I Workshop de Governança de TI
Embrapa, 30/08 a 03/09/2010

Governança de TI

Cláudio Silva da Cruz

MSc, CGEIT, Auditor Federal de Controle Externo/TCU

As ideias relacionadas neste trabalho são interpretações do autor com base na legislação, doutrina e jurisprudência; não há garantia de que as instâncias de controle (consultoria jurídica, controle interno e controle externo) adotem necessariamente essas posições; a fundamentação das ideias apresentadas é um referencial para o posicionamento dos dirigentes.

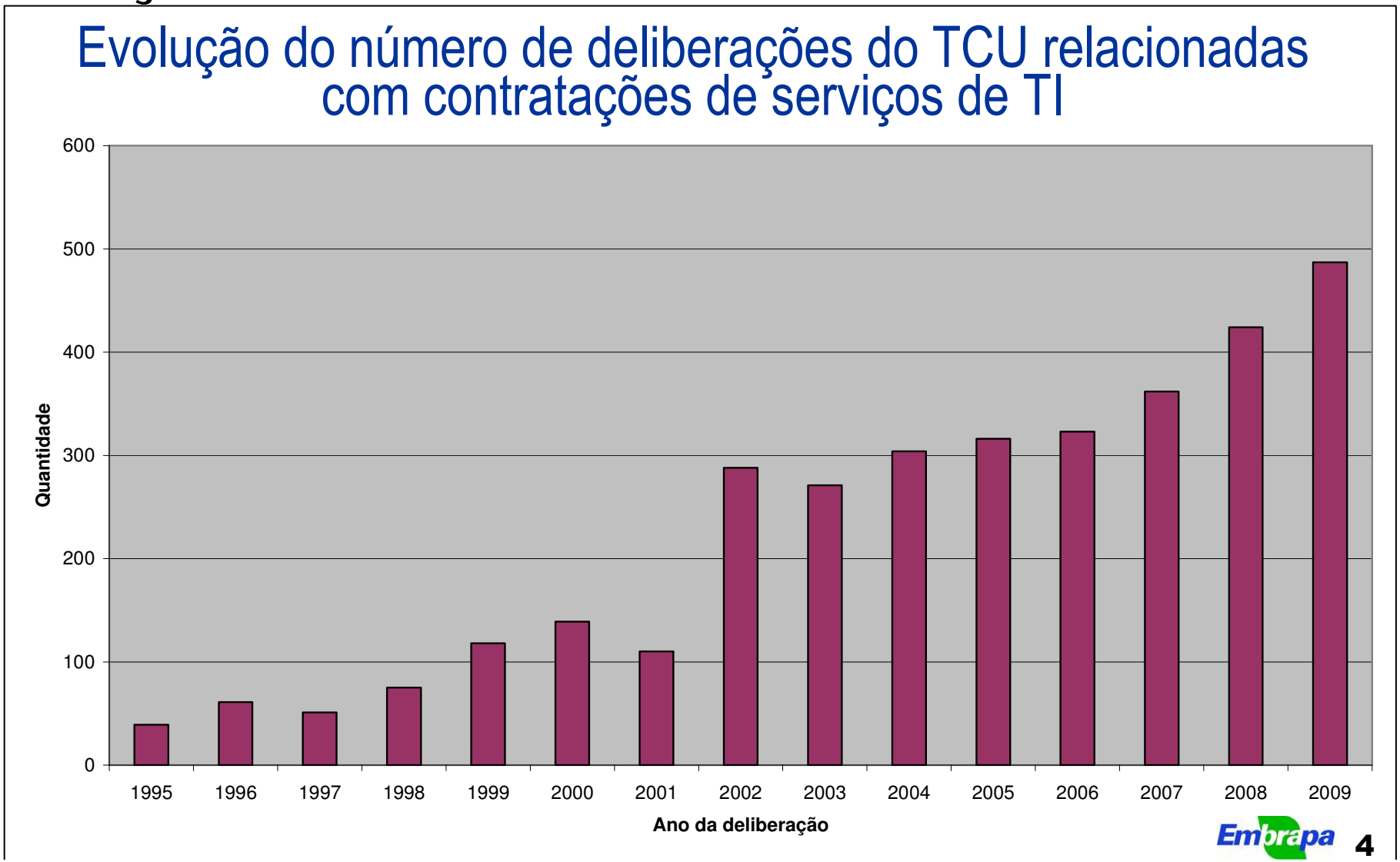
Impactos da ausência de Governança de TI

O problema

- Congresso Nacional (1999-2000): solicitação de apuração de denúncias de fraudes em contratações de TI
- TCU (2001-2002)
  - Exame de informações de mais de 79.000 contratos de TI
  - Entre 1995 e 2000 foram gastos **R$15 bilhões** em TI por inexigibilidade de licitação
  - **TI passou a ser foco de auditorias**
- Possível origem do problema:
  - achar que TI não é o negócio e que se pode terceirizar tudo: perda da capacidade de Governança de TI

O problema

- Problemas recorrentes nas contratações de serviços de TI



Evidências de falta de Governança de TI

- Ausência de posse/domínio de seus sistemas e bases de dados: Acórdão 2.203/2005-Plenário

"**Documentação técnica e programas fontes não estão disponíveis para a Administração Pública** e, por mais absurdo que possa parecer, **ela não tem acesso aos dados gerados por esses sistemas**, a não ser da forma como a dita empresa oferece. Ademais, atualmente é **impossível para a Administração Pública auditar esses dados**, para verificar se são fidedignos ou buscar indícios de fraudes. A [contratada] condiciona sua entrega, bem como da documentação técnica dos sistemas, à assinatura de um Termo de Ajuste, objeto de pendência judicial que se arrasta há mais de um ano, numa verdadeira afronta à soberania nacional."

Evidência de falta de Governança de TI

- Completa dependência tecnológica: Acórdão 889/2007-Plenário

"Tal providência, de inserção nos contratos de manutenção a serem celebrados, de cláusula que possibilite a migração dos dados, de propriedade do [ente público] para base de padrão aberto reconhecida por outros softwares, **obviamente depende de negociação junto à empresa [contratada] e do seu interesse em prestar o serviço, especialmente se esse processo migratório depender dos conhecimentos exclusivos dessa empresa** sobre o sistema, ..."

"... não compartilhados por outras empresas ou profissionais de informática. **Tal providência, em verdade, deveria ter sido adotada desde a licitação realizada para a aquisição do sistema, época em que ainda não havia qualquer dependência** do [ente público] junto ao fornecedor da solução pretendida."

Evidência de falta de Governança de TI

- Ações paralelas, sem coordenação: TC 022.059/2008-0

"A deficiência da área de governança de TI aparece também por conta do desdobramento do projeto [...], oriundo de aditivo ao Contrato [...]."

"De acordo com a [Comissão], existe outro projeto em desenvolvimento [em outro setor do ente público], chamado Sistema [...], que teria a mesma finalidade do projeto [acima]. "

"Em reunião com a Assessoria [...], levantou-se que, embora haja certa diferença com relação à abrangência dos dois projetos, há uma superposição entre os mesmos, com relação a finalidades e a informações que devem ser encaminhadas [...]."

"Registra-se que esta equipe de auditoria não chegou a avaliar a congruência entre os dois projetos citados e outros atualmente em desenvolvimento na instituição, e que podem também conter ações paralelas, como o Sistema [...] e o Sistema [...]."

Evidência de falta de Governança de TI

- Sistema contratado, pago, mas inservível: TC 031.963/2008-0

"O edital e o projeto básico não possuíam indicadores de qualidade, acordos de níveis de serviço ou parâmetros de performance que permitisse que o [ente público] atuasse junto à contratada com relação a eventuais problemas de funcionamento."

"O processo de homologação adotado pelo [ente público] durante o desenvolvimento do [sistema] estava focado basicamente na usabilidade (do ponto de vista do usuário) e no aceite dos casos de uso individualmente, carecendo de um viés técnico que permitisse a identificação antecipada de inconsistências e problemas de funcionamento e performance para a solução integrada."

"O produto entregue pela [contratada] apresentou problemas de funcionamento, os quais foram identificados desde 2004 e também apontados após a entrega da solução completa em 2007. Os problemas de funcionamento foram também identificados no treinamento dos multiplicadores (setembro/2006) e na implantação piloto (julho/2007)."

Evidência de falta de Governança de TI

- Sistema contratado, pago, servível, mas não implantado
  Acórdão 2.203/2005-Plenário

"Um exemplo real constatado nesta auditoria concernente à **falta de planejamento** foi o desenvolvimento do sistema (...). Trata-se de sistema desenvolvido entre 2000 e 2001 e que, até os dias atuais, **não foi implantado, embora já tenham sido feitos vários testes satisfatórios e o gestor do negócio ache de extrema relevância** (...) o problema da não implantação do [sistema] está relacionado à **falta de infra-estrutura** necessária que comporte a execução desse sistema: infra-estrutura de rede, servidores ..."

Evidência de falta de Governança de TI

- Ausência de PCN (Plano de Continuidade do Negócio):
  TC 026.196/2007-9 e TC 026.200/2007-3

"Convivendo com total falta de recursos ou planos de contingência, a atual Diretoria [...] foi alarmada pela ocorrência do dia 19/07/2005, quando uma falha nos equipamentos de processamento centralizado provocou a **paralisação** [da entidade] **por mais de 20 horas, gerando danos à imagem e causando prejuízos financeiros à instituição**."
(TC 026.196/2007-9)

"Obteve-se a informação que, devido a um vírus, **houve uma paralisação na rede** [...] **por mais de duas semanas**, o que comprova que o Plano de Contingência [...] remetido [...] não tem aplicabilidade efetiva."
(TC 026.200/2007-3)

Será que as causas desses problemas estão somente na área de TI? ...

... Não! Trata-se de um problema sistêmico de ausência de governo do uso e da gestão de TI

Se os resultados advém da estratégia de ação ...

... então precisamos de gestores da estratégia de ação, pois, quem faz a estratégia funcionar é a área de negócio e, não, a área de TI.

Unidade de negócio

(unidade gestora)

Gestor de negócio (titular)

Papéis do gestor do negócio

- gestor de estratégia de negócio
- gestor de pessoas alocadas
- gestor de processos de negócio
- **gestor de tecnologias aplicadas**

Nesse sentido, como anda a Governança de TI no setor público?

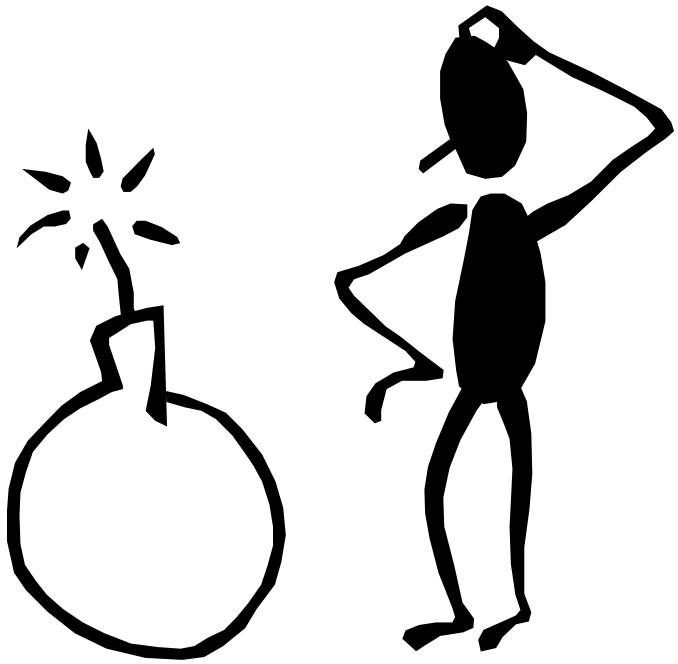
Importância de governar a TI do setor público

O problema

- Governo é grande contratador de TI
  - Em 2004, ~23% do mercado de outsourcing de TI
    (E-Consulting apud GONÇALVES; OLIVEIRA, 2004)
  - Em 2007, gastos com TI: R$ 6Bi
    (Ac1934/2007-P, primeira aproximação, sem detalhes)
  - Em 2010, TI gastará: (Fonte: SIDOR/DEST, 2010)
    - R$ 6,1Bi no orçamento fiscal e da seguridade social
    - R$ 6,4Bi em investimentos nas estatais/economia mista
    - Total: R$ 12,5Bilhões

O problema

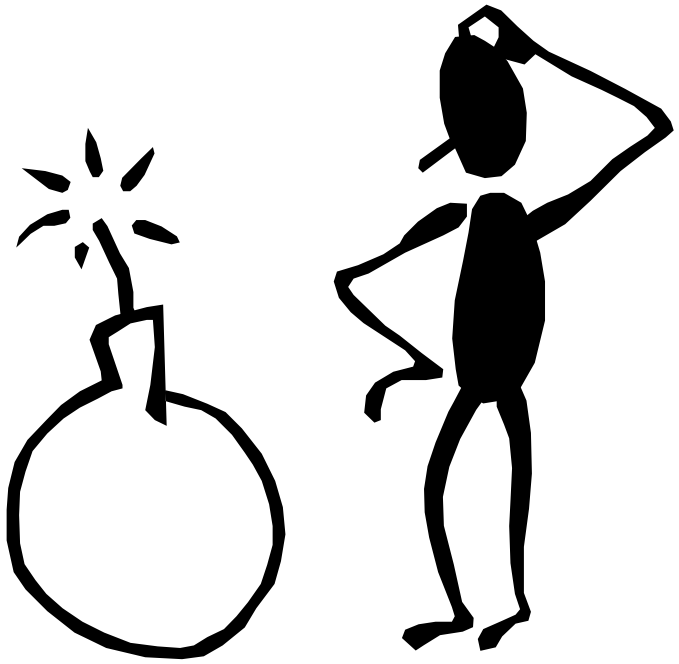
- Mas o que mais preocupa é que a TI.Gov ...
  ... implementa/controla/suporta (ou deveria) a execução do orçamento da União:
  R$ 1,86 TRILHÃO!!!



Temos Governança de TI para fazer isso?

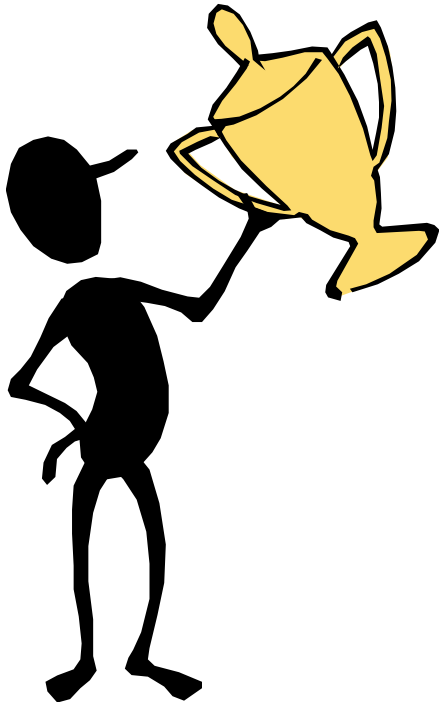
O problema

- Estamos usando TI com eficácia, eficiência, efetividade e economicidade?
- Os resultados atuais do uso de TI são satisfatórios ...
  ... OU PODEMOS OBTER MUITO MAIS?



Como obter mais resultados do uso de TI na Embrapa? ...

... adotando as diretrizes da norma ISO/IEC 38500



A norma ABNT NBR ISO/IEC 38500

Escopo da NBR ISO/IEC 38500

- NBR ISO/IEC 38500:
  - Esta norma oferece princípios para orientar os **dirigentes máximos** das organizações sobre o uso eficaz, eficiente e aceitável da TI mas suas organizações
  - Aplicação geral:
    - Organizações privadas
    - Organizações públicas
    - Entidades governamentais
    - Organizações sem fins lucrativos
    - ... de qualquer tamanho

Benefícios da NBR ISO/IEC 38500

- Gerais:
  - Uso eficaz, eficiente e aceitável da TI
  - Melhor avaliação dos dirigentes acerca dos riscos e oportunidades de uso de TI
- Conformidade:
  - Redução do risco de não-conformidades legais, regulatórias e contratuais
  - Redução dos riscos decorrentes de falta de conformidade com:
    - Normas de segurança, legislação de privacidade, legislação comercial, propriedade intelectual, regulamentos ambientais e trabalhistas, normas públicas de licitações e contratos, políticas públicas, normas contábeis etc.
- Desempenho:
  - Melhoria do desempenho institucional por meio do uso de TI
  - Continuidade e sustentabilidade do negócio
  - Alocação eficiente de recursos
  - Competitividade
  - Obtenção dos benefícios de investimentos de TI etc.

Princípios para Governança de TI

- ISO/IEC 38500: seis princípios para governança de TI:
  - Responsabilidade
  - Estratégia
  - Aquisições
  - Desempenho
  - Conformidade
  - Comportamento Humano

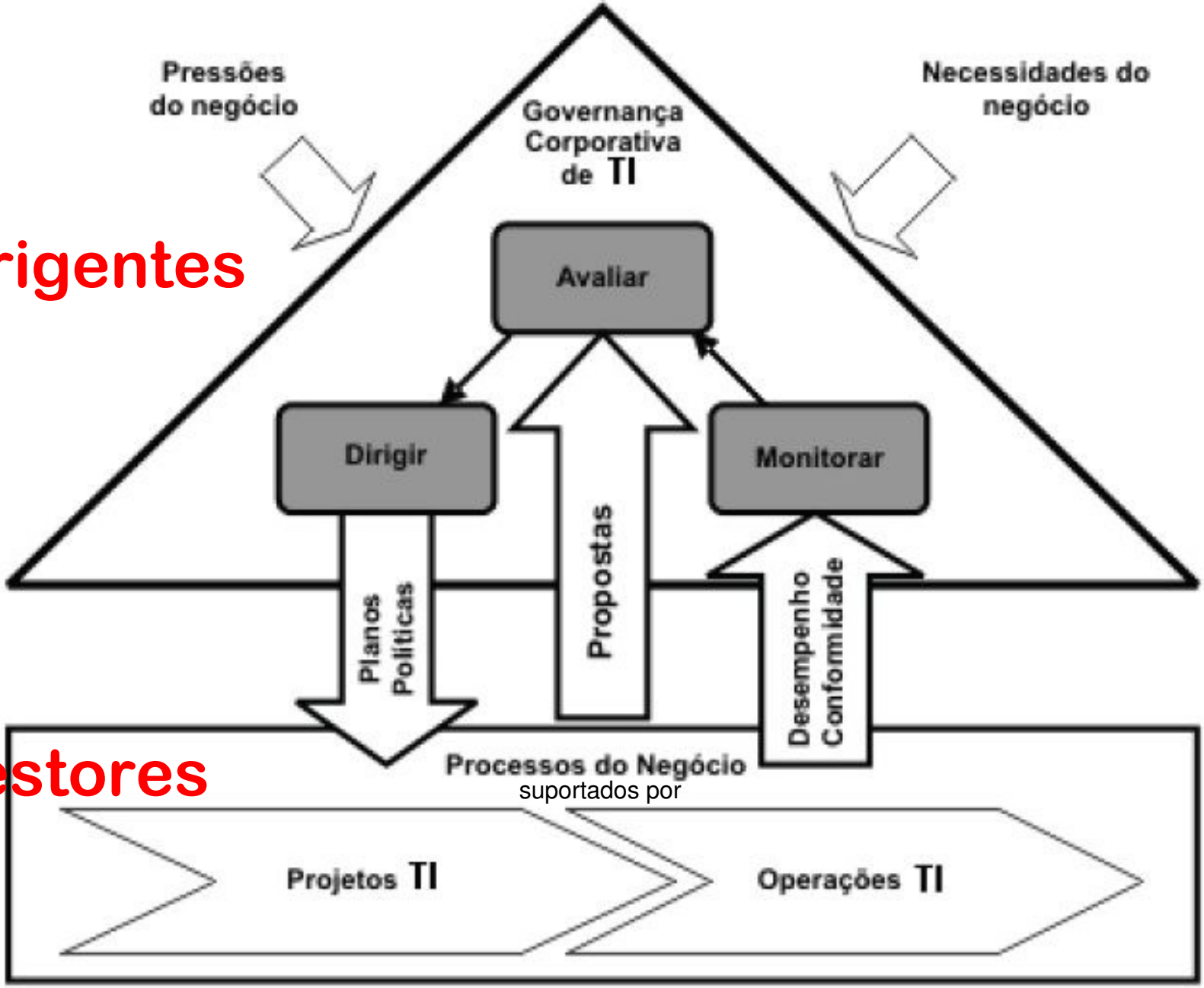
Princípios de Governança de TI

- ISO/IEC 38500: seis princípios para governança de TI:
  1. **Responsabilidade** – papéis e responsabilidades bem definidos na entrega de TI aos clientes e na sua aquisição, e garantia de autoridade compatível para o exercício desses papéis.
  2. **Estratégia** – O desenvolvimento da estratégia de negócio considera a as capacidades atuais e futuras de TI e o planejamento de TI busca atender às necessidades atuais e continuadas do negócio da organização (alinhamento).
  3. **Aquisições** – As aquisições de TI são adequadamente motivadas por meio de análises apropriadas e continuadas e de decisões claras e transparentes, de modo a garantir o alcance de equilíbrio adequado entre benefícios, oportunidades, custos e riscos, tanto no curto como no longo prazo.
  4. **Desempenho** – A TI é estruturada para suportar adequadamente a organização e dispor serviços com os níveis e com a qualidade necessários para responder aos requisitos atuais e futuros do negócio.
  5. **Conformidade** – A TI está em conformidade com a legislação e regulamentos aplicáveis. As políticas e as práticas estão claramente definidas, encontram-se implementadas e são aplicadas.
  6. **Comportamento Humano** – As políticas, práticas e decisões relativas ao uso e gestão da TI consideram e respeitam o comportamento humano e incluem as necessidades atuais e a evolução das necessidades de todas as pessoas envolvidas no processo.

Tarefas da AA para governar a TI

- Para implementar esses princípios e, portanto, governar a TI, a alta administração (AA) da organização precisa:
  - **Avaliar** o uso atual e futuro da TI;
  - **Dirigir** a elaboração e implementação de políticas e planos que assegurem que o uso e a gestão de TI atingem os objetivos de negócio;
  - **Monitorar** a conformidade com as políticas estabelecidas e o desempenho da execução dos planos traçados.
- As três tarefas devem ser realizadas para atender a cada um dos seis princípios

Modelo de Governança da NBR38500



Exemplo:
A governança nas contratações de serviços de TI

Requisito legal para contratar serviços

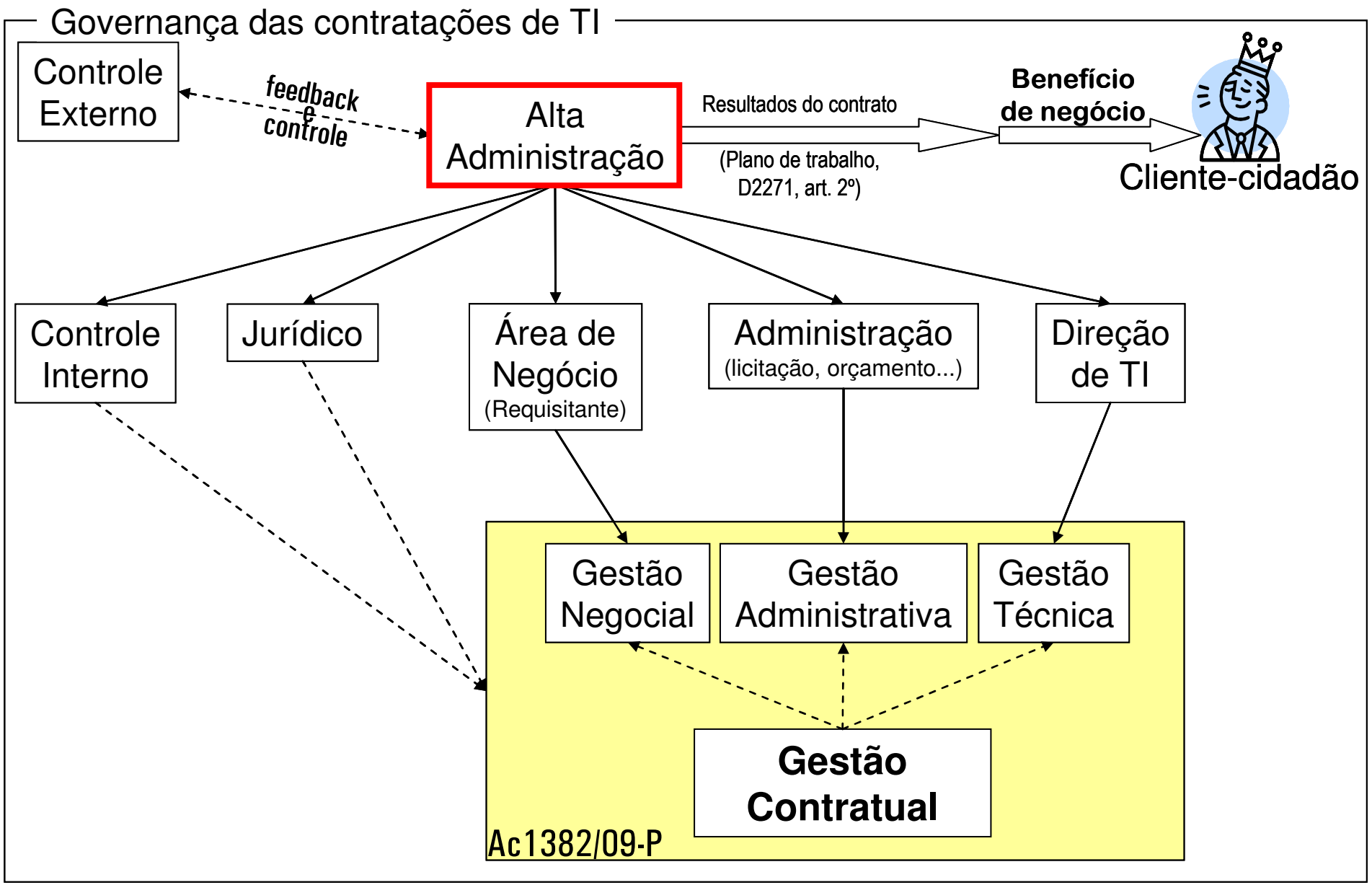
Dec. 2271/1997, art . 2º A contratação deverá ser precedida e instruída com plano de trabalho aprovado pela **autoridade máxima** do órgão ou entidade, ou a quem esta delegar competência, e que conterá, no mínimo:

I - justificativa da **necessidade** dos serviços;

II - relação entre a demanda prevista e a quantidade de serviço a ser contratada;

III - demonstrativo de **resultados** a serem alcançados em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais ou financeiros disponíveis.

A governança das contratações



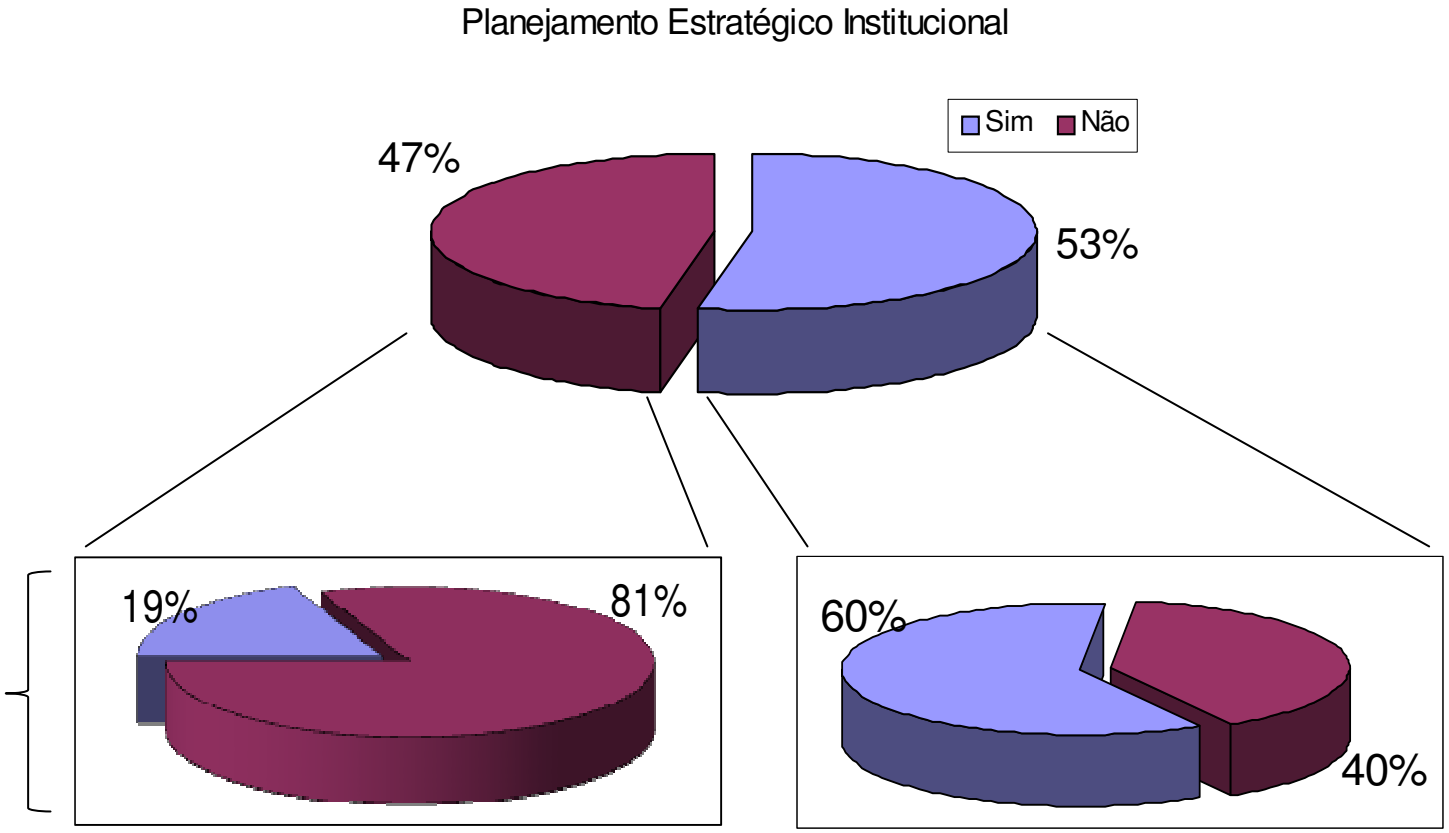
TCU:
Como anda a Governança de TI no setor público?

Levantamento GovTI/2007

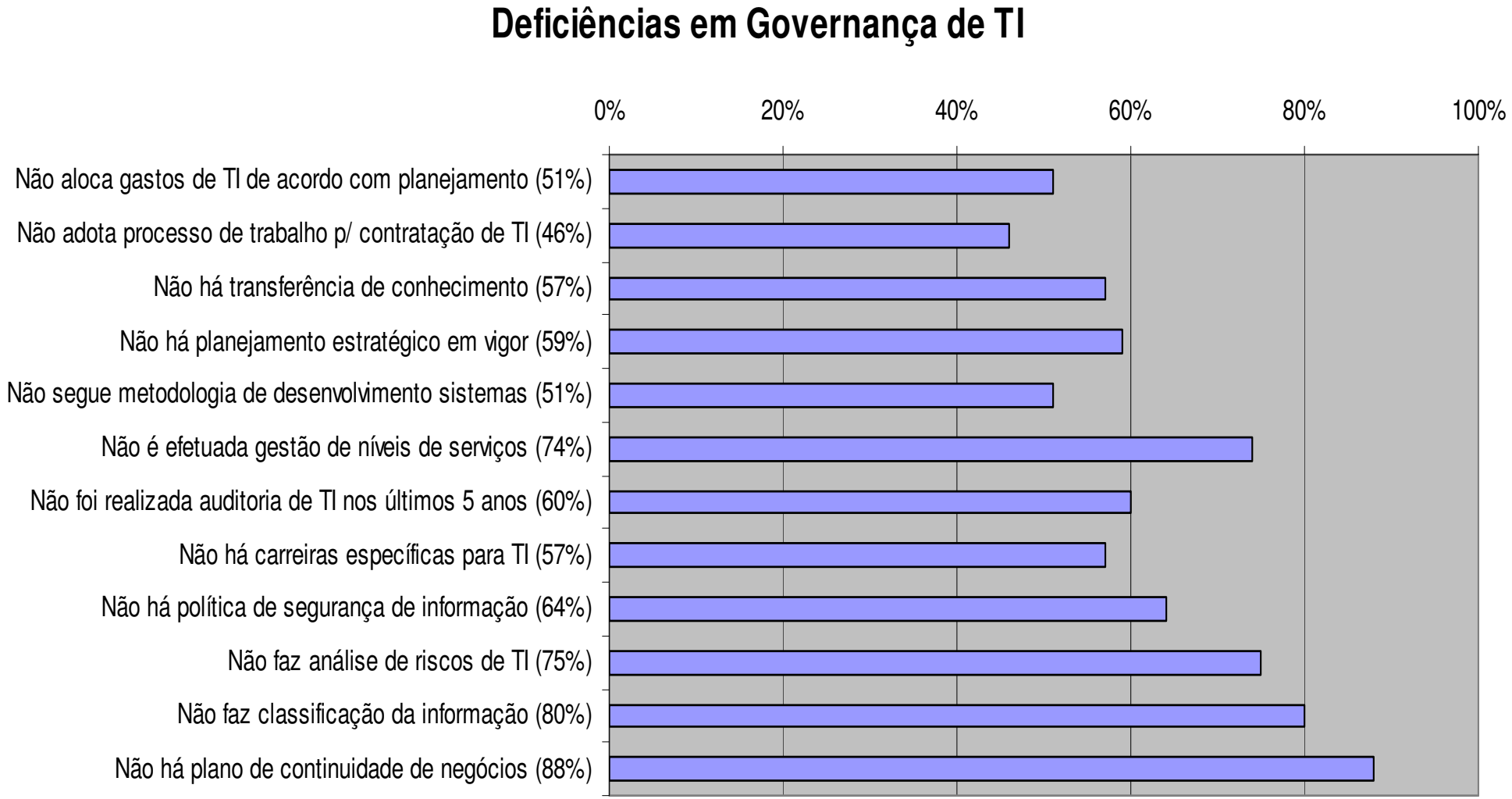
- Etapas do trabalho:
  - ✓ Elaboração de questionário (**39 questões**).
  - ✓ Identificação do público alvo (**255 órgãos/entidades** da APF).
  - ✓ Identificação dos responsáveis pela resposta.
  - ✓ Utilização de software para coleta das respostas.
  - ✓ Resposta à pesquisa (**respostas declarativas, com anexação de evidências**).
  - ✓ Suporte ao processo de resposta dos questionários.
  - ✓ Encerramento da pesquisa.
  - ✓ Avaliação dos dados coletados.

Levantamento GovTI/2007

- Relação entre Plano Estratégico Institucional e Plano Estratégico de TI (PETI):

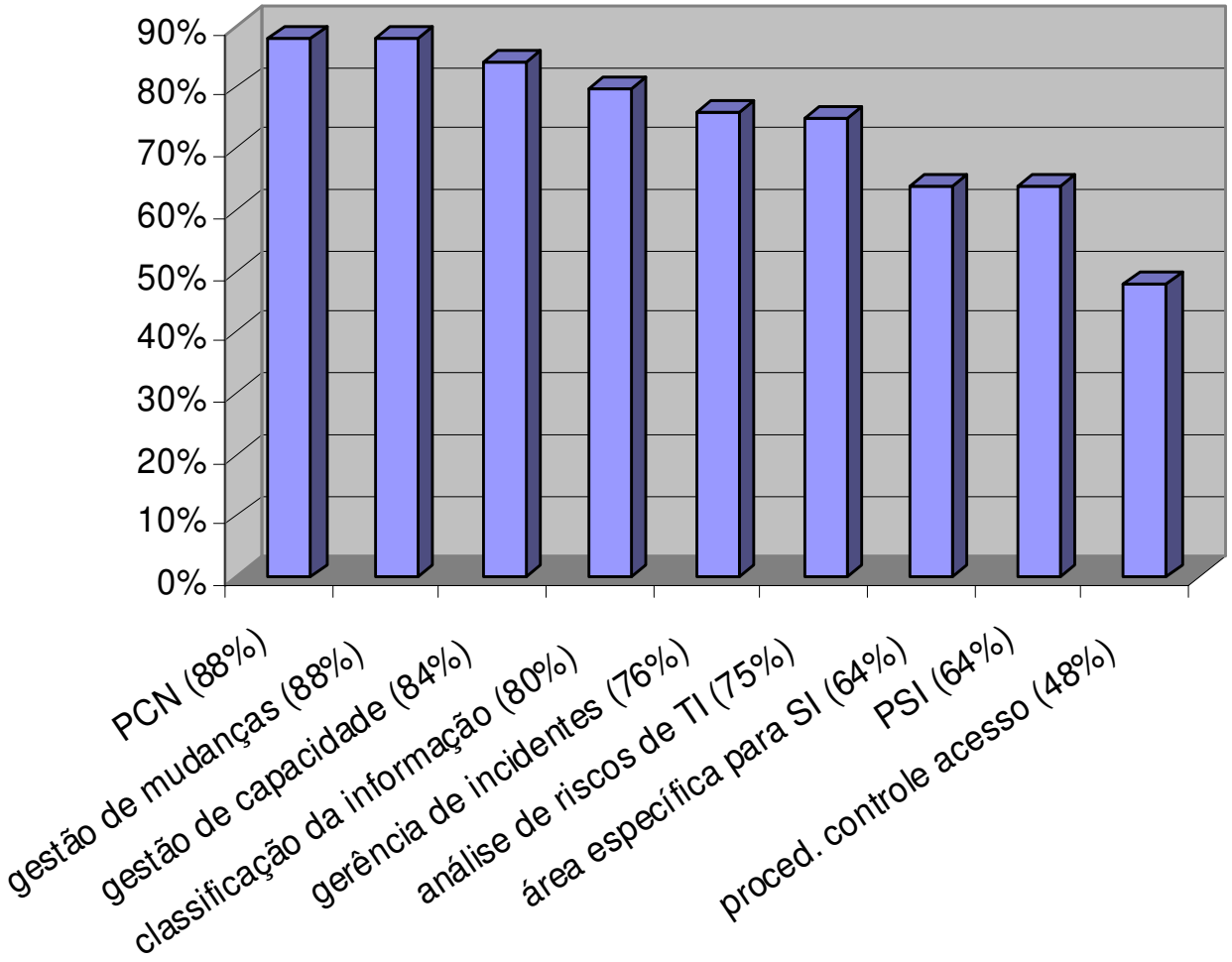


Levantamento GovTI/2007



Levantamento GovTI/2007

Deficiências na segurança da informação



Levantamento GovTI/2007

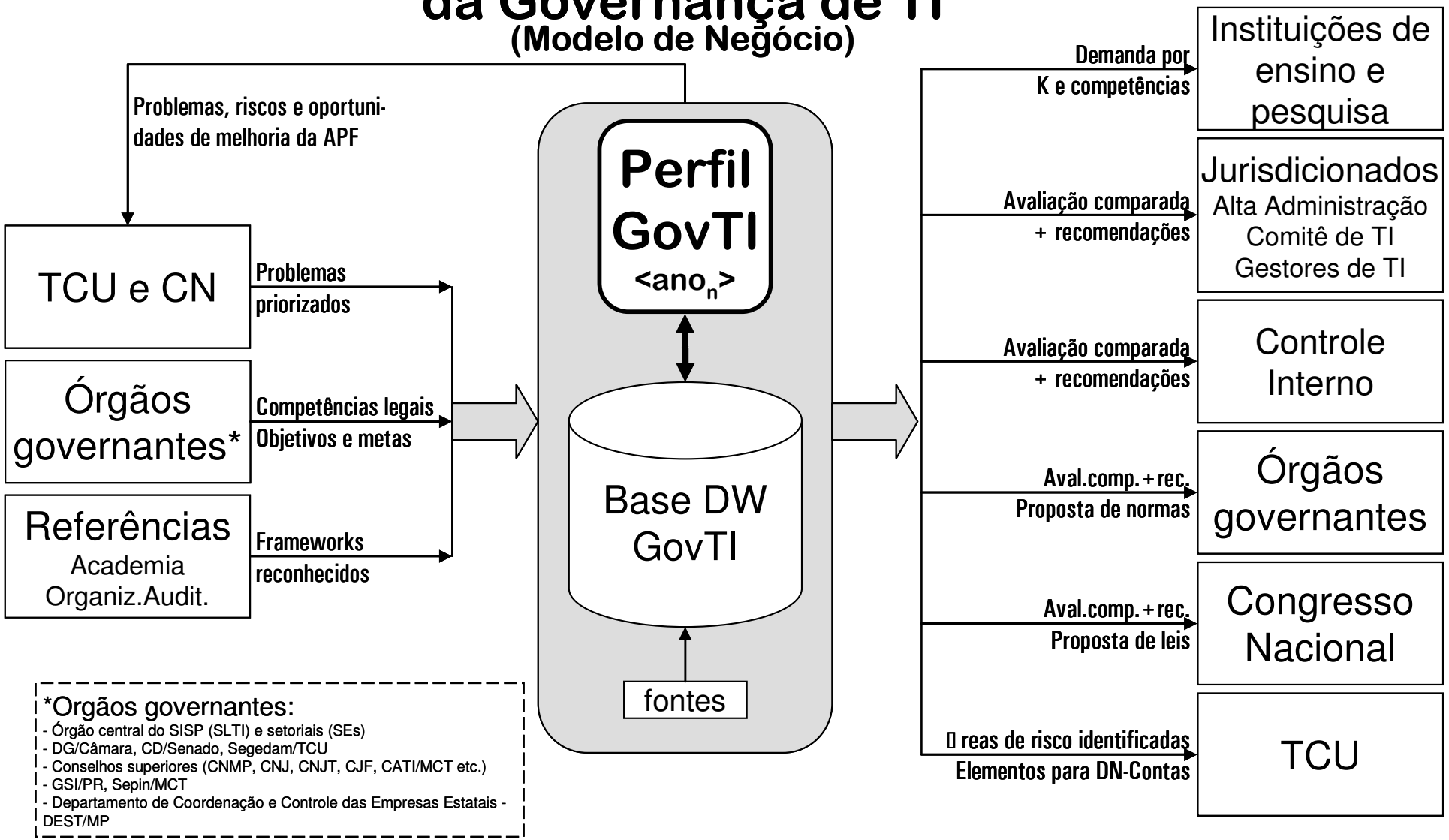
- Principais recomendações (Ac1603/2008-P):
  - Implantar processo de planejamento institucional e de TI
  - Criação do comitê de TI
  - Prover/manter quadro de servidores de TI adequado
  - Implantar processo de contratação de TI
  - Implantar política e processo de segurança da informação
  - Implantar processo de gestão de serviços
  - Implantar processo de software
  - Implantar processo de auditoria de TI
  - Implantar gestão orçamentária de TI, alinhada com negócio

Três anos depois, como anda a GovTI no setor público?

Levantamento GovTI/2010

- Principais objetivos:
  - ✓ Criar processo de mensuração periódico de Governança de TI
  - ✓ Fornecer feedback aos gestores, sugerindo onde melhorar
  - ✓ Identificar os melhores e piores casos e estudá-los
  - ✓ Subsidiar as fiscalizações em campo

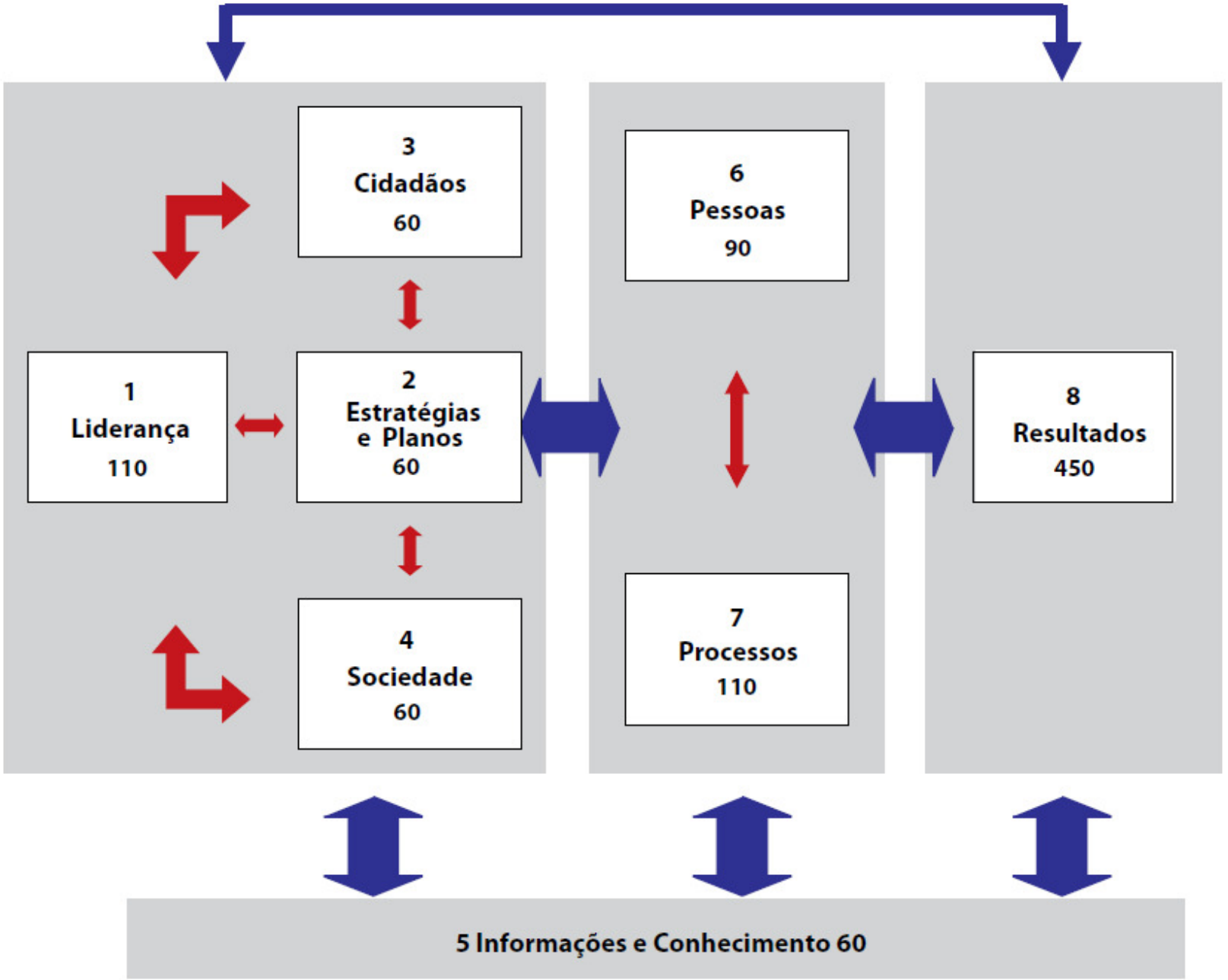
Processo de Acompanhamento da Governança de TI
(Modelo de Negócio)



Ciclo 2010 – Entradas

- Vindas do TCU: (Ac786/2006-P, Ac1603 e 2471/2008-P)
  - Governança pela Alta Administração
  - Suporte de TI às principais ações orçamentárias
  - Pessoal para gestão de TI
  - Processos (Segurança da Informação/Software/Projetos/Gestão de serviços/Contratações)
- Vindas do Min. Planej., Orç. e Gestão
  - Pessoal (cargos, funções, capacitação)
  - Estrutura de governança – Comitês de TI
  - Gespública
- Vindas das normas/frameworks
  - NBR 38500 – Responsabilidade da Alta Administração
  - Cobit, ITIL, NBR 27002, NBR 15504

Gespública (Decreto n° 5.378/2005)



Ciclo 2010 – Saídas

- Perfil GovTI 2010
- Base DW GovTI disponível para consultas
  - Dados do questionário
  - Dados de outras fontes (SIDOR, SIAFI etc.)
- Recomendações:
  - Jurisdicionados
  - Órgãos Governantes de TI (normas)
  - Controle Interno (verificação de controles)
  - Instituições de Ensino e Pesquisa
- Relatório ao Congresso Nacional

Resultados

- Apreciação pelo TCU prevista para 08SET
- Maioria das instituições públicas ainda está abaixo no nível mínimo de governança de TI
- Melhorias começam a ser sentidas em dois aspectos:
  - Melhoria na percepção da Alta Administração quanto a seu papel na Governança de TI
  - Melhoria do quadro de pessoal (quantidade e qualidade)
- Auditorias de governança de TI serão intensificadas

Agradeço muito a honra de ter partilhado esses momentos com vocês!

Cláudio Cruz

cscruz@tcu.gov.br