TRIBUNAL DE CONTAS DA UNIÃO

Uso de TIC nas IFES
Planejamento e Governança

IV Encontro do Forplad

Daniel Moreira Guilhon, CISA

Novembro/2012

O que pretendemos?

- ✓ Conceituar os aspectos relacionados à boa governança para assegurar uma boa gestão de TI
- ✓ Avaliar casos em que a falta de governança gerou situações problemáticas para a Administração
- ✓ Analisar a evolução dos modelos de contratação de TI
- ✓ Obter um panorama da situação da Governança de TI na Administração Pública Federal

TRIBUNAL DE CONTAS DA UNIÃO

AGENDA

- ✓Conceitos
- ✓Governança x Gestão
- ✓E se não houver Governança de TI?
- ✓Governança de TI e a NBR ISO/IEC 38.500:2009
- ✓Modelos de contratação
- ✓Avaliação de Governança de TI

Governança Corporativa

"Governança Corporativa 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 – Instituto Brasileiro de Governança Corporativa)

"O Sistema pelo qual as organizações são dirigidas e controladas"

(NBR ISO/IEC 38.500:2009, item 1.6.2)

Governança de TI

"O sistema pelo qual o uso atual e futuro da TI é dirigido e controlado."

(NBR ISO/IEC 38.500:2009, item 1.6.3)

- ✓ TI deve agregar valor ao negócio
- ✓ Riscos aceitáveis

Governança Corporativa x de TI

Recomendação do *Gartner Group*:

✓Use os princípios de Governança Corporativa e todos os recursos apropriados para obter a participação e o suporte da alta administração na Governança de TI.

TRIBUNAL DE CONTAS DA UNIÃO

AGENDA

- ✓Conceitos
- ✓Governança x Gestão
- ✓E se não houver Governança de TI?
- ✓Governança de TI e a NBR ISO/IEC 38.500:2009
- ✓Modelos de contratação
- ✓Avaliação de Governança de TI

Governança x Gestão

✓Gestão: “O sistema de controles e processos necessário para alcançar os objetivos estratégicos estabelecidos pela direção da organização.”

(NBR ISO/IEC 38.500:2009, item 1.6.9)

✓Gestão controla tarefas executivas, enquanto governança controla a gestão

✓Governança não controla diretamente tarefas executivas

Gestão

Definição do Cobit 5

✓Gestão trata de planejamento, criação, organização e controle operacional das atividades com vistas a alinhar com a direção definida pelo corpo governante.

(tradução livre)

Papel da Auditoria Interna

"A auditoria auxilia a organização a alcançar seus objetivos por meio de uma abordagem sistemática e disciplinada para a avaliação e [indução da] melhoria da eficácia dos processos de gerenciamento de risco, controle e governança corporativa."

(IIA, IPPF, Definição de Auditoria Interna)

TRIBUNAL DE CONTAS DA UNIÃO

AGENDA

- ✓Conceitos
- ✓Governança x Gestão
- ✓E se não houver Governança de TI?
- ✓Governança de TI e a NBR ISO/IEC 38.500:2009
- ✓Modelos de contratação
- ✓Avaliação de Governança de TI

Falta de Governança de TI

✓Política de Segurança da Informação (PSI) desatualizada e não aprovada formalmente

Acórdão 71/2007-TCU-Plenário

PSI desatualizada e não aprovada

- ✓ “Observou-se que não existem para o [sistema] políticas ou normas formalizadas que concorram para uma boa gestão da segurança da informação (item 2.4). A principal delas seria a Política de Segurança da Informação - PSI -, documento que expressa as orientações da organização quanto à gestão de segurança da informação. Da PSI nascem as demais políticas, como a Política de Controle de Acesso - PCA -, que estabelece as regras que devem ser seguidas para obtenção de acesso às informações.”

Falta de Governança de TI

✓Ausência de posse de seus sistemas e bases de dados.

Acórdão 2.023/2005-TCU-Plenário

Ausência da posse de sistemas e bases

- ✓ “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.”

Falta de Governança de TI

✓Completa dependência tecnológica.

Acórdão 889/2007-TCU-Plenário

Completa dependência tecnológica

✓ “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.”

Falta de Governança de TI

✓Ações paralelas, sem coordenação.

TC 022.059/2008-0

Ações paralelas, sem coordenação

- ✓ “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 [...]. “
- ✓ “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 [...].”

Falta de Governança de TI

✓Sistema contratado, pago, mas inservível.

TC 031.963/2008-0

Sistema contratado, pago, mas inservível

- ✓ “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).”
- ✓ “Apesar de não ter sido possível a implementação e utilização do [Sistema] em sua versão final entregue pela [contratada], o produto foi homologado e pago, inclusive a última parcela reservada para efetivação após o aceite final da solução de TI contratada.”

Falta de Governança de TI

✓Sistema contratado, desenvolvido, servível, pago, mas não implantado.

Acórdão 2.023/2005-TCU-Plenário

Sistema servível, mas não implantado

- ✓ “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 ...”

Materialidade

Gastos do Governo Federal em TI:

- ✓2006: R$ 6 bilhões (Siafi)
- ✓2010: estimados R$ 16 bilhões (LOA 2010)
- ✓2011: estimados R$ 18 bilhões (LOA 2011)
- ✓ 2012: estimados R$ 11 bilhões (LOA 2012)

Criticidade

✓TI é setor estratégico (também) na Administração Pública e os problemas na área são grandes vulnerabilidades na organização

✓Fiscalizações realizadas pelo TCU identificaram que na APF a TI está muito terceirizada e com deficiências nos controles

O problema não é terceirizar

✓Decreto-Lei 200/1967:

"Art. 10. A execução das atividades da Administração Federal deverá ser amplamente descentralizada.

§ 7º Para melhor desincumbir-se das tarefas de planejamento, coordenação, supervisão e controle [...] recorrendo, sempre que possível, à execução indireta, mediante contrato, desde que exista, na área, iniciativa privada suficientemente desenvolvida e capacitada a desempenhar os encargos de execução."

O problema é terceirizar mal

- ✓É não saber o que nem como terceirizar.
- ✓É não avaliar os riscos:
  - Estamos terceirizando áreas estratégicas?
  - Temos pessoal para controlar a terceirização?
  - O pessoal que temos está capacitado?
- ✓É não criar controles:
  - Como criar controle sem processos de contratação e gestão contratual?
- ✓É se ver completamente dependente dos terceiros:
  - Temos um plano “B”?

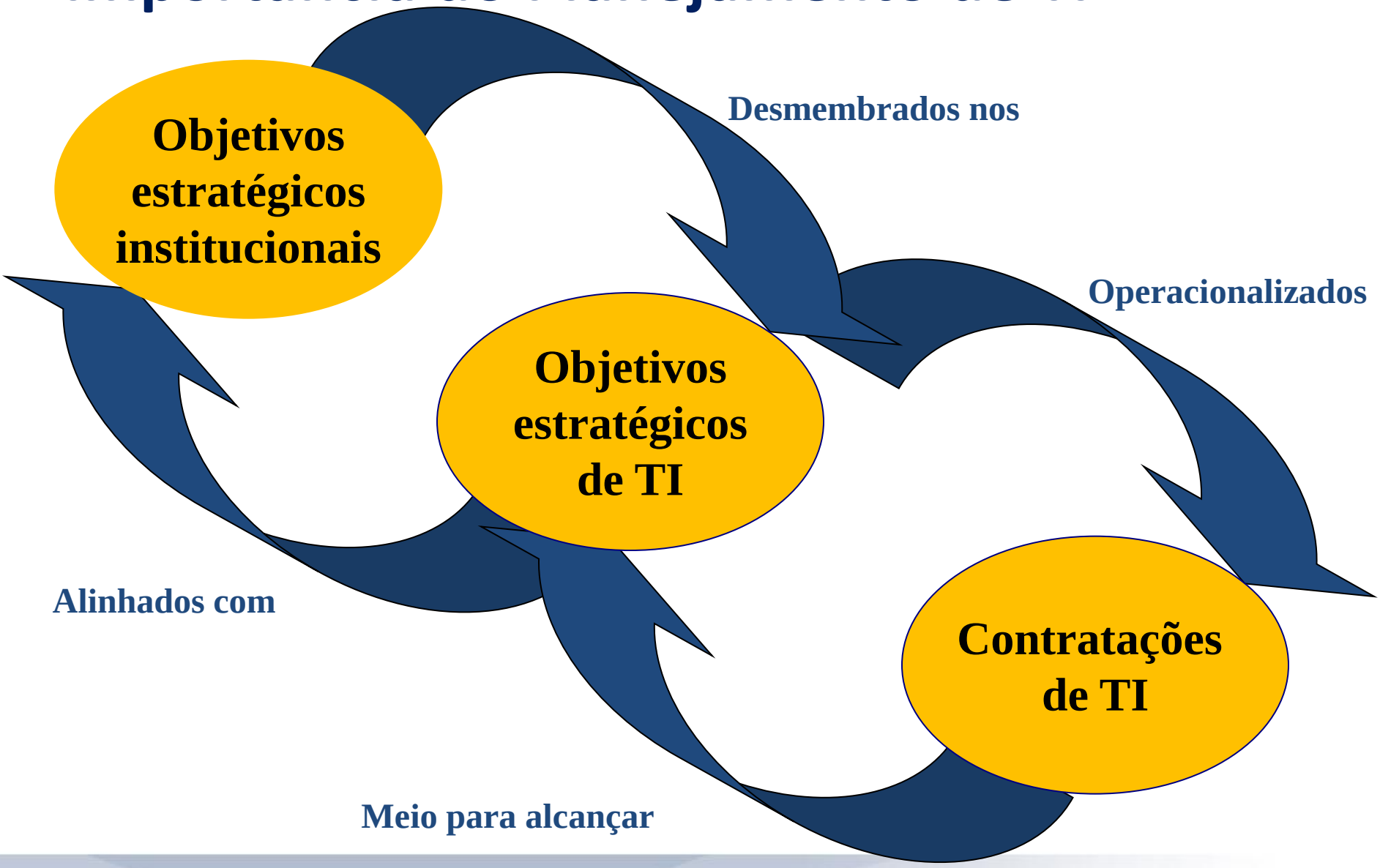
O problema é terceirizar
sem estratégia!

Planejamento de TI

Necessidade de Planejamento de TI:

- ✓ Constituição Federal, art. 37;
- ✓ Decreto-Lei 200/1967, art. 6º, I;
- ✓ Decreto nº 7.174/2010;
- ✓ Instrução Normativa - SLTI/MP 4/2010, art. 4º;
- ✓ Acórdão 1.558/2003-TCU-Plenário, item 9.3.9;
- ✓ Acórdão 1.603/2008-TCU-Plenário, item 9.4.1;
- ✓ Cobit 4.1 PO1.4 Plano Estratégico de TI.

Importância do Planejamento de TI



AGENDA

- ✓Conceitos
- ✓Governança x Gestão
- ✓E se não houver Governança de TI?
- ✓Governança de TI e a NBR ISO/IEC 38.500:2009
- ✓Modelos de contratação
- ✓Avaliação de Governança de TI

NBR ISO/IEC 38.500:2009

Tecnologia da Informação:

- ✓ “Os recursos necessários para adquirir, processar, armazenar e disseminar informações.”

(NBR ISO/IEC 38.500:2009, item 1.6.7)

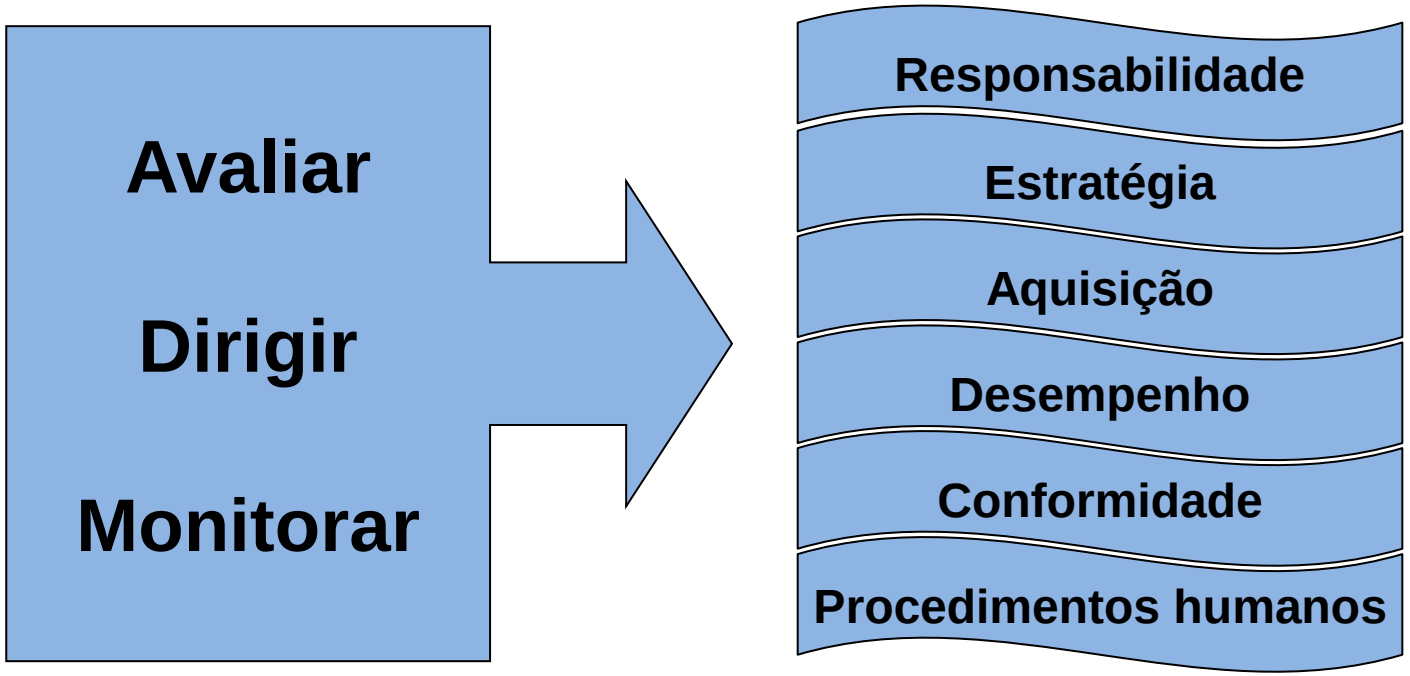
Recursos:

- ✓ “Pessoas, procedimentos, software, informações, equipamentos, consumíveis, infraestrutura, capital e tempo”

(NBR ISO/IEC 38.500:2009, item 1.6.13)

NBR ISO/IEC 38.500:2009

Governar a TI é realizar 3 tarefas sobre 6 princípios:



NBR ISO/IEC 38.500:2009

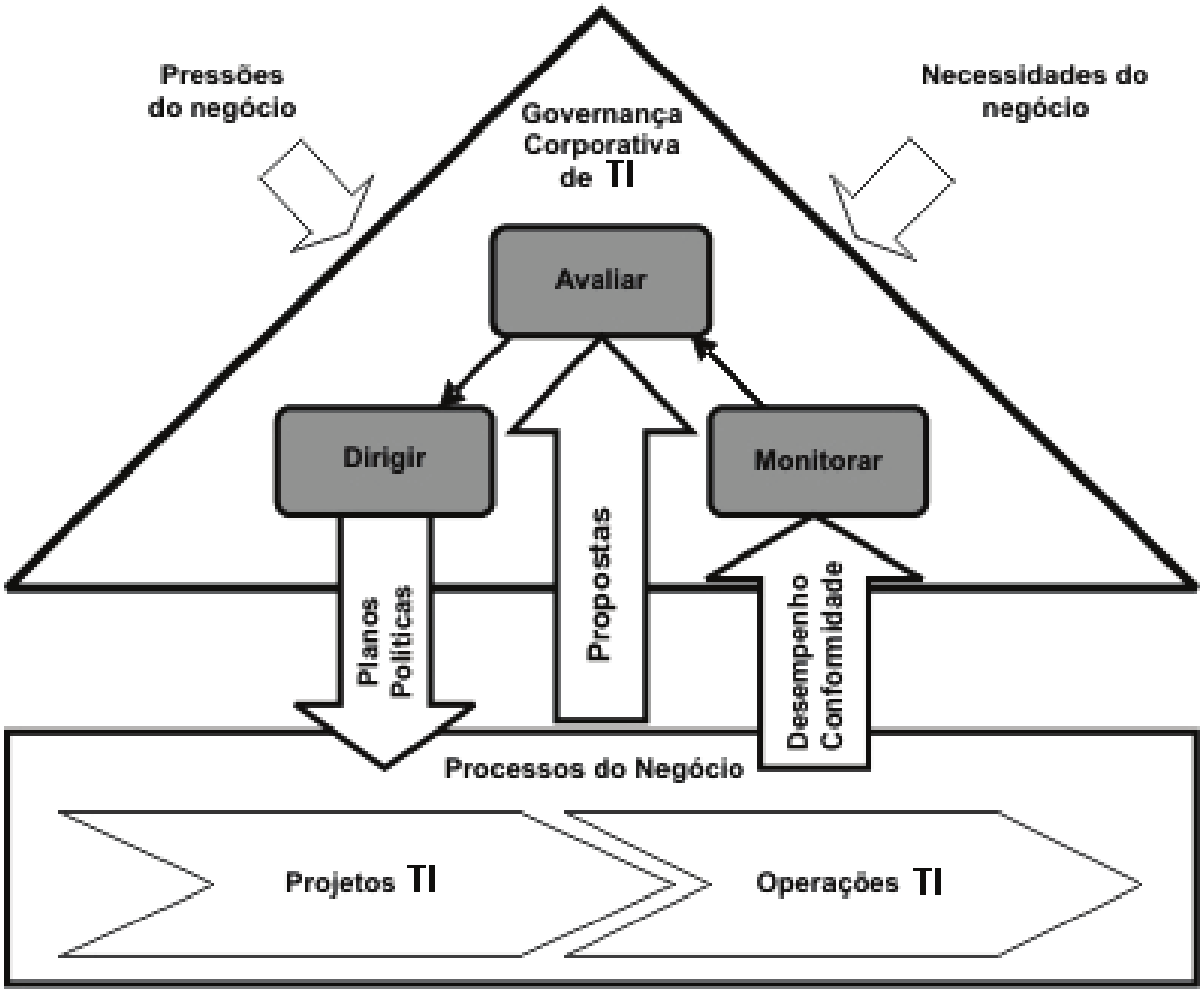
Responsabilidade:

- ✓ "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 38.500:2009, item 2.2)

- ✓ Ex: Acórdão 2.079/2009-TCU-Plenário

NBR ISO/IEC 38.500:2009



TRIBUNAL DE CONTAS DA UNIÃO

AGENDA

- ✓Conceitos
- ✓Governança x Gestão
- ✓E se não houver Governança de TI?
- ✓Governança de TI e a NBR ISO/IEC 38.500:2009
- ✓Modelos de contratação
- ✓Avaliação de Governança de TI

Antigo modelo de contratação de TI

✓Consistia na reunião de todos os serviços de informática da organização em um único e grande contrato, adjudicado a uma única empresa, com pagamentos realizados por hora-trabalhada.

✓Essas contratações equivaliam a um setor de TI completo e terceirizado.

Antigo modelo de contratação de TI

- ✓Ausência de parcelamento do objeto
  - – Potencial limitação à competição
  - – Risco de onerar indevidamente o contrato
  - – Risco estratégico (dependência)
  - – Risco na segurança da informação
- ✓Pagamento por homem-hora (HH)
  - – Risco exclusivo do contratante
  - – Risco de remuneração de horas improdutivas
  - – Anti-economicidade: “Paradoxo lucro-incompetência”

Novo Modelo de Contratação de TI

- ✓ Estruturação dos recursos humanos de TI com servidores permanentes e capacitados na gestão de TI (Acórdãos 786/2006-Plenário e 1.603/2008-Plenário)
- ✓ Planejamento da contratação
- ✓ Parcelamento dos serviços de TI em tantos itens quantos sejam tecnicamente possíveis, convenientes ao órgão e economicamente viáveis
- ✓ Licitação independente (adjudicação) para cada um dos itens

Novo Modelo de Contratação de TI

- ✓ Prestação e pagamento por serviços mensurados por resultado alcançado e verificado, e não por horas trabalhadas
- ✓ Avaliação da qualidade dos serviços
- ✓ Controle efetivo da execução dos serviços (aperfeiçoamento da gestão do contrato)

TRIBUNAL DE CONTAS DA UNIÃO

AGENDA

- ✓Conceitos
- ✓Governança x Gestão
- ✓E se não houver Governança de TI?
- ✓Governança de TI e a NBR ISO/IEC 38.500:2009
- ✓Modelos de contratação
- ✓Avaliação de Governança de TI

Levantamento de Governança da 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 de TI
- ✓ 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

2007: 2 grandes fiscalizações de TI

- ✓ Acórdão 1.603/2008-TCU-Plenário
  (Min. Guilherme Palmeira)
- ✓ Acórdão 2.471/2008-TCU-Plenário
  (Min. Benjamin Zymler)

Acórdão 1.603/2008-TCU-Plenário (Min. Guilherme Palmeira)

Alguns dados do TC 008.380/2007-1

- ✓1º Levantamento de Governança de TI
- ✓255 jurisdicionados pesquisados
- ✓Questionário com 39 questões
- ✓Jurisdicionados deveriam anexar evidências

Acórdão 1.603/2008-TCU-Plenário

- ✓51% NÃO alocam gastos de TI de acordo com planejamento
- ✓51% NÃO seguem metodologia de desenvolvimento de sistemas
- ✓57% NÃO têm carreira específica para TI
- ✓59% NÃO têm planejamento estratégico em vigor
- ✓64% NÃO têm política de segurança da informação
- ✓75% NÃO fazem análise de riscos de TI
- ✓80% NÃO fazem classificação da informação
- ✓88% NÃO têm plano de continuidade de negócios

Acórdão 2.471/2008-TCU-Plenário (Min. Benjamin Zymler)

- ✓Verificação da Governança de TI *in loco*
- ✓12 auditorias, em 7 UF
- ✓25 questões de auditoria
- ✓77 achados (auditoria integrada)

Verificação *in loco* da Governança de TI

Conclusão:

✓Confirmada a falta de governança nos 12 casos

✓Situação pior que a declarada no questionário

Acórdão 2.308/2010-TCU-Plenário (Min. Aroldo Cedraz)

Alguns dados do TC 000.390/2010-0

- ✓2º Levantamento de Governança de TI
- ✓300 jurisdicionados pesquisados
- ✓30 perguntas – 152 subitens
- ✓Divididas segundo 7 dimensões do Gespública
    - Liderança, Estratégias e planos, Cidadãos, Sociedade, Informações e conhecimento, Pessoas, Processos
- ✓Evidências conforme solicitado

Acórdão 2.308/2010-TCU-Plenário

Dimensão Processos:

✓53% **NÃO** têm processo de software ao menos gerenciado
✓63% **NÃO** aprovam e publicam PDTI interna ou externamente
✓65% **NÃO** possuem política corporativa de SI
✓74% **NÃO** inventariam todos os ativos de informação
✓75% **NÃO** gerenciam os incidentes de SI
✓83% **NÃO** analisam os riscos aos quais a informação está submetida
✓89% **NÃO** classificam a informação para o negócio
✓97% **NÃO** possuem plano de continuidade de negócio em vigor

Acórdão 2.308/2010-TCU-Plenário

Dimensão Liderança:
A Alta Administração **NÃO** :

✓... se responsabiliza pelas políticas de TI (51%)
✓... designou formalmente um comitê de TI (48%)
✓... estabeleceu objetivos de desempenho de gestão e uso de TI (57%)
✓... definiu indicadores de desempenho de gestão e uso de TI (76%)

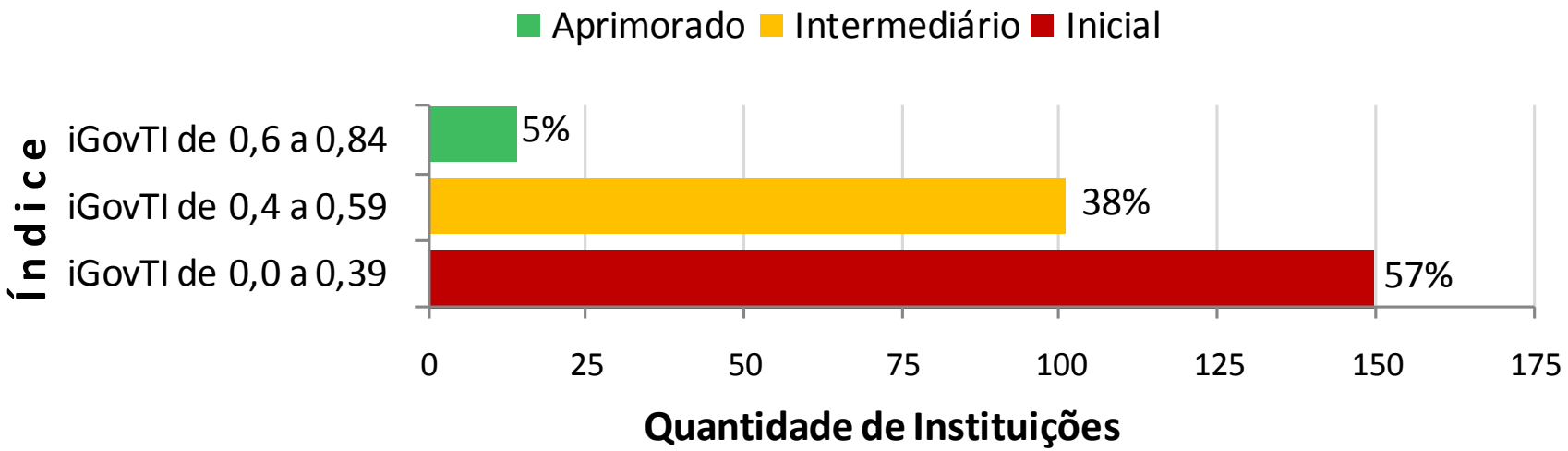
Acórdão 2.308/2010-TCU-Plenário

Melhorias observadas:

- ✓ Planejamento estratégico institucional
  - 2007 – 53%
  - 2010 – 79% (e.g.: Resolução - CNJ 70/2009)
- ✓ Carreira de TI
  - 2007 – 43%
  - 2010 – 78% (e.g.: SISP – ATI+GSISP)

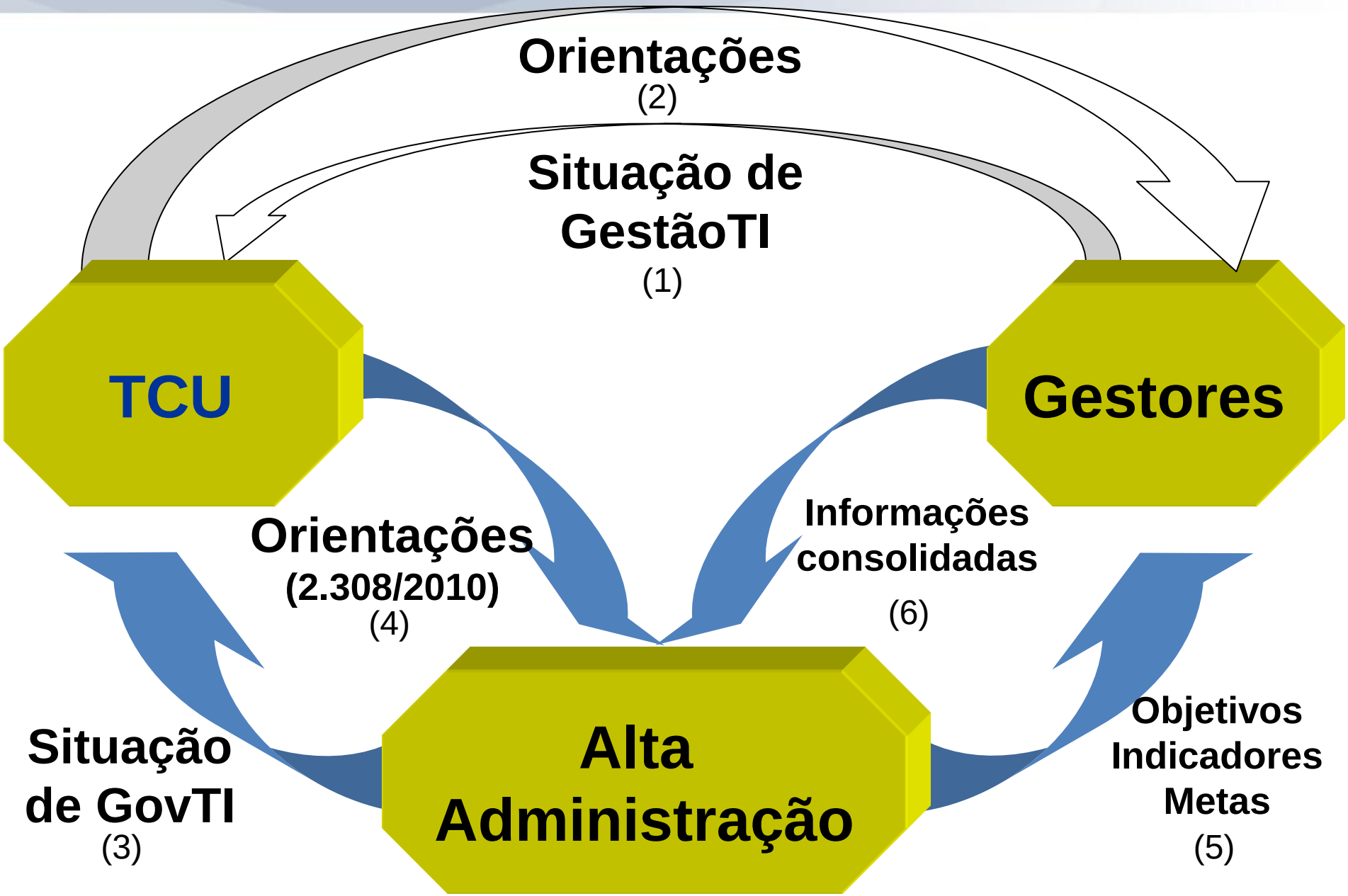
2010 - iGovTI

Instituições x Estágios do iGovTI

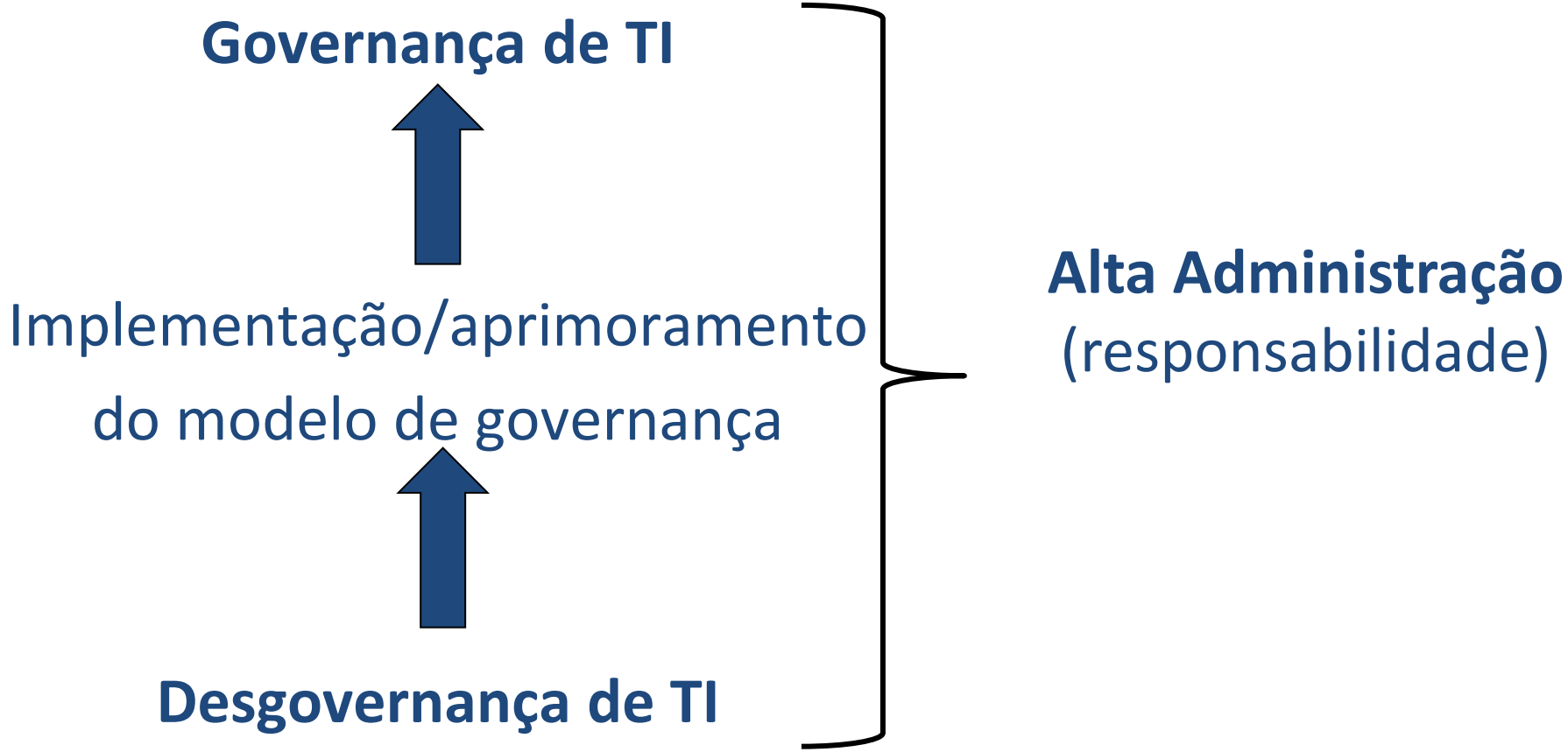


Acórdão 2.308/2010-TCU-Plenário

- ✓Recomendações aos OGS para que oriente a Alta Administração a definir:
  - ✓Objetivos institucionais de TI
  - ✓Indicadores para cada objetivo
  - ✓Metas para cada indicador
  - ✓Mecanismos para acompanhar desempenho da TI


Orientações
(2)
Situação de GestãoTI
(1)
TCU
Gestores
Orientações
(2.308/2010)
(4)
Informações consolidadas
(6)
Situação de GovTI
(3)
Alta Administração
Objetivos
Indicadores
Metas
(5)

E essa dinâmica deve gerar mudanças...



O que fazer? Por onde começar?

- ✓ Conhecemos a situação da nossa Governança de TI?
  - ✓ Precisamos fazer um diagnóstico!
- ✓ A Alta Administração da APF recebeu o resultado (inclusive comparativo) contido no Acórdão 2.308/2010-TCU-Plenário.

A Alta Administração deve...

- ✓Estabelecer formalmente:
  - ✓Objetivos institucionais de TI alinhados às estratégias de negócio (dirigir)
  - ✓Indicadores para cada objetivo (dirigir)
  - ✓Metas para cada indicador (dirigir)
  - ✓Mecanismos para acompanhar o desempenho da TI da instituição (monitorar)

Atingimos nossos objetivos?

- ✓ Conceituar os aspectos relacionados à boa governança para assegurar uma boa gestão de TI
- ✓ Avaliar casos em que a falta de governança gerou situações problemáticas para a Administração
- ✓ Analisar a evolução dos modelos de contratação de TI
- ✓ Obter um panorama da situação da Governança de TI na Administração Pública Federal

TRIBUNAL DE CONTAS DA UNIÃO

Uso de TIC nas IFES
Planejamento e Governança

OBRIGADO!

Daniel Moreira Guilhon, CISA
guilhondm@tcu.gov.br
(98) 8400-8534