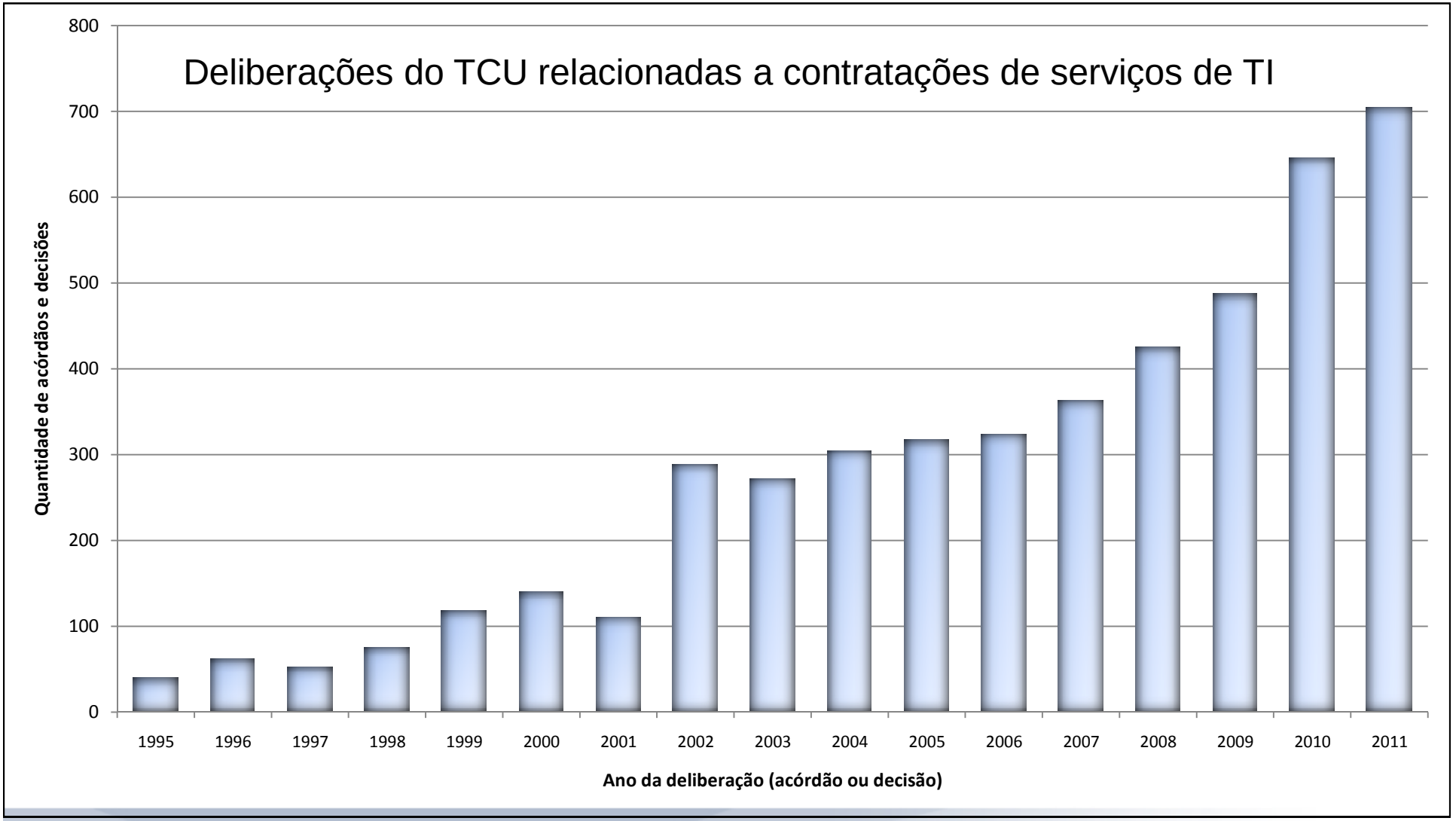
TRIBUNAL DE CONTAS DA UNIÃO

Estratégia e Riscos no Planejamento das Contratações de TI

Cláudio Silva da Cruz, MSc, CGEIT

Sefti

O problema



Fonte: Pesquisa textual na base do Sistema Juris (TCU)

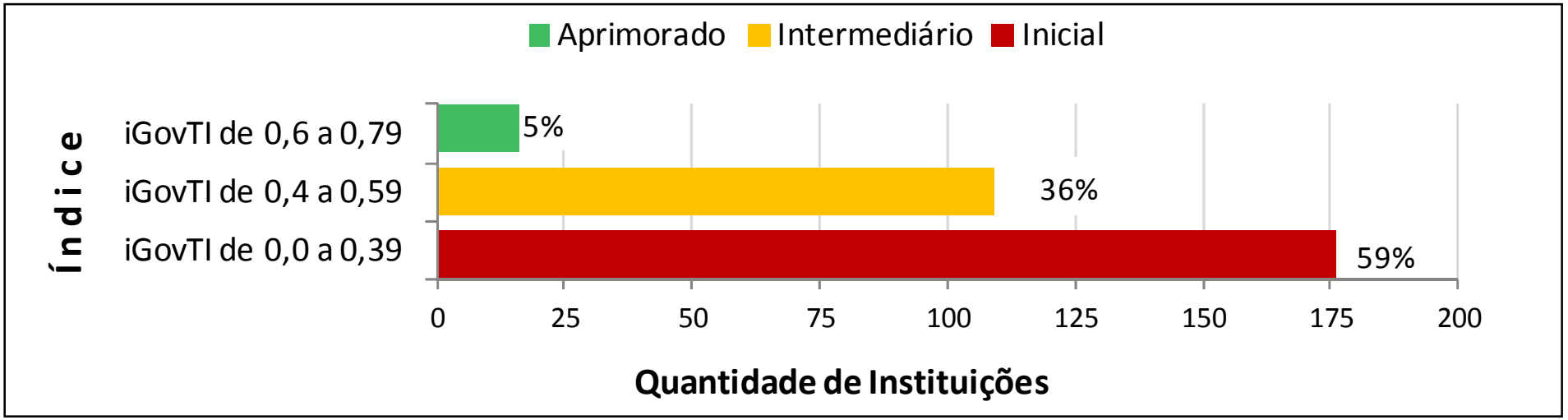
Por que isso acontece?

- Pesquisas de Governança de TI
  - 2007
    - 255 respondentes, maioria em situação ruim
    - 12 auditorias in loco ➔ ainda pior que o declarado
  - 2010
    - 301 respondentes, maioria em situação ruim
    - 18 auditorias in loco ➔ ainda pior que o declarado

O que está havendo?

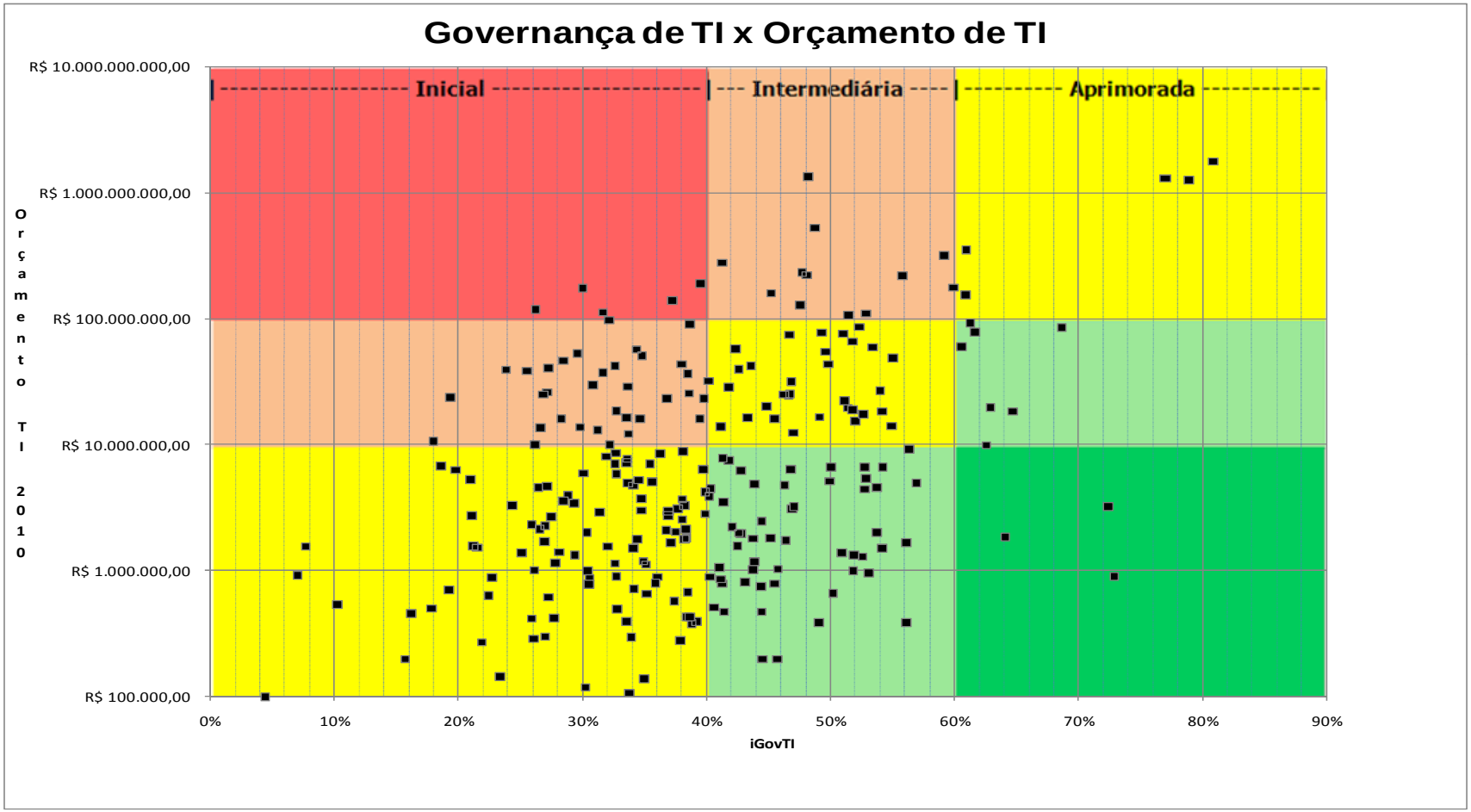
2010 - iGovTI

Instituições x estágios do iGovTI

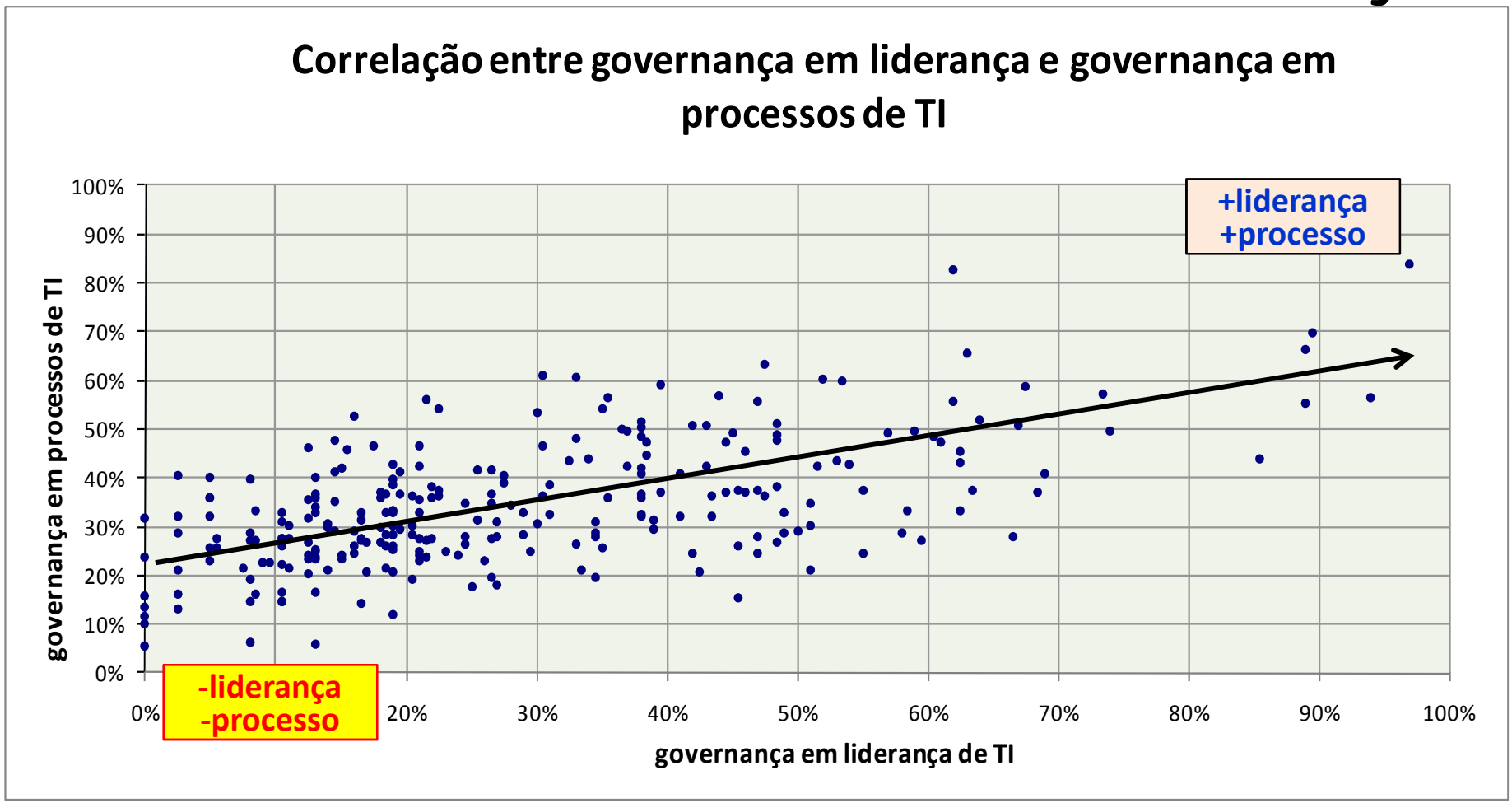


N=301

Risco de TI em função de iGovTI e Orçamento de TI

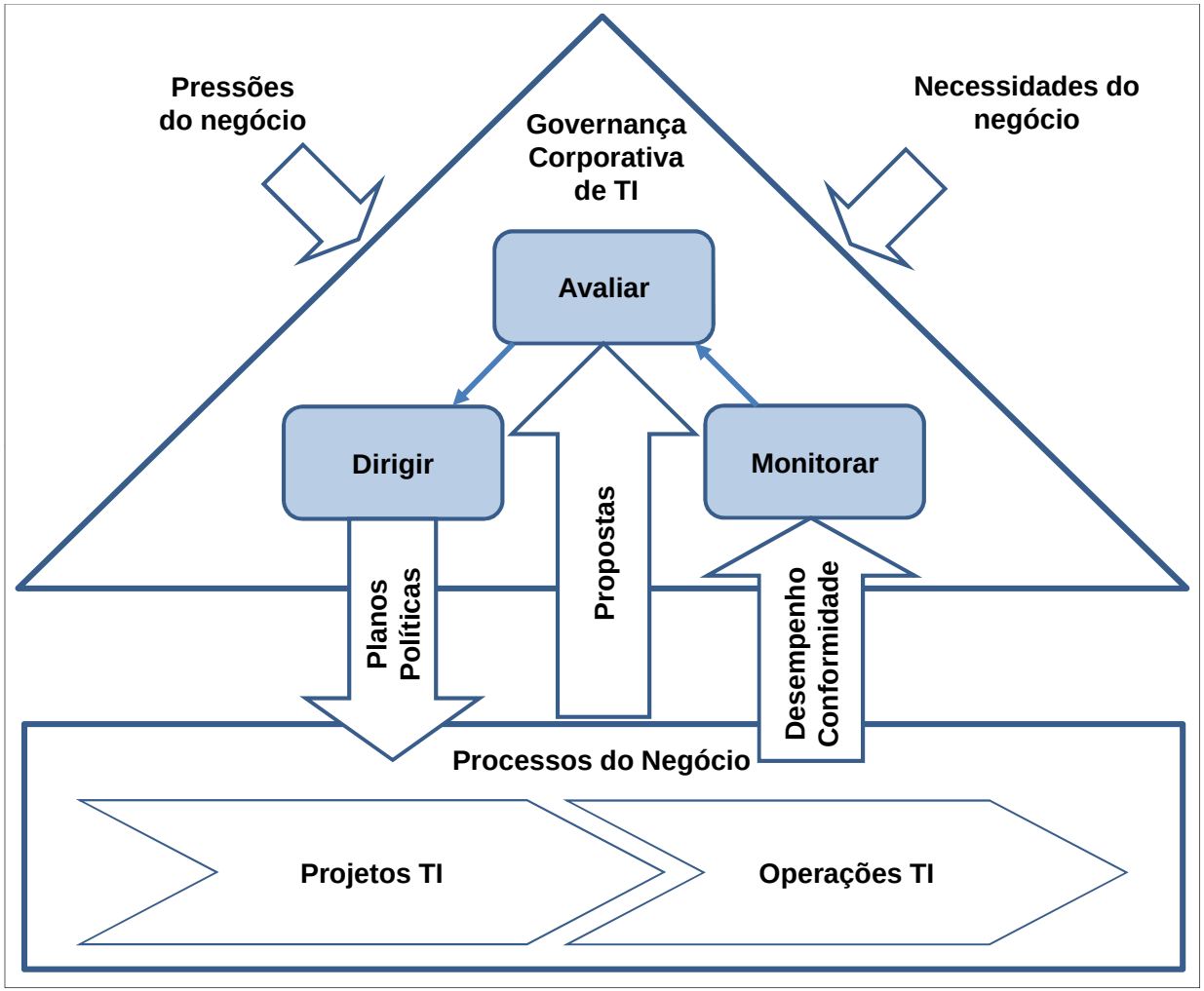


2010 - Liderança



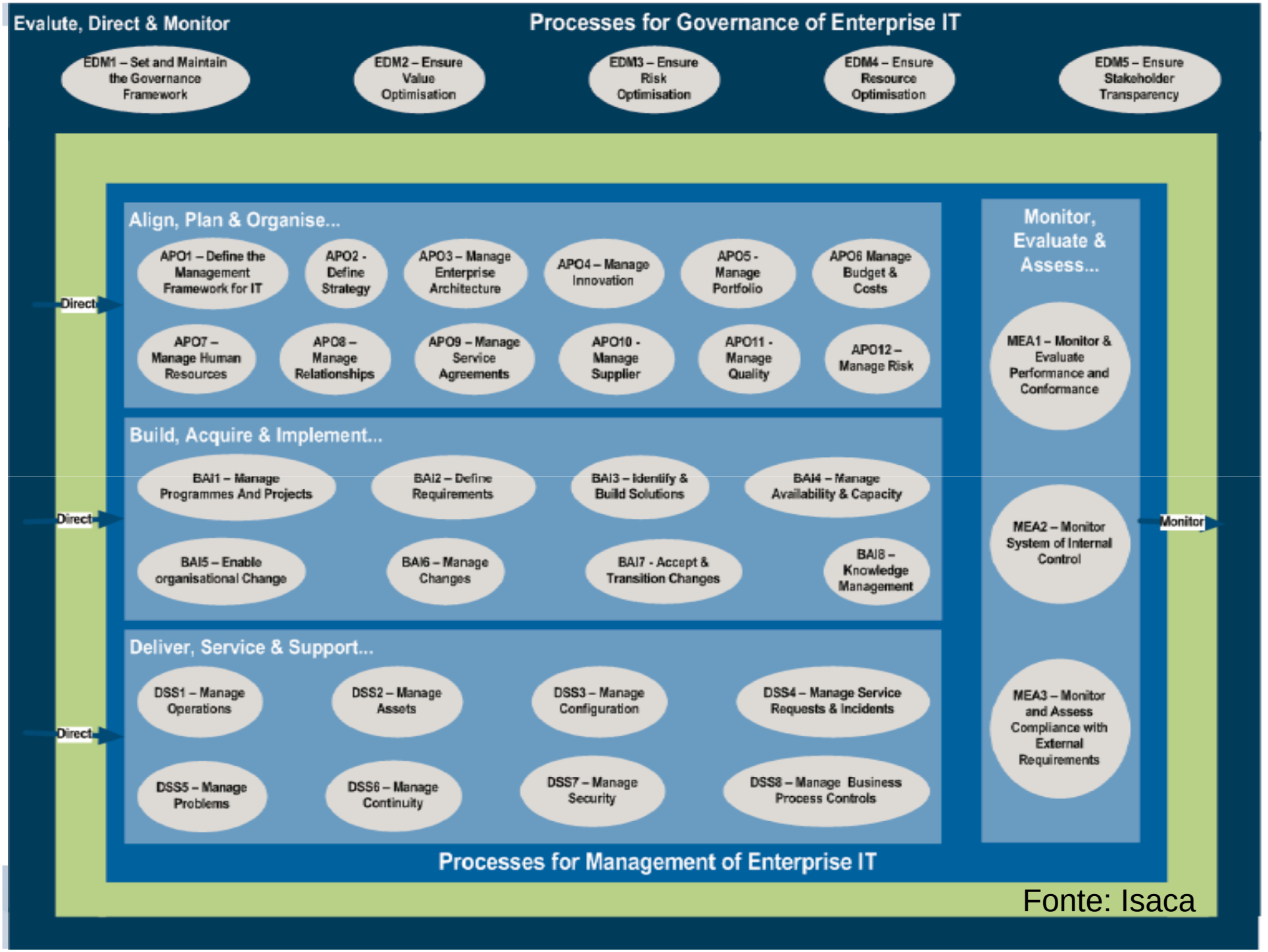
Coeficiente de correlação=0,60

A norma ABNT ISO/IEC NBR 38500



Princípios:

- Responsabilidade
- Estratégia
- Aquisição
- Desempenho
- Conformidade
- Comport. humano


Evalute, Direct & Monitor
Processes for Governance of Enterprise IT
EDM1 – Set and Maintain the Governance Framework
EDM2 – Ensure Value Optimisation
EDM3 – Ensure Risk Optimisation
EDM4 – Ensure Resource Optimisation
EDM5 – Ensure Stakeholder Transparency
Direct
Align, Plan & Organise...
APO1 – Define the Management Framework for IT
APO2 - Define Strategy
APO3 – Manage Enterprise Architecture
APO4 – Manage Innovation
APO5 - Manage Portfolio
APO6 Manage Budget & Costs
APO7 – Manage Human Resources
APO8 – Manage Relationships
APO9 – Manage Service Agreements
APO10 - Manage Supplier
APO11 - Manage Quality
APO12 – Manage Risk
Direct
Build, Acquire & Implement...
BAI1 – Manage Programmes And Projects
BAI2 – Define Requirements
BAI3 – Identify & Build Solutions
BAI4 – Manage Availability & Capacity
BAI5 – Enable organisational Change
BAI6 – Manage Changes
BAI7 - Accept & Transition Changes
BAI8 – Knowledge Management
Direct
Deliver, Service & Support...
DSS1 – Manage Operations
DSS2 – Manage Assets
DSS3 – Manage Configuration
DSS4 – Manage Service Requests & Incidents
DSS5 – Manage Problems
DSS6 – Manage Continuity
DSS7 – Manage Security
DSS8 – Manage Business Process Controls
Monitor, Evaluate & Assess...
MEA1 – Monitor & Evaluate Performance and Conformance
MEA2 – Monitor System of Internal Control
MEA3 – Monitor and Assess Compliance with External Requirements
Monitor
Processes for Management of Enterprise IT

Fonte: Isaca

Órgãos Governantes Superiores (OGS)

“Têm a responsabilidade por normatizar e fiscalizar o uso e a gestão de TI em seus respectivos segmentos da Administração Pública Federal”

(Voto do Acórdão 1.145/2011-TCU-Plenário)

- AGU
- CGU
- CNJ
- CNMP
- Dest/MP
- Enap/MP
- GSI/PR
- SLTI/MP
- SOF/MP
- STN/MF

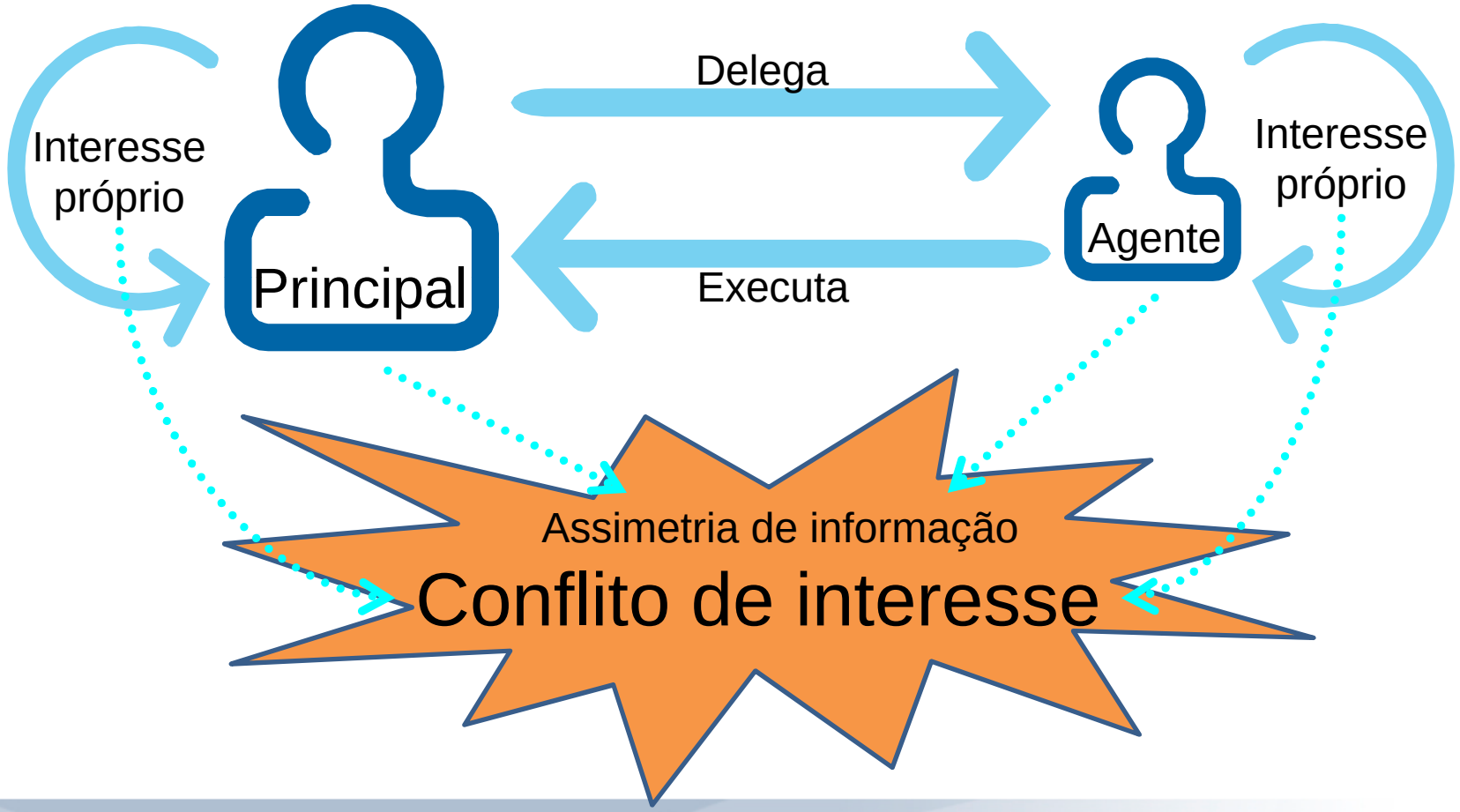
Acórdão 2.308/2010-Plenário

- Orientar a alta administração a estabelecer formalmente:
  - os objetivos institucionais de TI alinhados às estratégias de negócio (dirigir)
  - os indicadores para cada objetivo (dirigir)
  - as metas para cada indicador (dirigir)
  - os mecanismos que a alta administração adotará para acompanhar o desempenho da TI da instituição (monitorar)

Afinal, o que é Governança?

O problema da agência (agente)

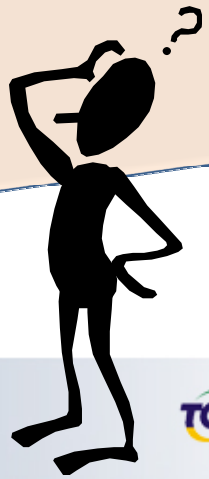
(público e privado)



O que é Governança?

O desenvolvimento das teorias sobre governança visa encontrar melhores respostas à seguinte pergunta:

Como maximizar a probabilidade de que o comportamento (ações) do Agente (altos administradores) seja dirigido pelo atendimento dos interesses do Principal, e não pelos seus próprios interesses ou de outrem?



Conceito de Governança

- *É o sistema pelo qual as organizações são **dirigidas, monitoradas** e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle.* *(IBGC, 2009, p.19)*
- ***Os princípios e práticas da boa Governança Corporativa aplicam-se a qualquer tipo de organização**, independente do porte, natureza jurídica ou tipo de controle [...] este Código foi desenvolvido [...] adaptável a outros tipos de organizações, como, por exemplo, [...] **órgãos governamentais**, entre outros.*
  (IBGC, 2009, p.15)

Conceito de Governança

- *O sistema pelo qual as organizações são **dirigidas e controladas**. (*NBR ISO/IEC 38.500, item 1.6.2*)*

- Consiste no **conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle** que visam assegurar que as decisões e ações relativas à gestão e ao uso dos recursos da organização estejam alinhadas às **necessidades** institucionais e contribuam para o alcance das **metas** organizacionais. (adaptado de Res-TCU 247/2011 (PGTI-TCU), art. 2º, II)

O que é Governança?

- Alguns princípios que norteiam as práticas de Governança:
  - Transparência
  - Equidade
  - Prestação de contas (*accountability*)
  - Responsabilidade corporativa

IBGC (2009)

O que é Governança?

- Governança funciona?
  - Sim, pois: reduz riscos e agrega valor (aumenta eficácia, eficiência, efetividade e economicidade).
  - Exigido, por exemplo, no sistema financeiro mundial (COSO; Sox; Basiléia etc.).
  - Aumenta o retorno sobre o ativo – no Brasil. (SILVA; LEAL, 2005)

E a Governança no setor público?

- Qualquer mandatário é um Agente.
- O Principal é a sociedade brasileira, que concede mandato por meio do voto e do sustento da estrutura do Estado para agir em seu nome.

O que é Governança no setor público?

- Há conflito de interesse?
  - Pode haver!
  - É necessário identificar com clareza os interesses e as expectativas da sociedade mandante na concessão do mandato a seus representantes.

O que é Governança no setor público?

- Há princípios que norteiam as práticas que conciliam os interesses?
  - Sim! ...
  - ... esses princípios estão positivados no ordenamento jurídico brasileiro ...

O que é Governança no setor público?

- Princípios da Administração Pública:
  - Planejamento e Controle (DL200/1997, art. 6º)
  - Transparência e publicidade (CF, art. 37 e LRF)
  - Moralidade (CF, art. 37)
  - Impessoalidade (CF, art. 37)
  - Economicidade (CF, art. 70)
  - Legalidade (CF, arts. 37 e 70)
  - Legitimidade (CF, art. 70)
  - Eficiência (CF, art. 37)
  - Eficácia e efetividade (L10180/2001, arts. 7º, III, 20, II)
  - etc.

O que é Governança no setor público?

Que práticas derivam desses princípios e permitem garantir o alinhamento dos interesses dos agentes mandatários ao genuíno interesse público?

O que é Governança no setor público?

- Práticas de governança: (principais)
  - Planejamento Institucional (missão, objetivos, indicadores, metas e alocação de recursos)
  - Comitês estratégicos (Negócio, RH, TI etc.)
  - Excelência de pessoal e descentralização
  - Controles internos
  - Publicação de planos, portfolios e resultados
  - Avaliação de desempenho individual e institucional
  - Auditoria Interna
  - Controle externo (CN com auxílio do TCU)

Resumindo...

- Gestão controla tarefas executivas, enquanto governança controla a gestão.
- Governança não controla diretamente tarefas executivas. Avalia se há controles sobre as tarefas executivas, monitorando-os e adotando medidas corretivas sob certas situações de risco (pré-definidas).

Tribunal de Contas da União

planejamento estratégico
construindo o TCU do futuro

MISSÃO

Controlar a Administração Pública para contribuir com seu aperfeiçoamento em benefício da sociedade

VISÃO

Ser reconhecido como instituição de excelência no controle e no aperfeiçoamento da Administração Pública

RESULTADOS

- Contribuir para melhoria da gestão e do desempenho da Administração Pública
- Contribuir para transparência da Administração Pública
- Coibir a ocorrência de fraudes e desvios de recursos
- Condenar efetiva e tempestivamente os responsáveis por irregularidades e desvios

PESSOAS E INOVAÇÃO

- Fortalecer cultura orientada a resultados
- Desenvolver cultura de inovação
- Desenvolver competências gerenciais e profissionais
- Estruturar a gestão do conhecimento organizacional
- Modernizar e integrar as práticas de gestão de pessoas

PROCESSOS INTERNOS

Governança e desempenho

- Intensificar ações que promovam a melhoria da gestão de riscos e de controles internos da Administração Pública
- Aprimorar as ações de controle voltadas à melhoria do desempenho da Administração Pública
- Intensificar ações de controle para combate ao desperdício e utilização irregular de recursos públicos

Parcerias

- Aprimorar o relacionamento com o Congresso Nacional
- Atuar em cooperação com a Administração Pública e com a rede de controle

Tempestividade e seletividade

- Assegurar razoabilidade no tempo de apreciação dos processos
- Atuar de forma seletiva e sistêmica em áreas de risco e relevância

Transparência

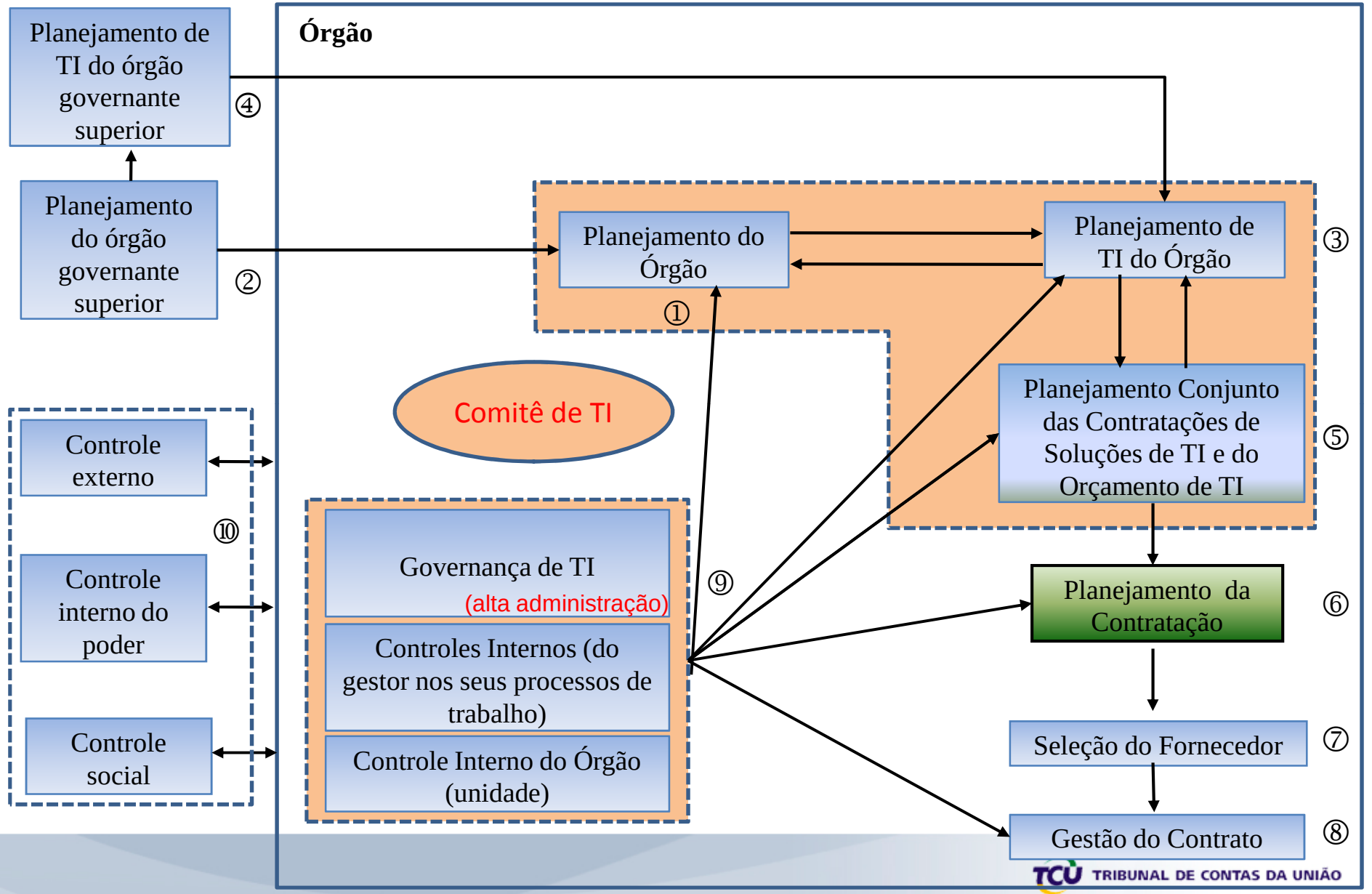
- Induzir a Administração Pública a divulgar informações de sua gestão
- Intensificar a comunicação com a sociedade
- Facilitar o exercício do controle social

ORÇAMENTO E LOGÍSTICA

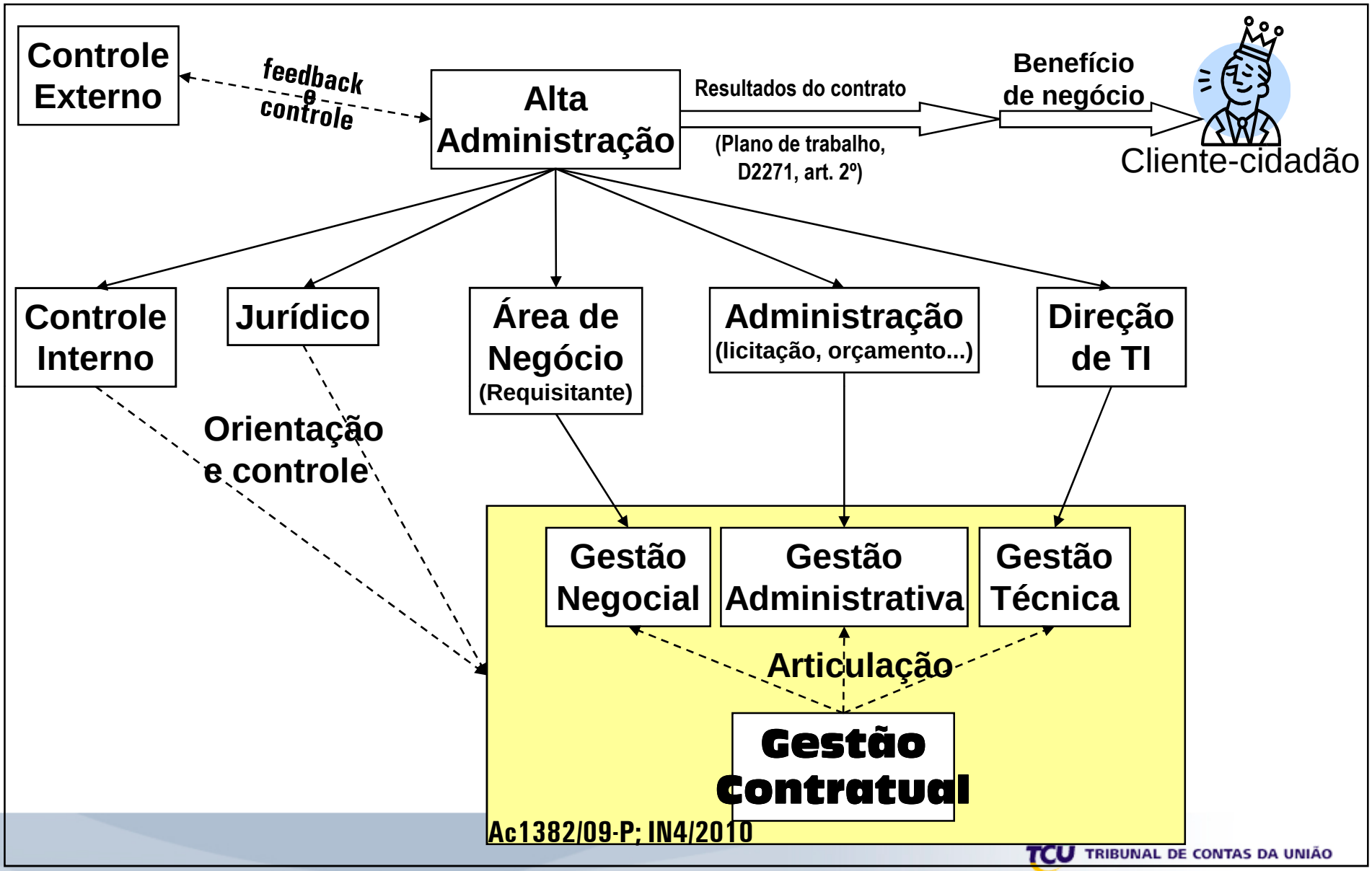
- Promover a melhoria da governança do TCU
- Otimizar o uso de TI na gestão do TCU
- Intensificar e aprimorar o uso de TI nas ações de controle
- Assegurar adequado suporte logístico às necessidades do TCU
- Assegurar recursos para modernização do TCU

Governança das contratações de TI

Governança das contratações de TI



Governança das contratações de TI



Governança das contratações de TI

- Principais controles:
  - Plano Estratégico Institucional
  - Plano Diretor de TI
  - Comitê de TI
  - Auditoria Interna
  - Monitoramento de resultados (AA)
  - Processo padronizado de contratação
  - **Treinamento e seleção de gestores (!!!)**
  - **Exame e aprovação por assessoria jurídica (!!!)**

Todos incluídos no questionário do Levantamento Perfil GovTI2012 e 2012!

Planejando a contratação

- Artefatos essenciais
  - **Estudos técnicos preliminares** (L8666, art. 6º, IX)
  - **Plano de trabalho** (D2271, art. 2º)
    - Autoridade máxima
    - Necessidade, quantidade e resultados
    - Resultados: projetados, acompanhados e medidos)
  - **Termo de referência** (L10520/D3555) ou Projeto básico (L8666)

E a IN4?

Planejando a contratação

- Artefatos da IN SLTI/MP 4/2010
  - Documento de oficialização da demanda (DOD)
  - Análise de Viabilidade
  - Plano de sustentação
  - Estratégia de contratação
  - Análise de risco

- São inovações à lei?
  - Não! São formas organizadas (e mais auditáveis) de chegar aos artefatos essenciais.

Riscos e controles

- Riscos (NBR 31000)
  - Risco é o efeito da incerteza nos objetivos
  - O efeito do risco pode ser positivo ou negativo
- Controles internos (NBR 31000)
  - atuam sobre o risco
  - são necessários para maximizar a probabilidade de alcance dos objetivos
  - qualquer diretriz, política, processo, dispositivo, prática ou ação que vise modificar o risco

Riscos e controles

- Etapa: definição da necessidade da contratação
  - Risco: solução de TI desalinhada com necessidade de negócio
  - Controle(s):
    - Objetivos institucionais claros no PEI
    - Objetivos de TI claros no PDTI, alinhados ao PEI
    - Lista fundamentada de contratações no PDTI
      - Comitê de TI atuante (visão sistêmica e foco em resultados)
      - Decisão fundamentada e formal da alta administração

Riscos e controles

- Etapa: definição da necessidade da contratação
  - Risco: solução de TI com foco em TI e não no negócio
  - Controle(s):
    - Requisição vem da área de negócio (DOD)
    - Prioridades definidas no Comitê de TI, aprovadas pela AA
    - Objetivos institucionais claros no PEI
    - Objetivos de TI claros no PDTI, alinhados ao PEI
    - Lista fundamentada de contratações no PDTI
      - Comitê de TI atuante (visão sistêmica e foco em resultados)
      - Decisão fundamentada e formal da alta administração

Riscos e controles

- Etapa: definição da necessidade da contratação
  - Risco: aplicação de TI em processo sem prévia otimização (O&M)
  - Controle(s):
    - Demonstração pelo requisitante de que só otimização O&M não resolve, mas que solução de TI é necessária ou a melhor alternativa
    - Prioridades definidas no Comitê de TI, aprovadas pela AA
    - Lista fundamentada de contratações no PDTI
      - Comitê de TI atuante (visão sistêmica e foco em resultados)
      - Decisão fundamentada e formal da alta administração

Riscos e controles

- Etapa: definição da necessidade da contratação
  - Risco: manutenção de solução de TI irrelevante
  - Controle(s):
    - Atribuição de um gestor de negócio para cada solução de TI
    - Definição do processo de gestão de portfólio, com critérios objetivos para inclusão, exclusão e manutenção de solução de TI

Riscos e controles

- Etapa: requisitos da contratação
  - Risco: requisitos desalinhados com a necessidade
  - Controle(s):
    - Revisão dos artefatos intermediários por servidor sênior
    - Avaliação e aprovação desse quesito pela autoridade competente
    - Avaliação e aprovação do cuidado com esse aspecto pela assessoria jurídica (não é exame técnico, mas jurídico)

Riscos e controles

- Etapa: requisitos da contratação
  - Risco: requisitos não isonômicos ao mercado potencial
  - Controle(s):
    - Evidência de análise das potencialidades do mercado
    - Evidência da qualidade dos requisitos
      - demonstração da relevância de negócio dos requisitos mais vulneráveis a questionamento
    - Matriz de análise “Requisito(s) x Fornecedor(es)”

Riscos e controles

- Etapa: requisitos da contratação
  - Risco: requisitos que impliquem ingerência na contratada
  - Controle(s):
    - Aperfeiçoamento dos padrões de contratação
      - Modelos de execução dos serviços
      - Modelos de gestão do contrato
    - Revisão dos artefatos intermediários por servidor sênior
    - Avaliação e aprovação desse quesito pela autoridade competente
    - Avaliação e aprovação do cuidado com esse aspecto pela assessoria jurídica (não é exame técnico, mas jurídico)

Riscos e controles

- Etapa: requisitos da contratação
  - Risco: quantitativos inadequados (sobra ou falta)
  - Controle(s):
    - Aperfeiçoamento dos mecanismos de quantificação da demanda (histórico e avaliações)
    - Planilhas claras nos autos
    - Aprovação pelo Comitê de TI (defesa dos quantitativos)

Riscos e controles

- Etapa: levantamento de mercado
  - Risco: licitação deserta ou direcionamento de licitação
  - Controle(s):
    - Evidência de análise das potencialidades do mercado
    - Evidência da qualidade dos requisitos
      - demonstração da relevância de negócio dos requisitos mais vulneráveis a questionamento
    - Matriz de análise “Requisito(s) x Fornecedor(es)”

Riscos e controles

- Etapa: estimativa inicial de preços
  - Risco: informação insuficiente para decidir se a contratação é adequada
  - Controle(s):
    - Evidência de análise das potencialidades do mercado
    - Estudos de contratos semelhantes celebrados por outras instituições (benchmarking)
    - “cesta de preços”
    - ATENÇÃO: a estimativa inicial em geral é muito imprecisa, pois ainda faltam elementos importantes na definição do preço por fornecedores.

Riscos e controles

- Etapa: definição da solução de TI
  - Risco: solução incompleta (não produz os resultados esperados)
  - Controle(s):
    - Evidência de análise das potencialidades do mercado
    - Estudos de contratos semelhantes celebrados por outras instituições (benchmarking)
    - Revisão dos artefatos intermediários por servidor sênior
    - Eventual consulta ou audiência pública

Riscos e controles

- Etapa: definição da solução de TI
  - Risco: parcelamento inadequado
  - Controle(s):
    - Evidência de análise das potencialidades do mercado
    - Análise segundo os critérios de parcelamento:
      - Técnica e economicamente viável
      - Aproveita as características do mercado
      - Não perde economia de escala
    - Análise segundo as hipóteses de parcelamento
      - Por item ou grupo de itens
      - Quarteirização
      - Subcontratação
      - Consórcio

Riscos e controles

- Etapa: definição dos resultados pretendidos
  - Risco: resultados subjetivos ou não realistas
  - Controle(s):
    - Benefícios (resultados) esperados definidos no Comitê de TI, aprovadas pela AA, em termos de negócio
    - Objetivos institucionais claros no PEI
    - Objetivos de TI claros no PDTI, alinhados ao PEI
    - Lista fundamentada de contratações no PDTI
      - Comitê de TI atuante (visão sistêmica e foco em resultados)
      - Decisão fundamentada e formal da alta administração
    - Clara avaliação do potencial do modelo de execução do objeto e de gestão do contrato para conduzir aos resultados

Riscos e controles

- Etapa: adequação do ambiente do contratante
  - Risco: ambiente inadequado para execução contratual
  - Controle(s):
    - Análise formal dos requisitos de ambiente
      - patrocínio da área de negócio, infraestrutura de TI, eletricidade, ar-condicionado, espaço físico, estrutura de gestão, acesso a sistemas, capacitação, impactos (ambiental, socio-político, rotinas, interessados externos etc.) etc.
    - Plano de obtenção das condições ainda não disponíveis (com lista de recursos necessários)
    - Revisão do plano de sustentação por servidor sênior

Riscos e controles

- Etapa: análise de risco
  - Risco: análise irrealista
  - Controle(s):
    - Avaliação formal dos riscos e proposta de controles
    - Revisão da análise de risco por servidor sênior
    - Aprovação pelo Comitê de TI
    - Aprovação pela autoridade competente

Riscos e controles

- Etapa: declaração de viabilidade ou não
  - Risco: análise irrealista
  - Controle(s):
    - Revisão da análise de risco por servidor sênior
    - Aprovação pelo chefe da área de TI (viabilidade técnica)
    - Aprovação pelo Comitê de TI (viabilidade negocial)
    - Aprovação pela autoridade competente (viabilidade administrativa, considerando a viabilidade técnica e negocial)

Riscos e controles

- Etapa: definição do objeto
  - Risco: falta de clareza e precisão
  - Controle(s):
    - Revisão por servidor sênior
    - Clareza nos autos (mesmo o não especialista e o cidadão comum devem entender a maior parte)
    - Coerência com todos os artefatos e estudos anteriores
    - Eventual consulta ou audiência pública

Riscos e controles

- Etapa: justificativa da contratação
  - Risco: falha ou ausência de justificativas
  - Controle(s):
    - Revisão por servidor sênior
    - Todos os elementos mais expostos a riscos de contestação (por qualquer interessado) devem ser suficientemente justificados
    - Coerência com todos os artefatos e estudos anteriores
    - Eventual consulta ou audiência pública

Riscos e controles

- Etapa: modelo de execução do objeto
  - Risco: falha ou deficiência no modelo de execução do objeto
  - Controle(s):
    - Revisão por servidor sênior
    - Planilha completa de serviços a realizar e itens a entregar
      - Incluir o cronograma físico-financeiro
    - Todos os elementos mais expostos a riscos de contestação (por qualquer interessado) devem ser suficientemente justificados
    - Coerência com todos os artefatos e estudos anteriores
      - Resumo dos estudos técnicos preliminares
    - Eventual consulta ou audiência pública

Riscos e controles

- Etapa: modelo de licitação do objeto
  - Risco: falha ou deficiência na escolha do modelo de licitação
  - Controle(s):
    - Revisão por servidor sênior e por assessoria jurídica
    - Regra é o pregão para TI; qualquer outro modelo (tipo/modalidade) exige exaustiva justificativa
    - Requisitos devem ASSEGURAR a qualidade da contratação
    - Requisitos não devem limitar injustificadamente a competição
    - Outros elementos: preços mínimos, máximos e estimados; inexequibilidade; desempate e preferência; clareza nas condições de habilitação; garantia.

Riscos e controles

- Etapa: modelo de gestão do contrato
  - Risco: falha ou deficiência no modelo de gestão
  - Controle(s):
    - Revisão por servidor sênior e por assessoria jurídica
    - **Regra**: pagar somente por resultado entregue, medido e aceito
    - Segregação de funções (recebimento provisório e definitivo)
      - Critérios claros de entrega e recebimento (qualidade e desempenho)
      - Critérios claros de medição
      - Critérios claros de sanção e rescisão
    - Papéis e responsabilidades bem definidos:
      - preposto, fiscal, gestor, contratos, contabilidade, autoridade superior, autoridade competente, autoridade máxima, Ministro de Estado

Riscos e controles

- Etapa: contratação como um todo
  - Risco: falhas ou deficiências
  - Controle(s):
    - Publicidade – publicar o extrato do edital no DOU e em jornais de grande circulação e colocá-lo à disposição na Internet
    - Transparência (L12527 combinada com L8666, art. 3º, §3º)
      - Deve-se dar a conhecer a informação sobre a contratação
      - É um princípio da boa governança (IBGC, 2009)
      - Recomenda-se publicar os autos
      - Recomenda-se que todos os elementos da contração que envolvam maior risco de questionamento tenham suas justificativas resumidas publicadas no próprio edital e referenciando aos autos
      - Recomenda-se redigir os autos como um documento público, destinado ao público (que é o cliente!) para fins de controle social

Grato pela atenção

Cláudio Silva da Cruz, MSc, CGEIT

Sefti/Segecex/TCU

sefti@tcu.gov.br