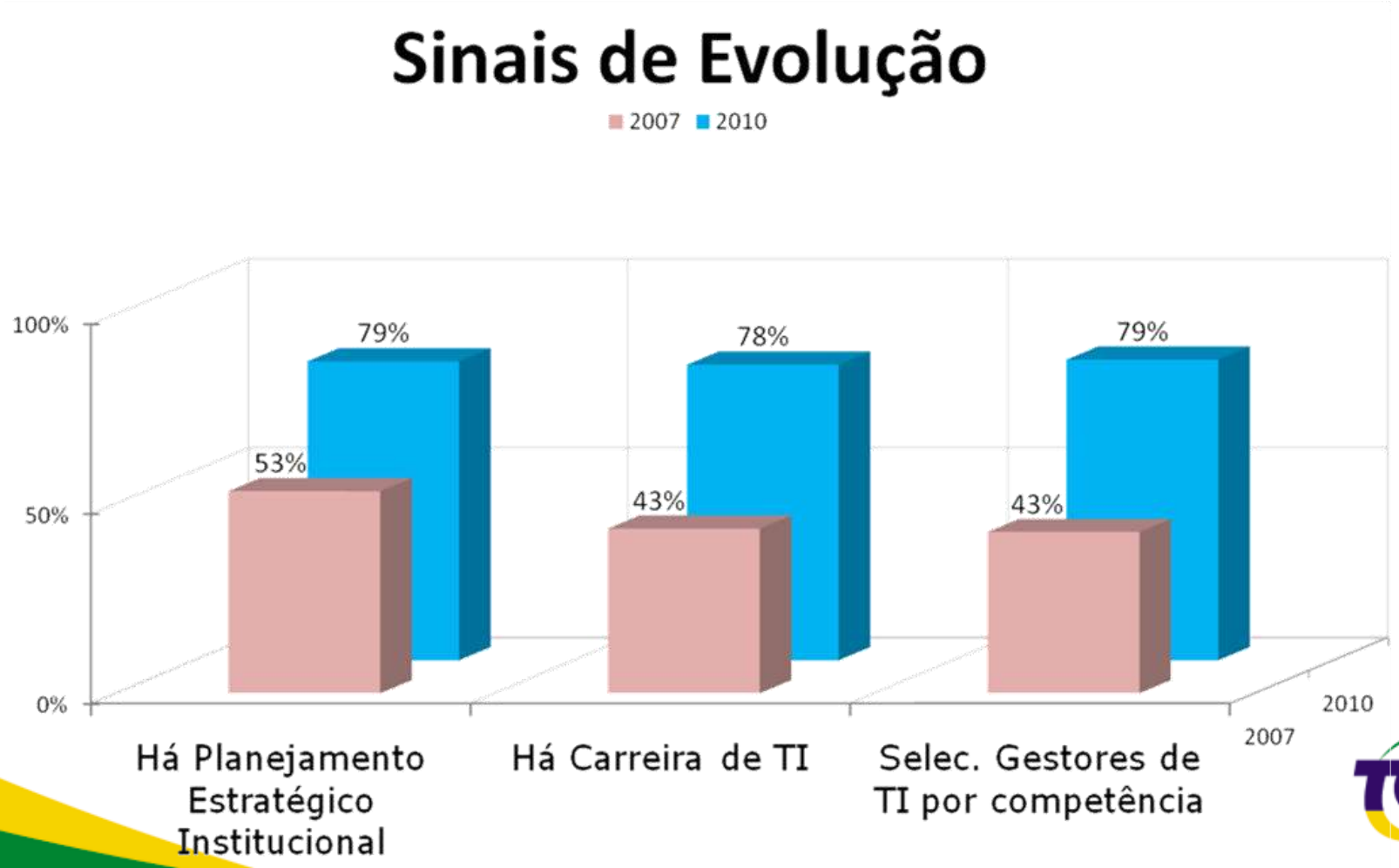



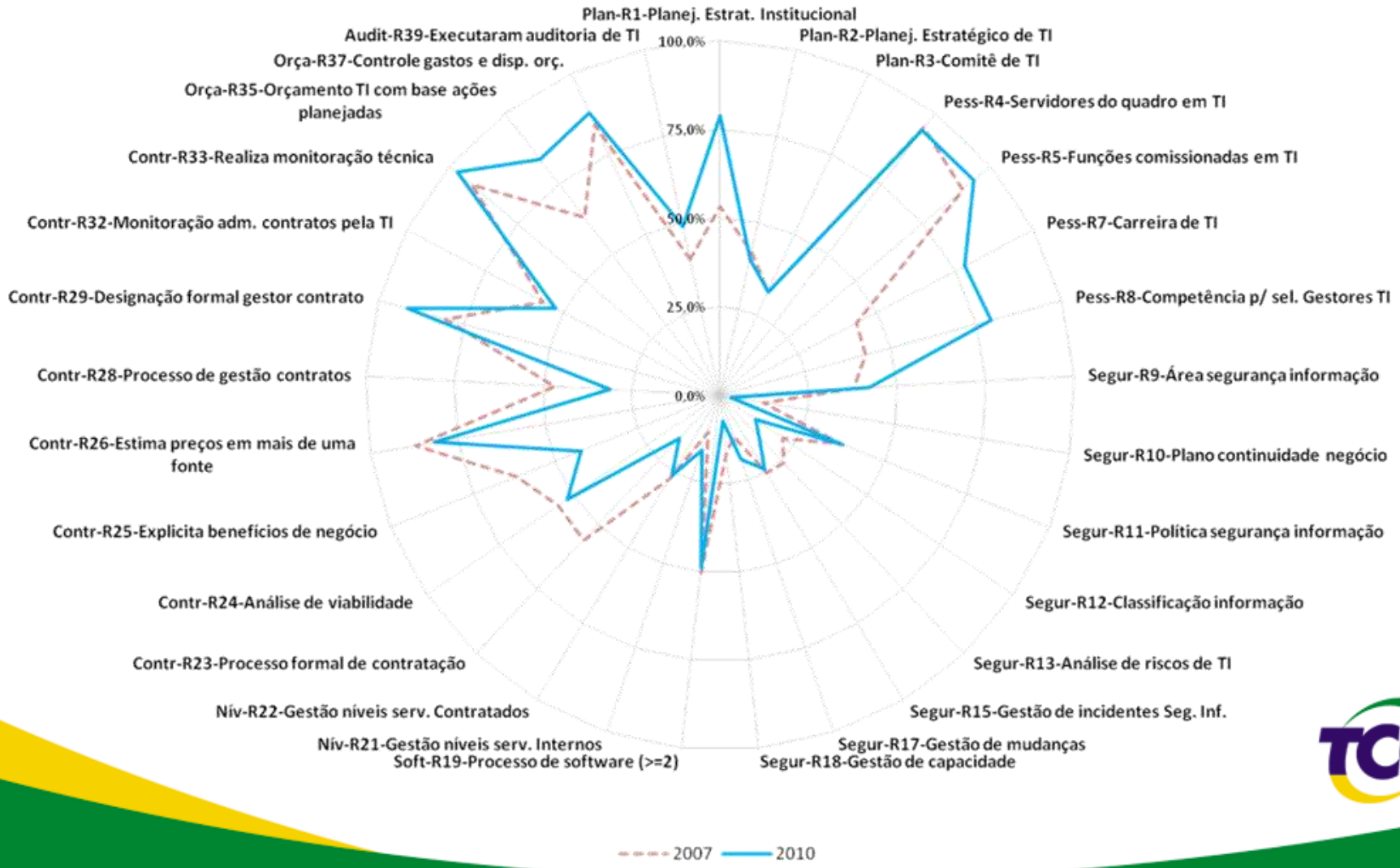
# Comparação 2007 x 2010



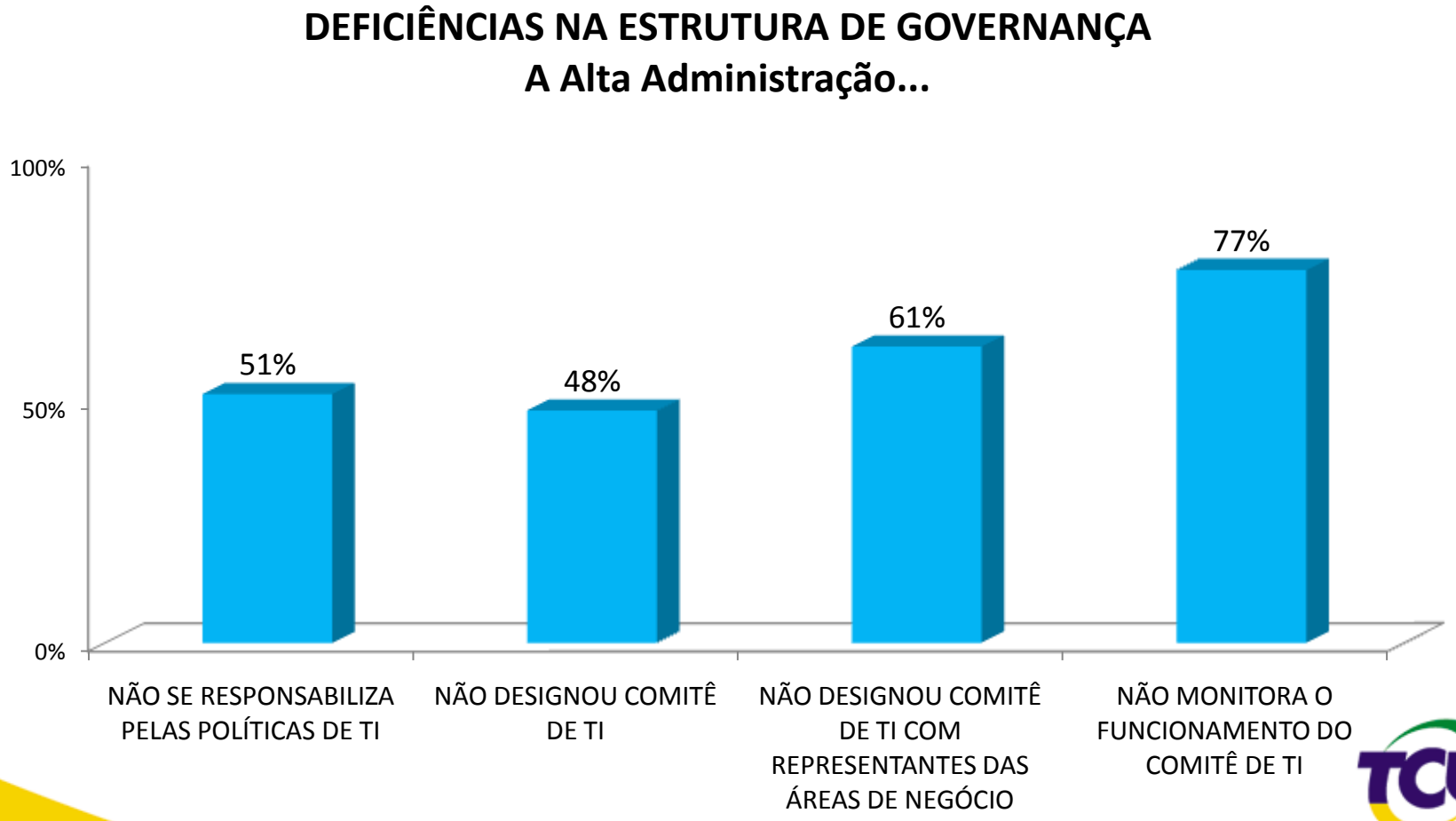
# Comparação 2007 x 2010



# Radar - Comparativo 2007/2010

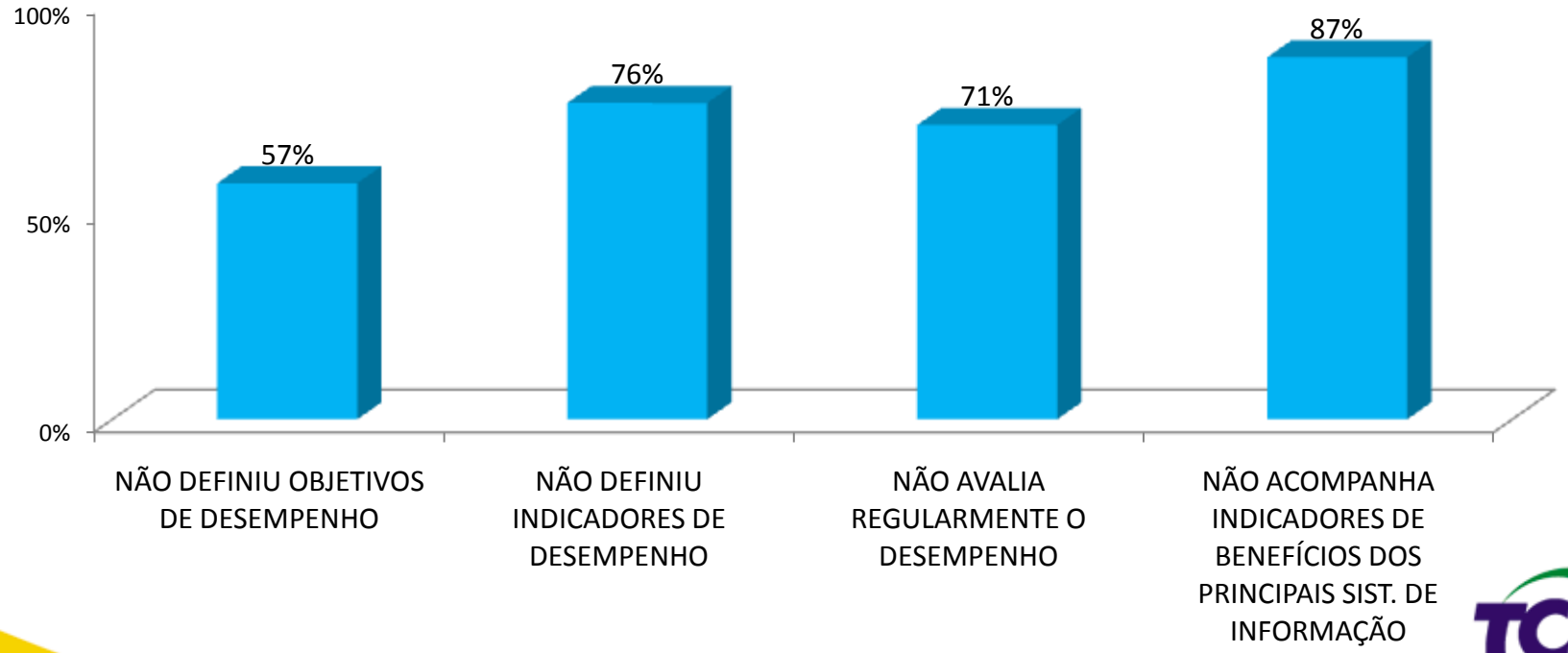


# Principais Achados

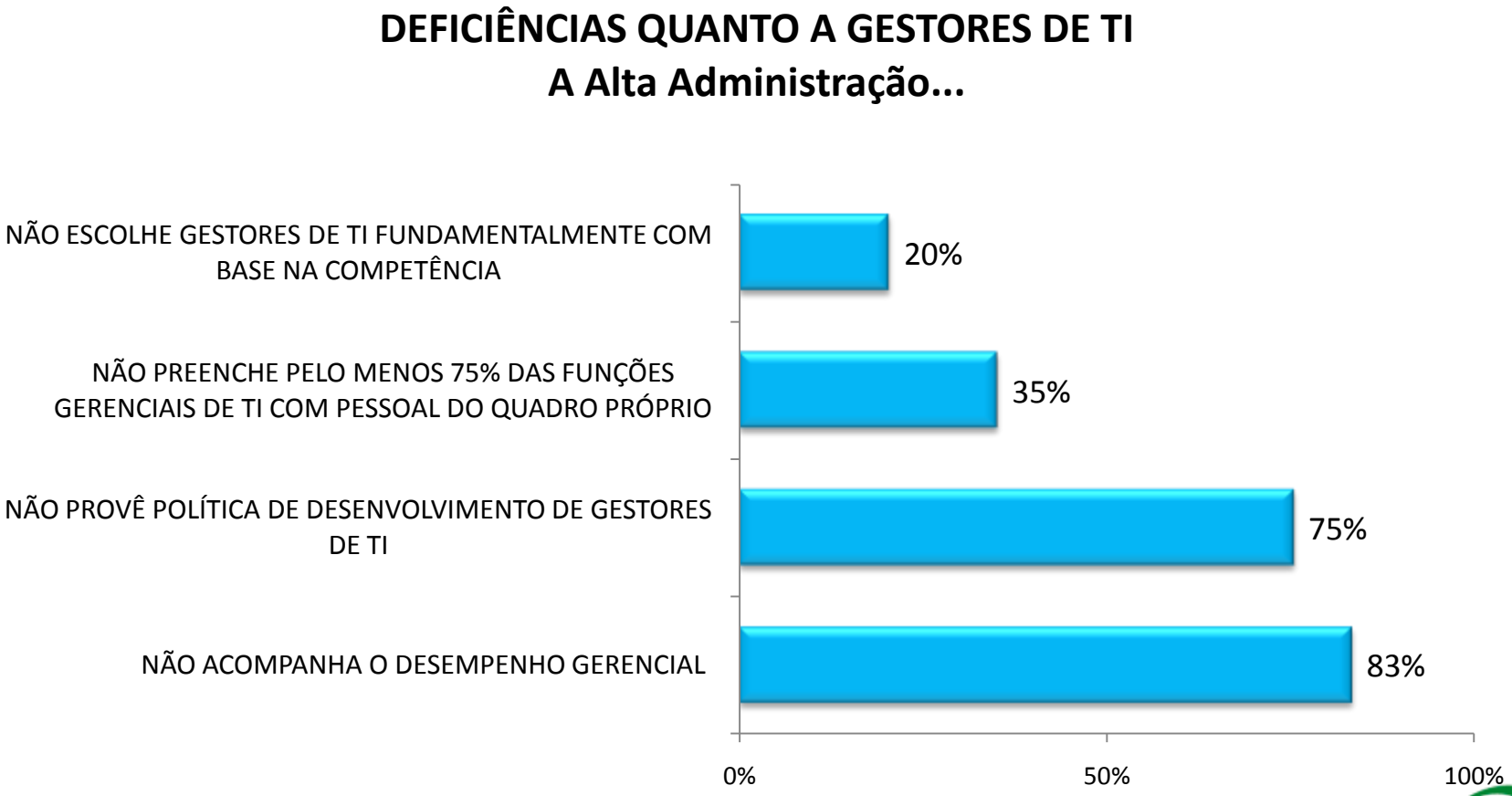


# Principais Achados

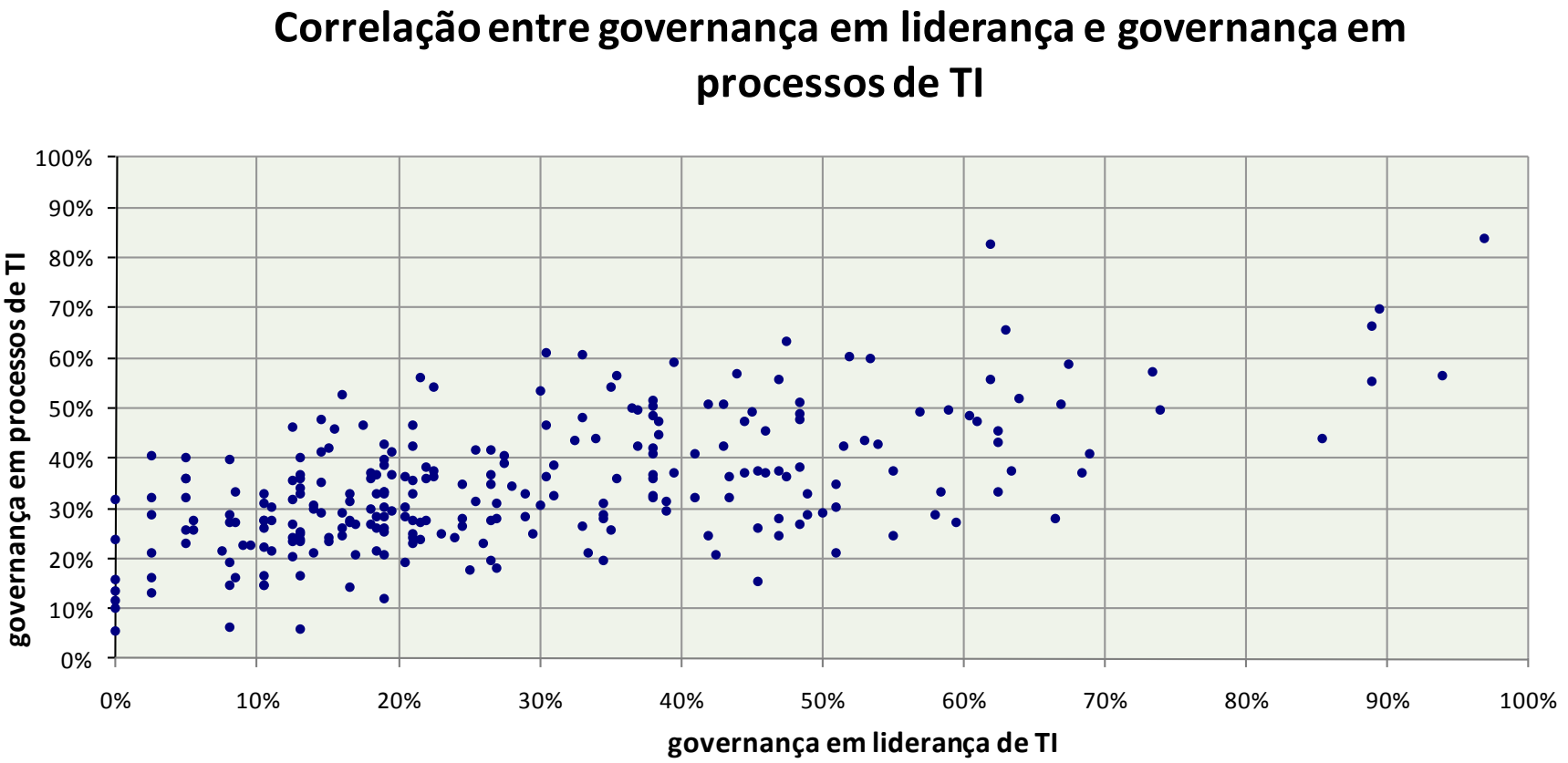
**DEFICIÊNCIAS INSTITUCIONAIS NA GESTÃO E USO DE TI**
**A Alta Administração...**



# Principais Achados



# Principais Achados



# Índice de Governança de TI iGovTI 2010

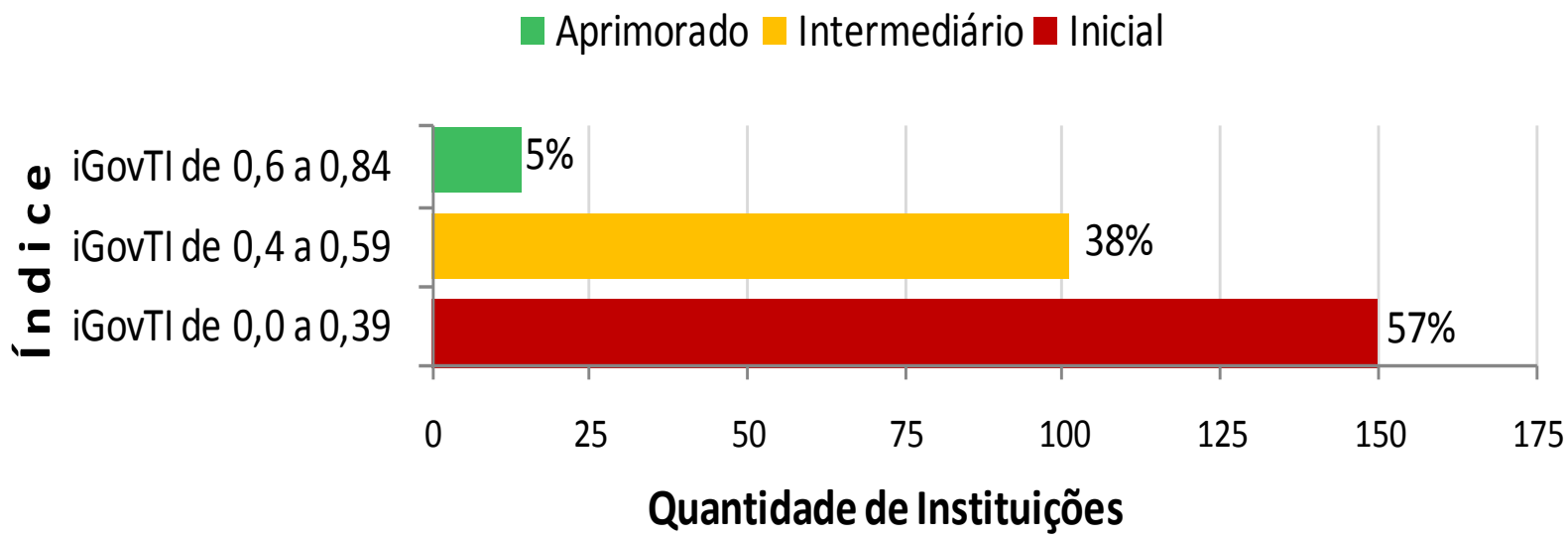
- ✓ iGovTI
  - Métrica de governança de TI criada pela Sefti
  - Calculado sobre as respostas 2010
- ✓ Critérios
  - Cobit 4.1
  - Gespública
  - Acórdão nº 1.603/2008-TCU-Plenário

# 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%

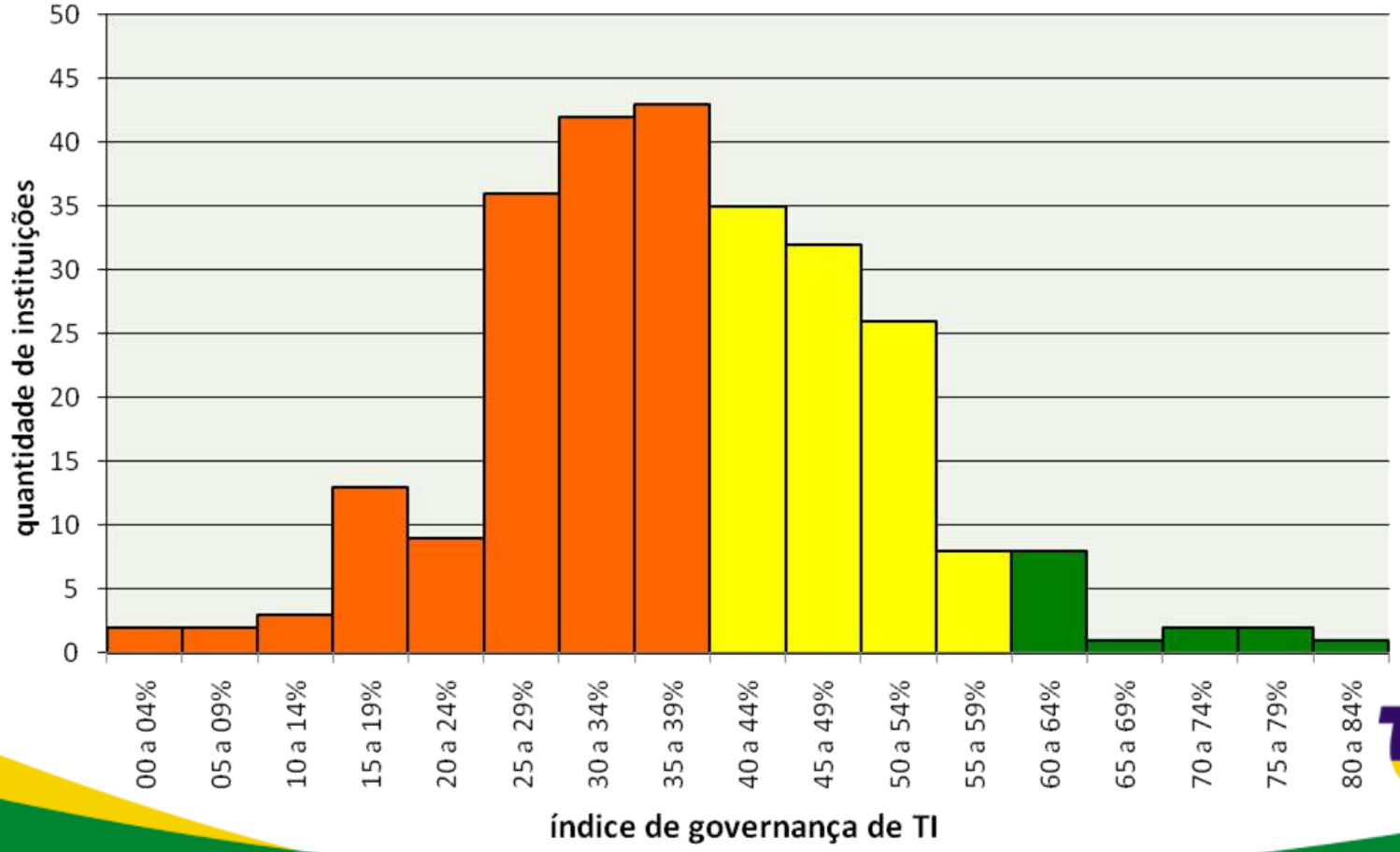
# Índice de Governança de TI iGovTI 2010

## Instituições x Estágios do iGovTI

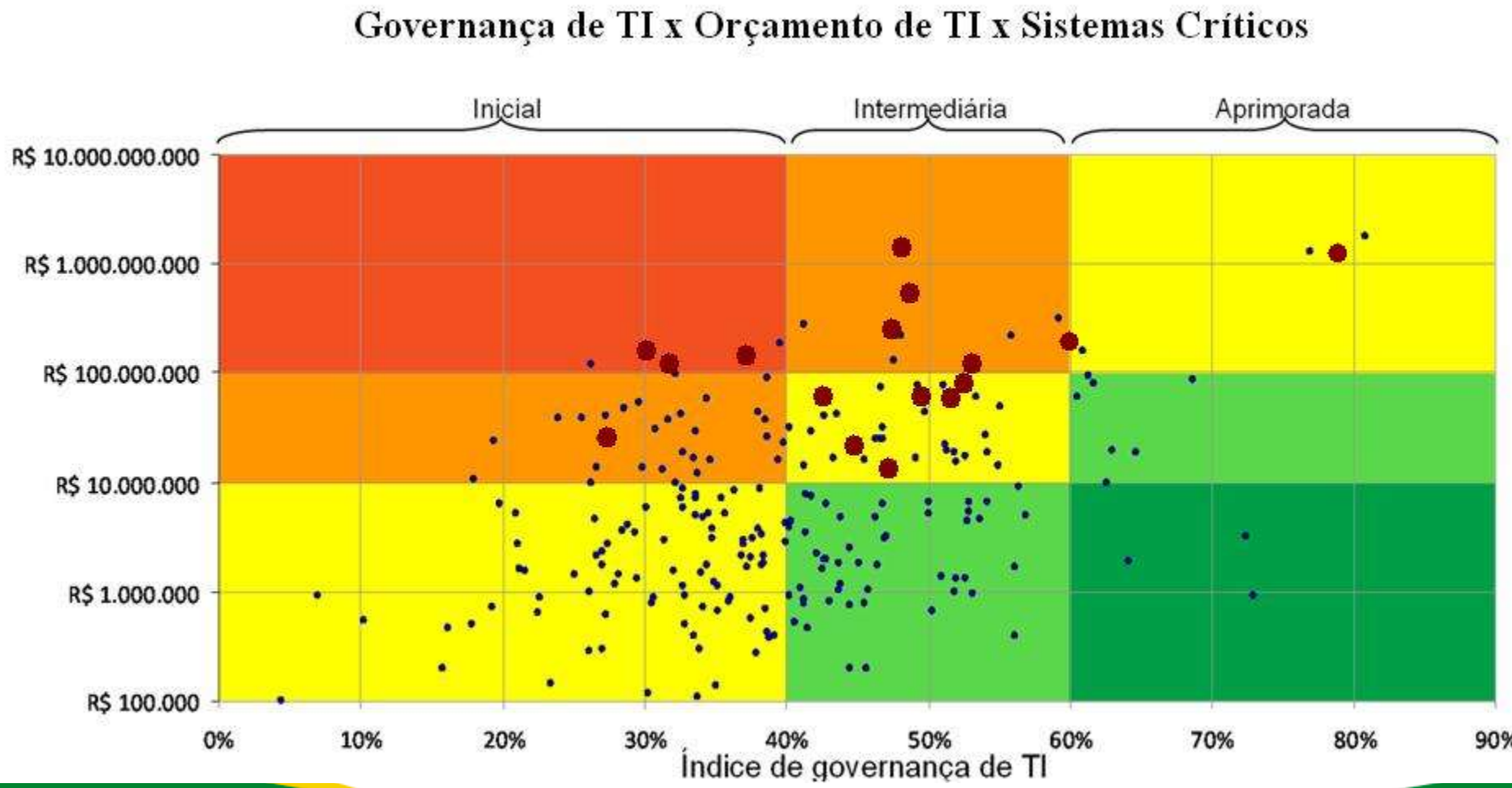


# Índice de Governança de TI iGovTI 2010

## 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;

e) realize levantamentos regulares com coleta de evidências;

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

# Responsabilidade Governança de TI

*"**A governança de TI é de responsabilidade da alta administração**, na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização"*

ITGI – *IT Governance Institute*

# Governança de TI – NBR ISO/IEC 38500

- ✓ *"A responsabilidade por aspectos específicos de TI pode ser delegada aos gerentes da organização. No entanto,* ***a responsabilidade pelo uso e entrega aceitável, eficaz e eficiente da TI pela organização permanece com os dirigentes e não pode ser delegada****".*

  (NBR ISO/IEC 38500, Nota do item 2.2)

- ✓ Ex: Acórdão nº 2.079/2009-TCU-Plenário

# Controles e o Papel do Gestor

- ✓ *"**Auditores** são parte do modelo governamental de controle interno, mas eles **não são responsáveis pela implementação dos procedimentos de controle** numa organização. Este trabalho é específico do gestor."*

  (Intosai, Padrões de Controle Interno)

- ✓ *"**Controle interno é uma ferramenta do gestor** usada para prover razoável certeza de que os objetivos da administração estão sendo alcançados."*

  (Intosai, Orientações para Padrões de Controle Interno)

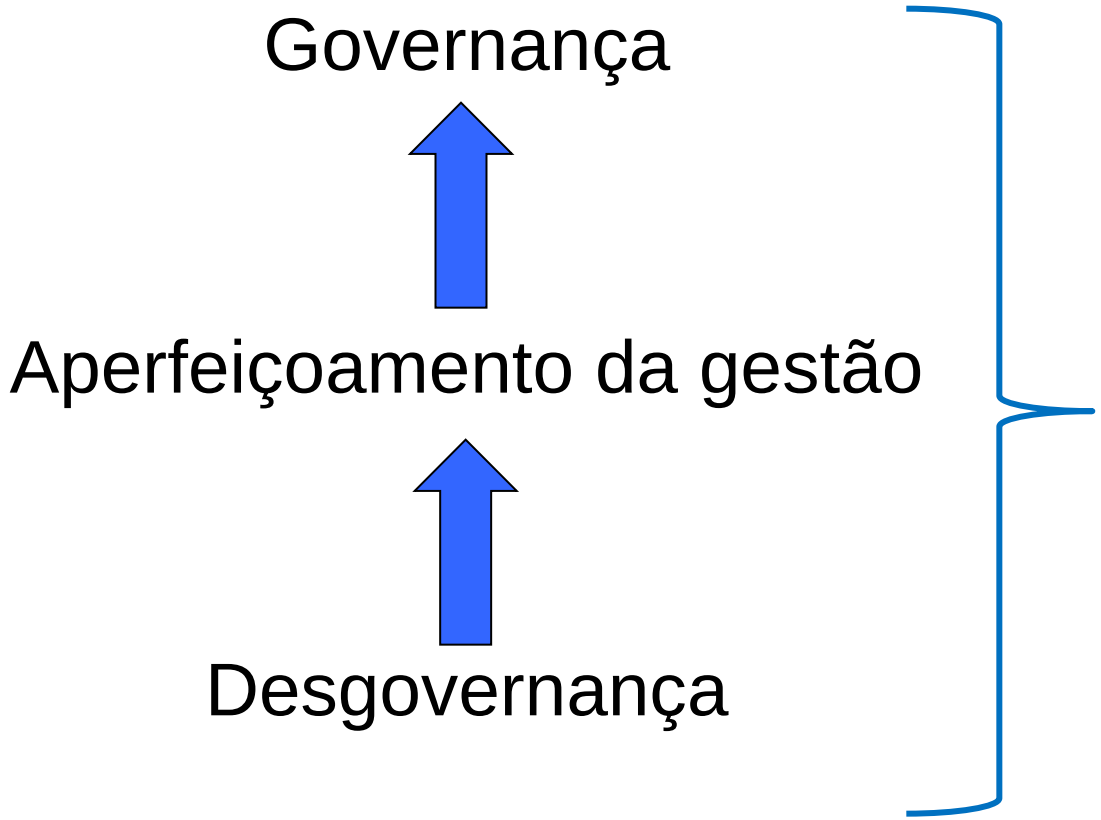
# Controles e o Papel do Gestor

***"O gestor e a alta administração são responsáveis pelos processos de gestão de risco e controles da organização."***

(IIA / IPPF - Padrão 2120-1)

# Conclusão

# Conclusão


Governança
Aperfeiçoamento da gestão
Desgovernança
Alta Administração apoiada pelo Controle Interno

# Obrigado

**André Luiz Furtado Pacheco, CISA**

**andrefp@tcu.gov.br**

**Sefti, 3316-5901**