TRIBUNAL DE CONTAS DA UNIÃO

Questionário de Governança de TI de 2014

Daniel Jezini Netto, CISA
TCU/Sefti
Brasília/DF, 8 de maio de 2014

Sefti

Criada em agosto de 2006 (Resolução TCU 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."*

Quantos somos

- 28 servidores: 25 auditores e 03 técnicos

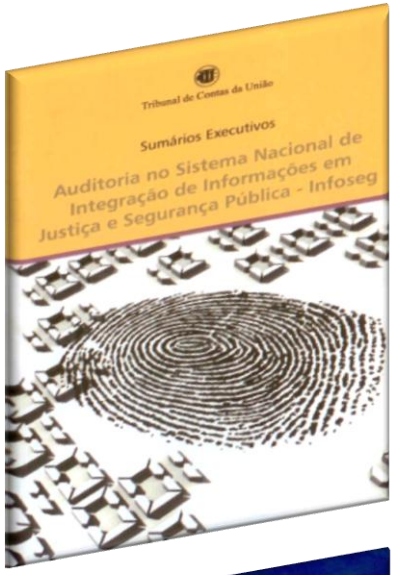
Estrutura

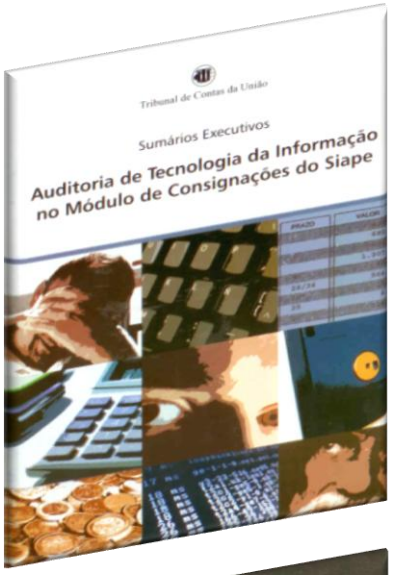
- 03 diretorias de fiscalização de governança de TI, 02 assessorias e 01 serviço de administração

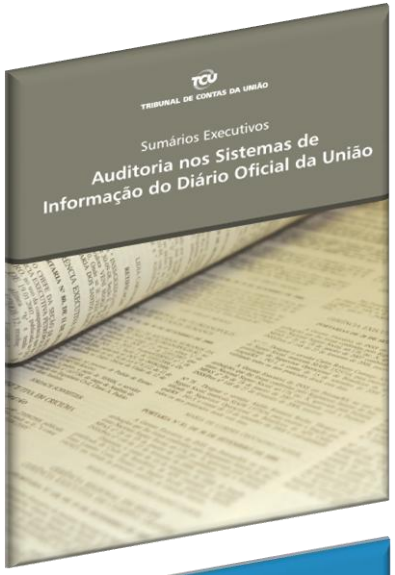
Competência profissional

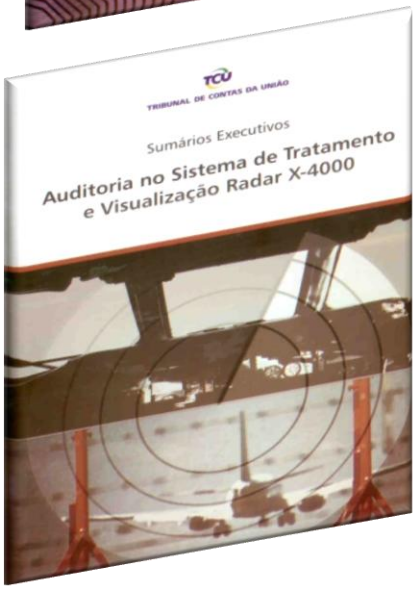
- Formação em áreas de tecnologia
  - Ciência da Computação, Engenharia e afins
- Certificações
  - 11 CISA (*Certified Information Systems Auditor*)
  - 1 CGEIT (*Certified in Governance of Enterprise IT*)
  - 4 Auditor Líder (ISO/NBR 27001)
  - 1 CISSP (Certified Information Systems Security Professional)
  - 5 MSc

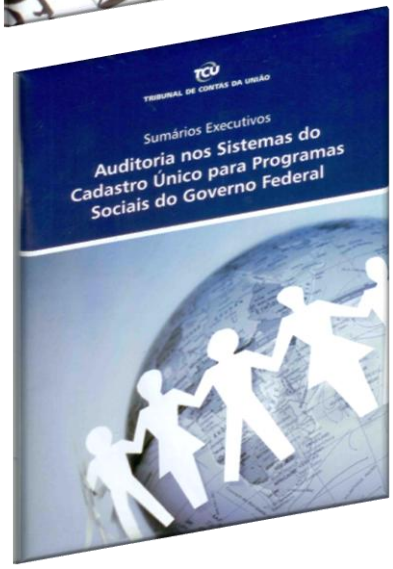

TRIBUNAL DE CONTAS DA UNIÃO
Sumário Executivo
Avaliação do Programa Governo Eletrônico

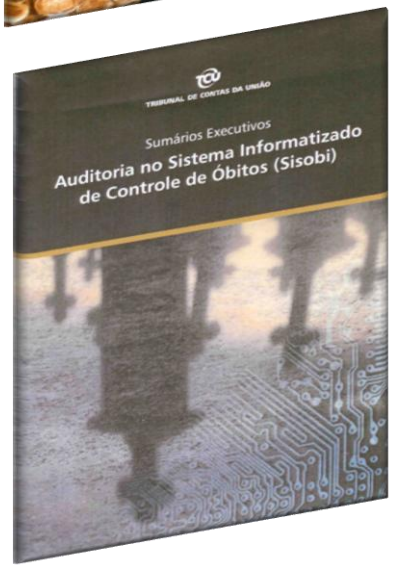

Tribunal de Contas da União
Sumários Executivos
Auditoria no Sistema Nacional de Integração de Informações em Justiça e Segurança Pública - Infoseg

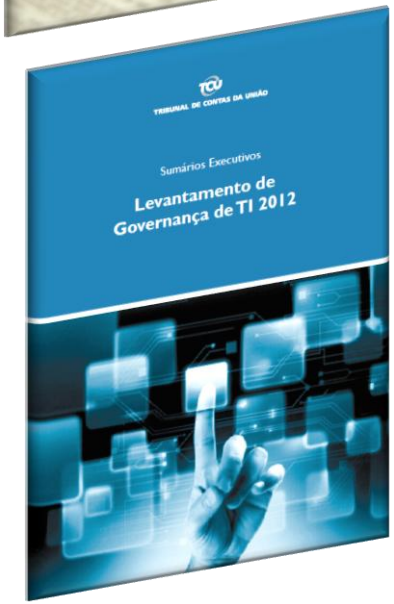

Tribunal de Contas da União
Sumários Executivos
Auditoria de Tecnologia da Informação no Módulo de Consignações do Siape


TRIBUNAL DE CONTAS DA UNIÃO
Sumários Executivos
Auditoria nos Sistemas de Informação do Diário Oficial da União


TRIBUNAL DE CONTAS DA UNIÃO
Sumários Executivos
Auditoria no Sistema de Tratamento e Visualização Radar X-4000


TRIBUNAL DE CONTAS DA UNIÃO
Sumários Executivos
Auditoria nos Sistemas do Cadastro Único para Programas Sociais do Governo Federal


TRIBUNAL DE CONTAS DA UNIÃO
Sumários Executivos
Auditoria no Sistema Informatizado de Controle de Óbitos (Sisobi)


TRIBUNAL DE CONTAS DA UNIÃO
Sumários Executivos
Levantamento de Governança de TI 2012

Benefícios

12 Bi+

Negócio

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

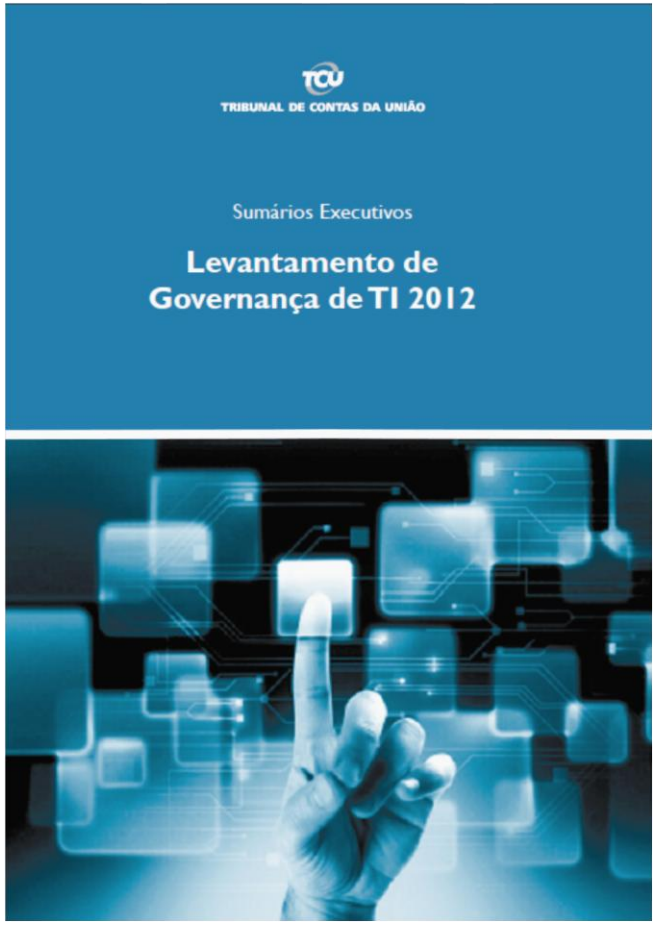
Missão

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

Vamos ao Levantamento De GovTI!



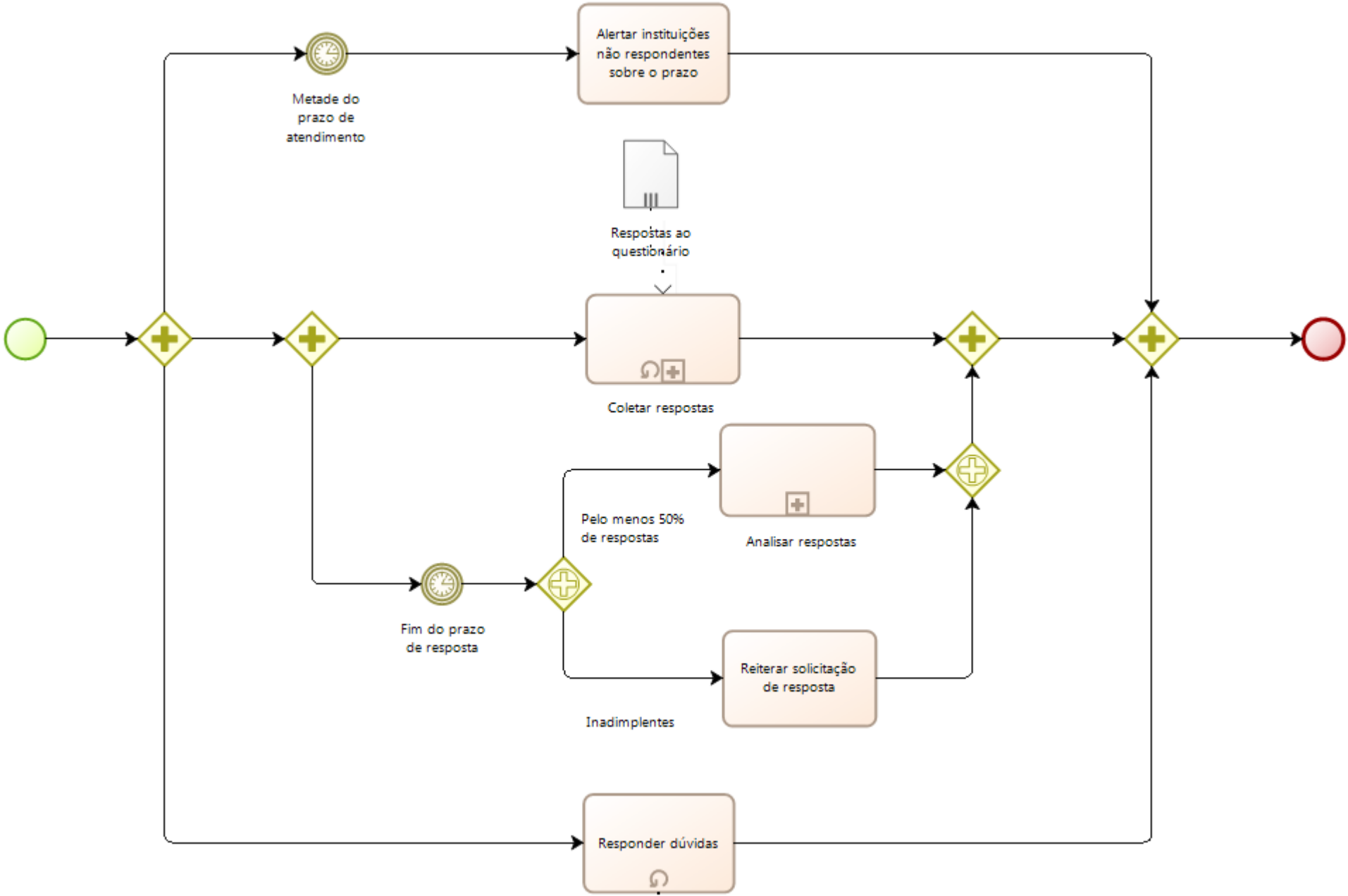
The Seven Phases of the Implementation Life Cycle

1º DESAFIO

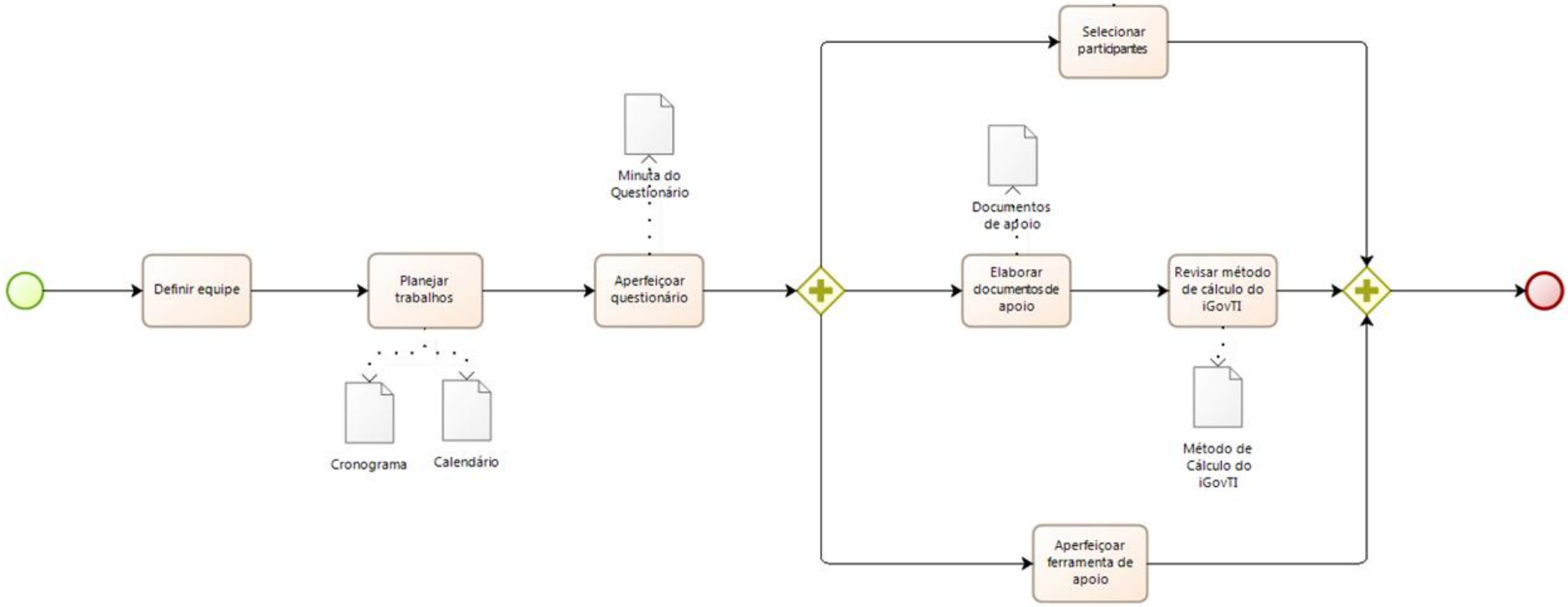
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

Source: COBIT 5, figure 17 and *COBIT 5 Implementation*, figure 6

Falando em práticas e processos...

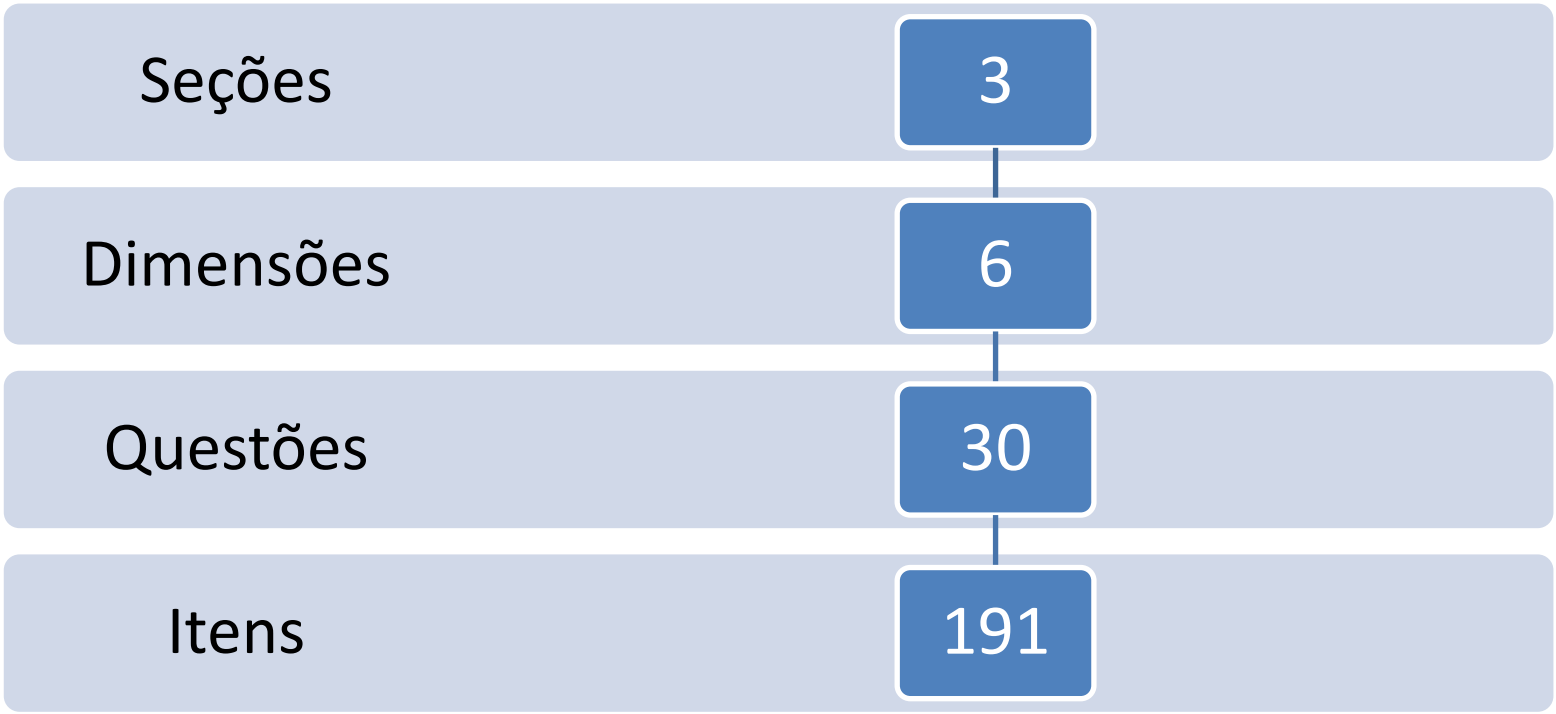


2º Ano

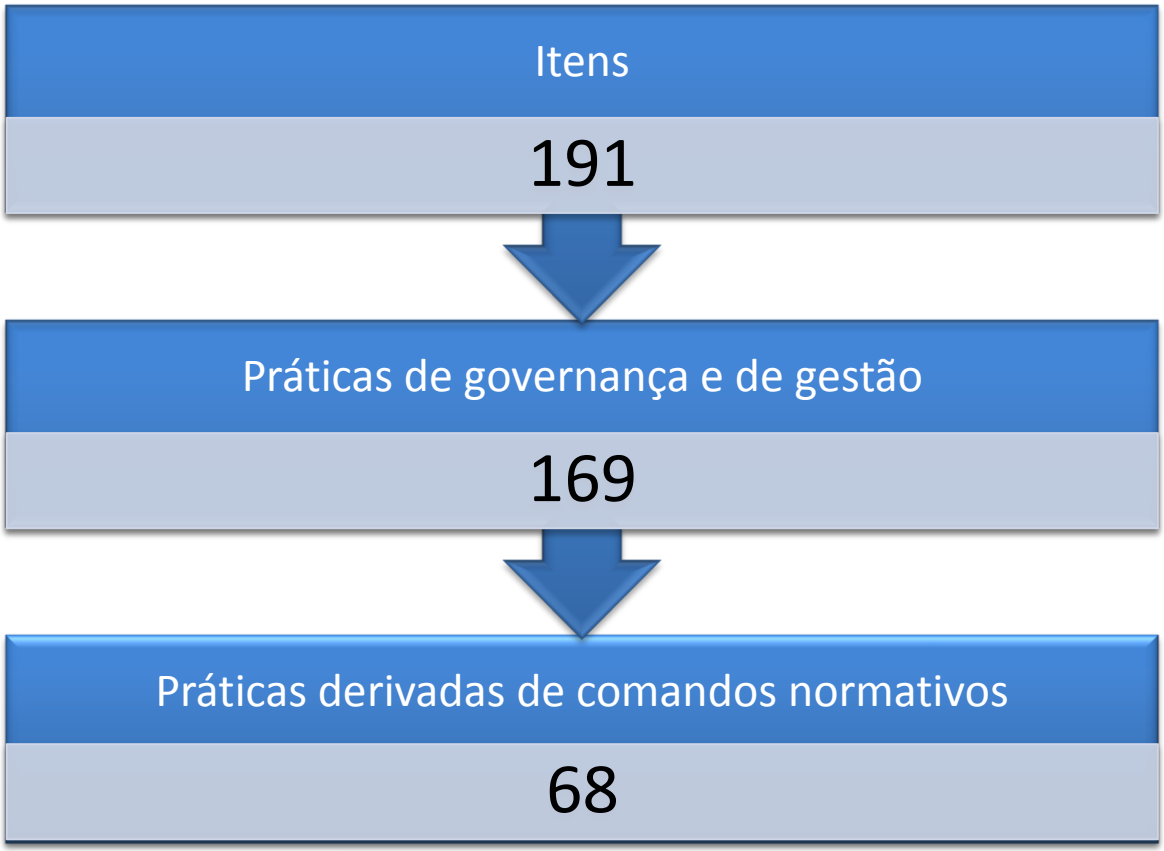

Definir equipe
Planejar trabalhos
Cronograma
Calendário
Minuta do Questionário
Aperfeiçoar questionário
Selecionar participantes
Documentos de apoio
Elaborar documentos de apoio
Revisar método de cálculo do iGovTI
Método de Cálculo do iGovTI
Aperfeiçoar ferramenta de apoio

Processo de Revisão

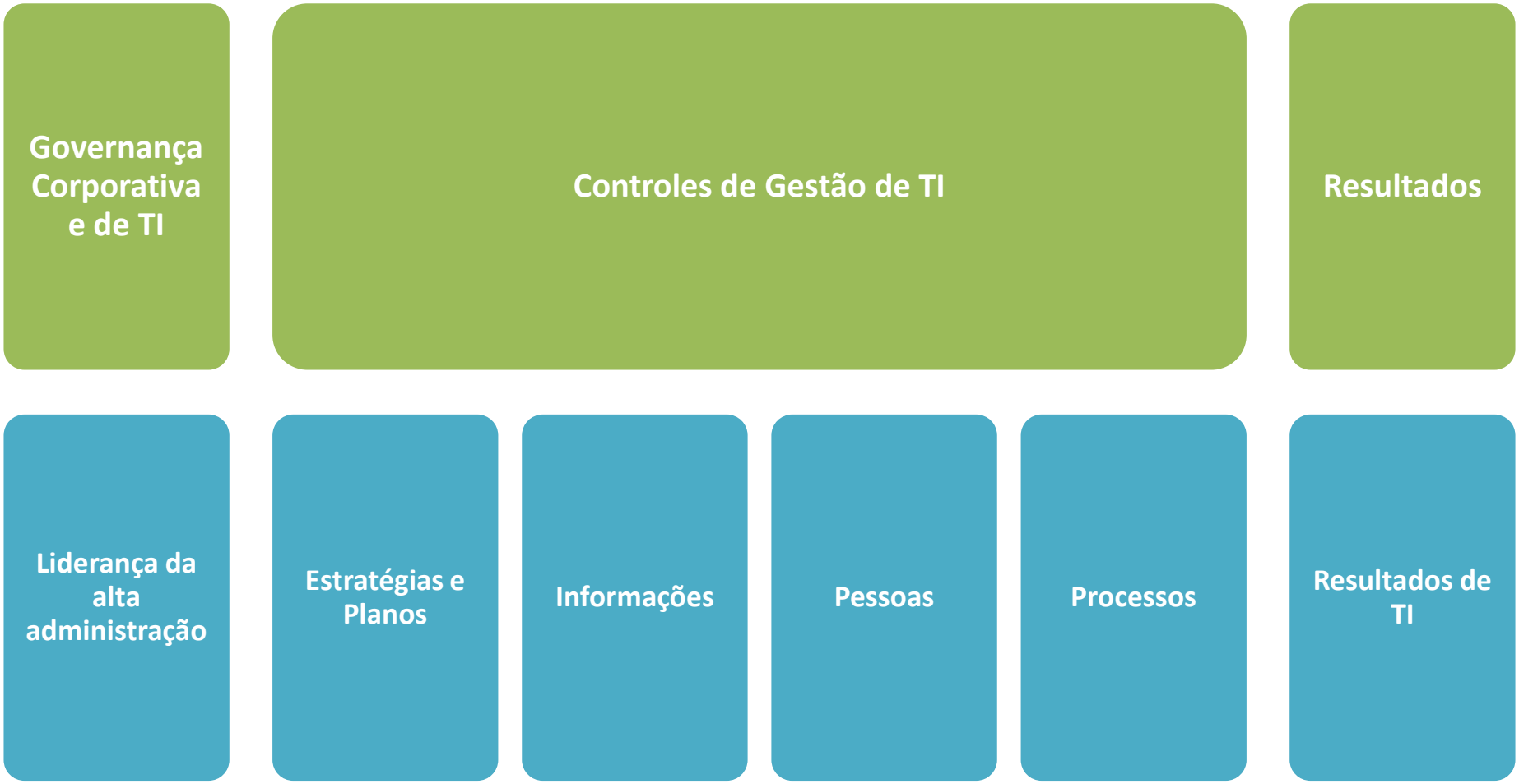
Estrutura do questionário



Estrutura do questionário



Estrutura do questionário



Estrutura do questionário

Governança Corporativa e de TI

D1 - Liderança da alta administração (37 práticas)

- Sistema de governança corporativa
- Sistema de GovTI
- Resultados de TI
- Riscos de TI
- Pessoal de TI
- Transparência
- Avaliação da TI
- Auditoria Interna

Estrutura do questionário

Controle de Gestão

D2 - Estratégias e Planos (20 práticas)		D3 – Informações (13 práticas)		D4 – Pessoas (24 práticas)		
PEI	PETI	Automação de processos	Transparência	Desenvolvimento	Desempenho	Força de Trabalho

Estrutura do questionário

Controles de Gestão

D5 – Processos (69 práticas)

- Gestão de serviços (Itil)
- Nível de serviço
- Riscos
- Segurança da informação
- Processo de software
- Projetos de TI
- Regras de contratação
- Planejamento das contratações
- Gestão de contratos
- Quadro de contratações

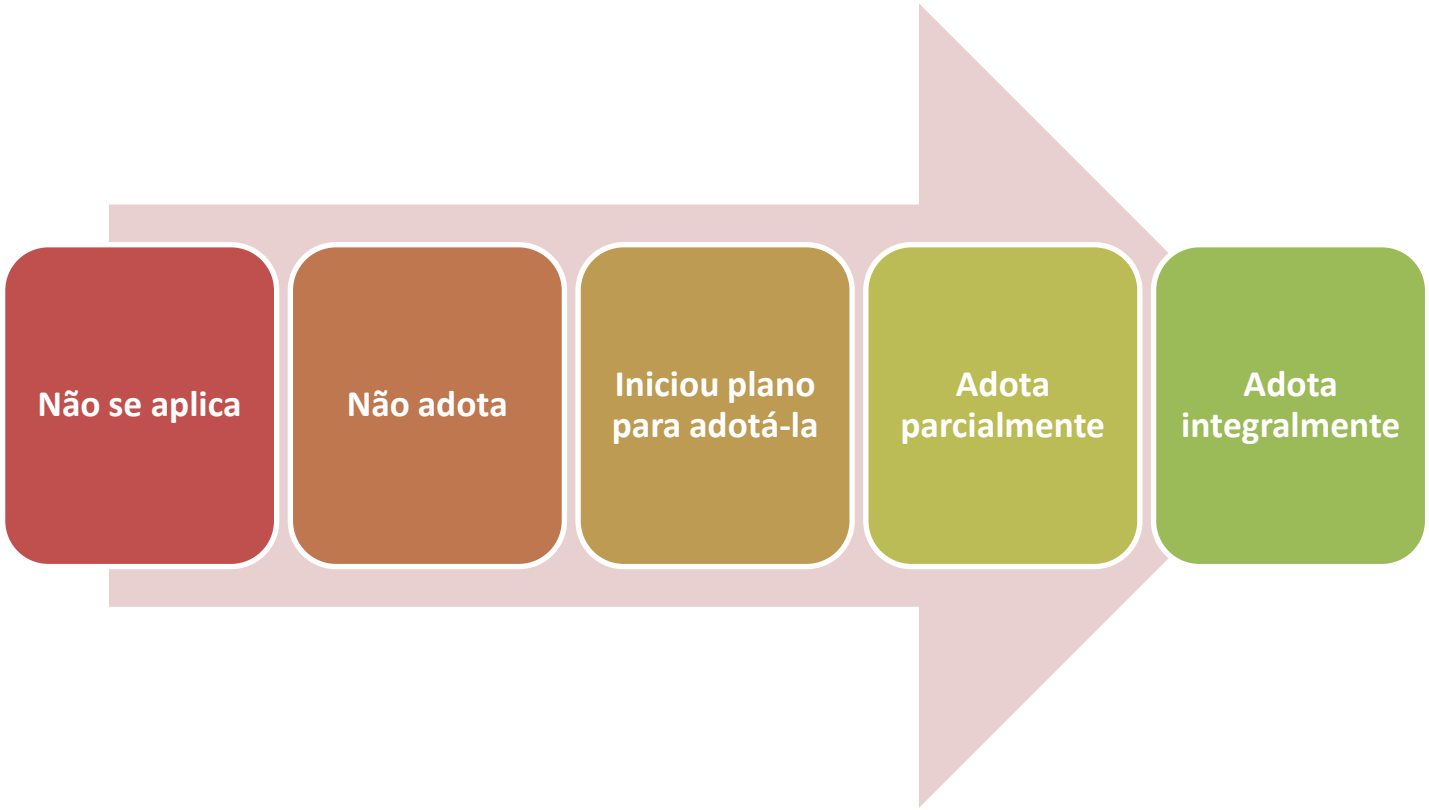
Estrutura do questionário

Resultados

D6 – Resultados de TI (6 práticas)

- Objetivos de TI
- Projetos de TI
- Serviços de TI (Internos)
- Serviços de TI (Externos)

Escala de resposta



Escala de resposta

Nível de adoção da prática	Definição
Não se aplica	A organização entende que a prática não se aplica à sua realidade, apresentando a justificativa no campo “Comentários” ao final do questionário.
Não adota	A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la.
Iniciou plano para adotá-la	A organização ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares *etc*).
Adota parcialmente	A organização iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento realizado; ou a prática não é executada uniformemente em toda a organização. Há, pelo menos, uma instância de execução da prática e os artefatos produzidos são evidências dessa execução.
Adota integralmente	A organização adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução.

Escala de resposta

1.4. Com relação aos riscos de TI:
a. a organização define **formalmente** as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto.
b. a organização define e comunica **formalmente** papéis e responsabilidades pela gestão de riscos de TI.
c. a organização define **formalmente** os níveis de risco de TI aceitáveis na consecução de seus objetivos (apetite a risco).
d. a organização toma decisões estratégicas considerando os níveis de risco de TI definidos.

Nível de adoção da prática				
Não se aplica	Não adota	Iniciou plano para adotá-la	Adota parcialmente	Adota integralmente
○	○	○	○	○

Escala de resposta

Benefícios:

1. Respostas mais representativas
2. Favorece a definição da fórmula do iGovTI
3. Não nivela por baixo as instituições
4. Menor peso para a formalização

Dificuldades:

1. Práticas em que não se aplica a escala (práticas binárias);
2. Dificuldade para definir a fronteira entre o parcial e o integral.

Práticas x Processos

Questionário 2012 - avaliava o nível de capacidade do processo

5.2. Em relação à gestão de nível de serviço de TI:

- ⦿ Não há um catálogo formal (aprovado e publicado) dos serviços de TI oferecidos aos clientes.
- ○ Há um catálogo formal e atualizado dos serviços de TI oferecidos aos clientes.
- ○ Além do item anterior, os níveis dos serviços de TI oferecidos nesse portfólio são monitorados pela área de TI.
- ○ Além do item anterior, são feitos Acordos de Nível de Serviço (ANS) formais com as áreas de negócio clientes de TI.
- ○ Além do item anterior, os ANS são monitorados e seus resultados relatados periodicamente aos clientes de TI.
- ○ Além do item anterior, os resultados do monitoramento são usados para melhorar os ANS.

Práticas x Processos

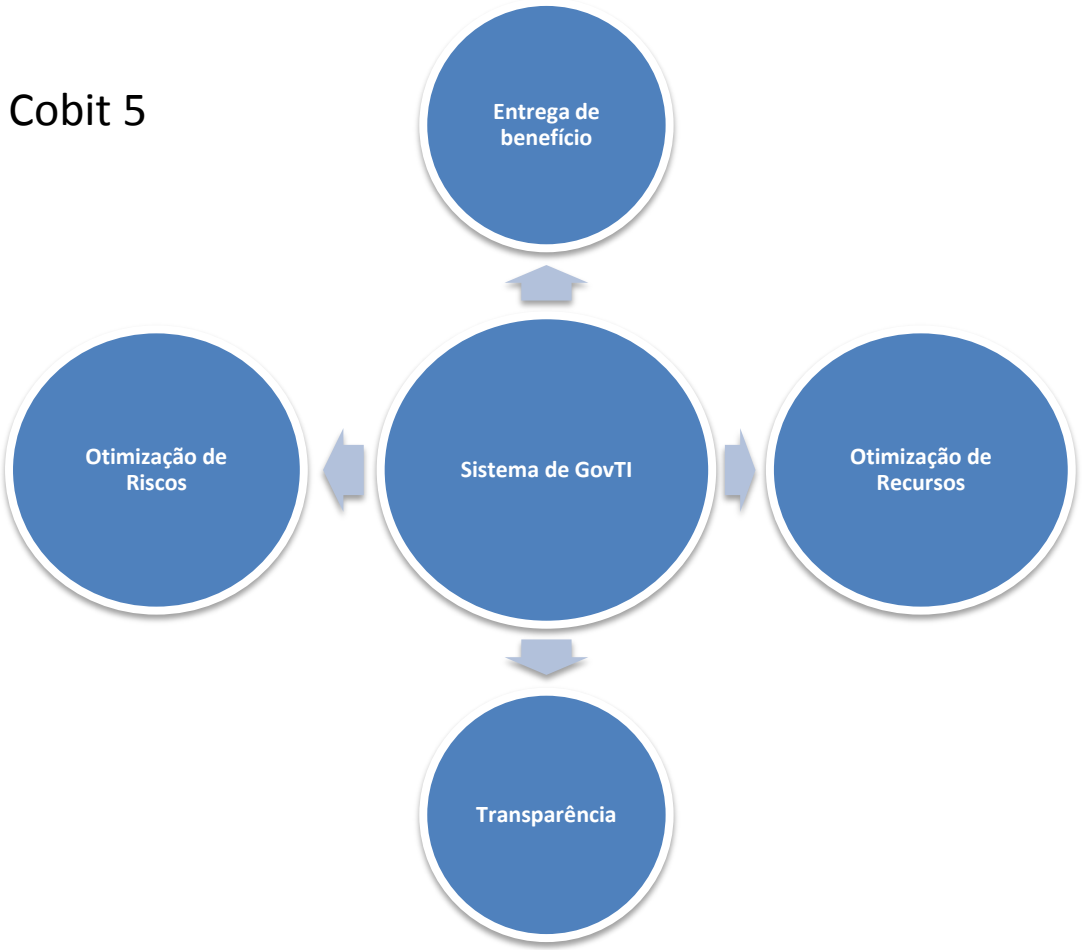
Questionário 2014 - foca as práticas adotadas e o nível de adoção

5.2. Com relação ao gerenciamento de nível de serviço de TI:
a. a organização mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes, incluindo os níveis de serviço definidos.
b. os níveis de serviço são formalmente definidos entre a área de TI e as áreas clientes (Acordo de Nível de Serviço - ANS).
c. os ANS incluem, como indicador de nível de serviço, o grau de satisfação dos usuários, apurado mediante a avaliação dos serviços de TI pelas áreas clientes.
d. a área de TI monitora o alcance dos níveis de serviço definidos e implementa ações corretivas em caso de não atendimento.
e. a área de TI comunica periodicamente o resultado desse monitoramento às áreas clientes.
f. os resultados desse monitoramento são usados para melhorar os níveis de serviço de TI.

Conteúdo

1. **Dimensão Liderança:**

   Processos de governança do Cobit 5



1. **Dimensão Liderança:**

   Lembrando: Papel da auditoria interna

1.8. Com relação à auditoria interna:	2014
a. a auditoria interna possui pessoal capacitado para avaliar a governança e a gestão de TI. Informe o quantitativo desse pessoal: _____	
b. a auditoria interna monitora **formalmente** as ações de governança e de gestão de TI.	
c. a organização aprova, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI.	
d. a auditoria interna avalia **formalmente** a gestão de riscos de TI.	
e. a auditoria interna avalia **formalmente** os riscos considerados críticos para o negócio e a eficácia dos respectivos controles.	
f. a auditoria interna avalia **formalmente** as respostas apresentadas aos questionários dos Levantamentos de Governança de TI realizados pelo TCU.	

2. **Dimensão Estratégias e Planos:**

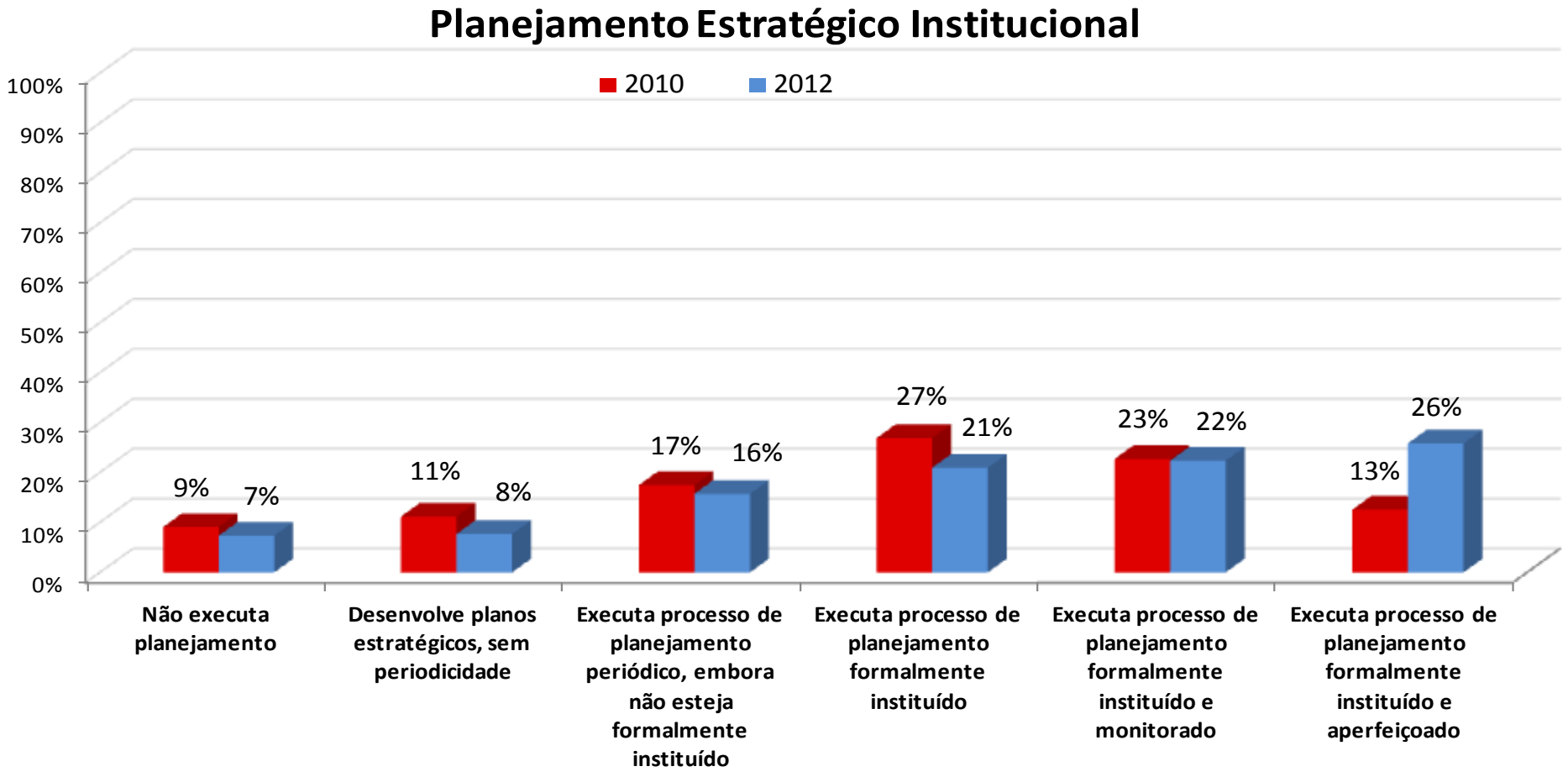
- Processo X Plano Vigente

Vejamos o que ocorreu em 2012:

2.1 Em relação ao processo de planejamento estratégico institucional, marque a opção que melhor descreve a sua instituição:

- ◉ a instituição não executa um processo de planejamento estratégico institucional.
- ○ a instituição desenvolve planos estratégicos, mas não de maneira periódica.
- ○ a instituição executa um processo periódico de planejamento, embora este não esteja formalmente instituído.
- ○ o processo de planejamento estratégico institucional é formalmente (aprovado e publicado) instituído.
- ○ o processo de planejamento estratégico institucional formal é acompanhado segundo indicadores e metas estabelecidos.
- ○ o processo de planejamento estratégico institucional formal é aperfeiçoado continuamente com base na análise de seus indicadores.

Efeitos


Planejamento Estratégico Institucional
2010
2012
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
9%
7%
11%
8%
17%
16%
27%
21%
23%
22%
13%
26%
Não executa planejamento
Desenvolve planos estratégicos, sem periodicidade
Executa processo de planejamento periódico, embora não esteja formalmente instituído
Executa processo de planejamento formalmente instituído
Executa processo de planejamento formalmente instituído e monitorado
Executa processo de planejamento formalmente instituído e aperfeiçoado

2.1. Com relação ao planejamento estratégico institucional:	2014
Processo	
a. a organização executa periodicamente **processo** de planejamento estratégico institucional.	
b. o **processo** de planejamento estratégico institucional prevê a participação das áreas mais relevantes da organização.	
c. o **processo** de planejamento estratégico institucional prevê a participação da área de TI.	
d. o **processo** de planejamento estratégico institucional está **formalmente** instituído.	
Plano Vigente	
e. a organização possui **plano** estratégico institucional **vigente**, formalmente instituído (aprovado e publicado) pelo dirigente máximo da organização.	
f. o **plano** estratégico institucional **vigente** contém pelo menos um indicador de resultado para quantificar o cumprimento de cada objetivo estratégico estabelecido.	
g. o **plano** estratégico institucional **vigente** contém metas de curto, médio e longo prazos, associadas aos indicadores de resultado.	
h. o **plano** estratégico institucional **vigente** estabelece os projetos e ações considerados necessários e suficientes para o alcance das metas fixadas.	
i. a execução do **plano** estratégico institucional **vigente** é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.	
j. o **plano** estratégico institucional **vigente** está publicado na internet para acesso livre. Informe a URL (completa): _____	

2.2. Com relação ao planejamento de tecnologia de informação:	2014
Processo	
a. a organização executa periodicamente **processo** de planejamento de TI.	
b. o **processo** de planejamento de TI prevê a participação das áreas mais relevantes da organização.	
c. o **processo** de planejamento de TI prevê o apoio do comitê de TI.	
d. o **processo** de planejamento de TI está **formalmente** instituído.	
Plano Vigente	
e. a organização possui **plano** de TI **vigente**, **formalmente** instituído pelo seu dirigente máximo.	
f. o **plano** de TI **vigente** contempla objetivos, indicadores e metas para a TI, com os objetivos explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional.	
g. o **plano** de TI **vigente** contém alocação de recursos (orçamentários, humanos e materiais) e estratégia de execução indireta (terceirização).	
h. a execução do **plano** de TI **vigente** é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.	
i. o **plano** de TI **vigente** vincula as ações (atividades e projetos) a indicadores e metas de negócio.	
j. o **plano** de TI **vigente** fundamenta a proposta orçamentária de TI.	

3. Dimensão Informação

- Transparência da gestão e uso de TI

2014

3.2. Com relação à transparência das informações relacionadas à gestão e uso de TI:
a. os planos de TI vigentes são divulgados na internet, sendo **facilmente** acessados.
b. as informações sobre o alcance dos objetivos de TI planejados são divulgados na internet, sendo **facilmente** acessadas.
c. as informações sobre o acompanhamento das ações e dos projetos de TI são divulgadas na internet, sendo **facilmente** acessadas.
d. os editais, seus respectivos, anexos e os resultados das licitações de TI (inteiro teor) são divulgados na internet, sendo **facilmente** acessados.
e. os estudos técnicos preliminares (inteiro teor) são divulgados na internet, juntamente com os editais de licitação de TI, sendo **facilmente** acessados.
f. os contratos de TI e os respectivos aditivos (inteiro teor) são divulgados na internet, sendo **facilmente** acessados.
g. a execução orçamentária de TI, ao longo do exercício, é divulgada na internet, sendo **facilmente** acessada.
h. as respostas aos questionários dos levantamentos de governança de TI realizados pelo TCU, bem como os respectivos relatórios de *feedback*, são divulgados na internet, sendo **facilmente** acessados.

Conteúdo

4. Dimensão Pessoas

Poucas alterações

4.2. Com relação ao desempenho do pessoal de TI:
a. a organização estabelece metas de desempenho para o pessoal de TI.
b. a organização avalia periodicamente o desempenho do pessoal de TI.
c. a organização estabelece benefício, financeiro ou não, em função do desempenho alcançado pelo pessoal de TI.

Nível de adoção da prática				
Não se aplica	Não adota	Iniciou plano para adotá-la	Adota parcialmente	Adota integralmente
○	○	○	○	○

5. Dimensão Processos

- Gerenciamento de serviços de TI

5.1. Informe os processos de gerenciamento de serviços de TI implementados formalmente pela organização: Obs.: conceitos baseados na biblioteca ITIL v.3
Desenho de serviço
a. processo de gerenciamento do catálogo de serviços
b. processo de gerenciamento da continuidade dos serviços de TI
Transição de serviço
c. processo de gerenciamento de mudanças
d. processo de gerenciamento de configuração e ativos
e. processo de gerenciamento de liberação e implantação
Operação de serviço
f. processo de gerenciamento de incidentes
g. processo de gerenciamento de problemas

5. Dimensão Processos

- Gestão de Riscos de TI

5.3. Com relação à gestão de riscos de TI:
a. a organização identifica os riscos de TI que podem afetar a realização de seus objetivos, bem como suas causas e suas consequências potenciais.
b. a organização avalia os riscos de TI em função da relevância para o negócio.
c. a organização trata os riscos de TI com base em um plano de tratamento de risco.
d. a organização **formalizou** um processo de gestão de riscos de TI.

Nível de adoção da prática				
Não se aplica	Não adota	Iniciou plano para adotá-la	Adota parcialmente	Adota integralmente
○	○	○	○	○

Conteúdo

6. Dimensão Resultados:

- Resultados de TI

1.1. **Com relação aos principais serviços de TI que sustentam as atividades da organização, informe:**

Nome do Serviço de TI	Principal indicador de nível do serviço	Meta prevista em 2013	Resultado apurado em 2013 (se não medido, indique "não medido")
1.			%
2.			%
3.			%
4.			%
5.			%

Apoio ao Questionário

- **Glossário**

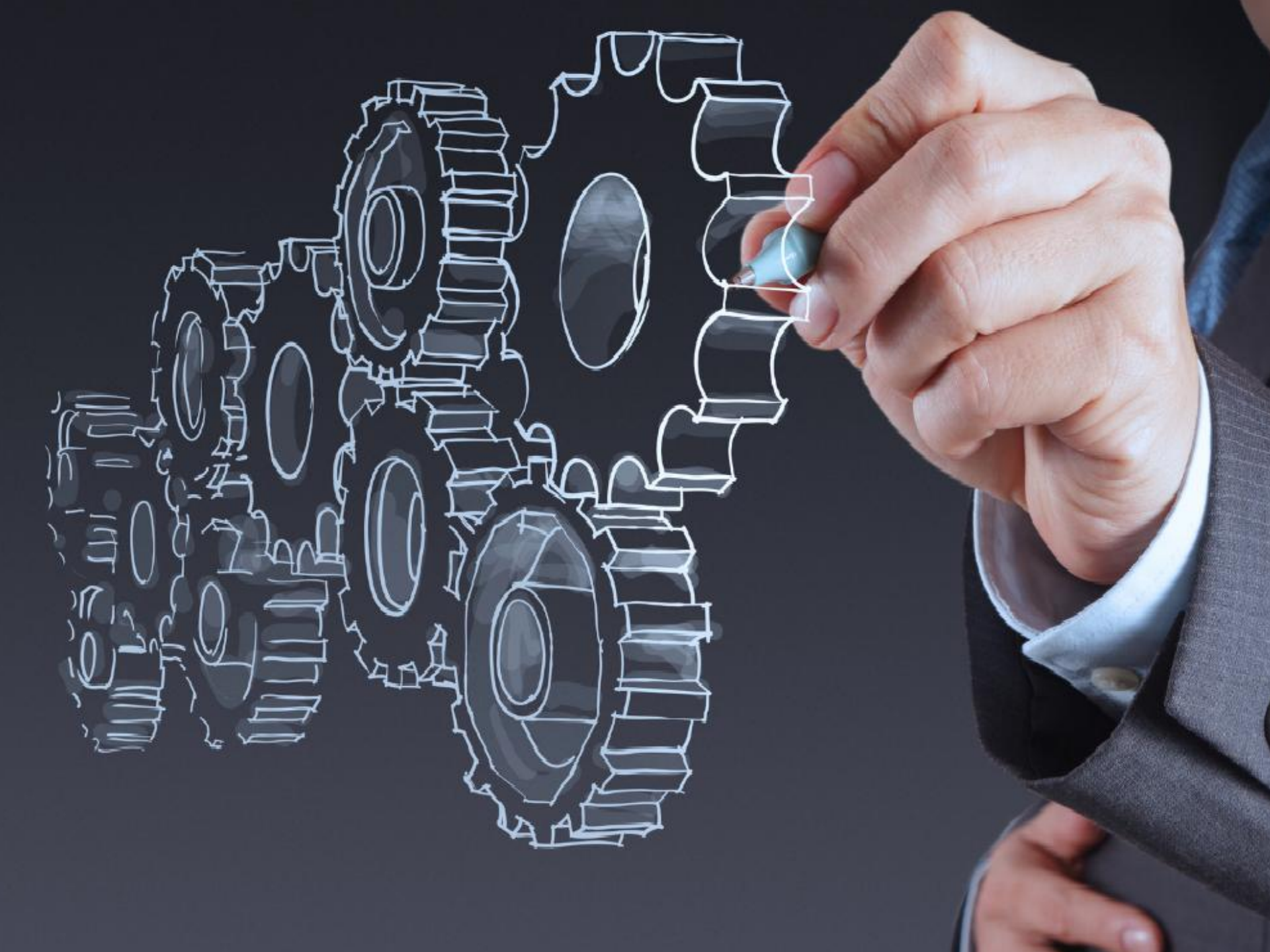
Definição de termos abordados no questionário

- **FAQ**

Perguntas e respostas mais frequentes atualizado a cada dúvida recebida

- **Referências**
  - Balizam as práticas exploradas no questionário
  - Buscam auxiliar as organizações em suas respostas
  - Apontam para
    - Leis
    - Decretos
    - Resoluções
    - Instruções Normativas
    - Jurisprudência do TCU
    - Normas Técnicas
    - Modelos de boas práticas de governança de TI
    - Modelos de boas práticas de governança corporativa
    - Outros
    - Mais alguns


Referência
Orientação



Finis!

Daniel Jezini Netto, CISA
TCU/Sefti
Brasília/DF, 8 de maio de 2014