Governança e Contratação de TI

Ministro-Substituto Augusto Sherman

Brasília, 9 de abril de 2012

Agenda

1. Governança de TI
2. Situação Governança de TI na Administração Pública Federal
3. O papel da Alta Administração na Governança de TI
4. Problemas advindos da baixa Governança de TI
5. Novo Modelo de Contratação de TI
6. Como implantar a Governança de TI na Administração Pública

1. Governança de TI

Alta dependência da TI

- ✓ O que ocorreria se falhassem, por exemplo, os sistemas que controlam:
  - ... o recebimento do IRPF?
  - ... o pagamento do Bolsa Família?
  - ... o pagamento de aposentadorias?
  - ... o andamento dos processos judiciais?
  - ... as sessões do Congresso Nacional?
  - ... as publicações da Imprensa Nacional?
  - ... as eleições no País?

Governança de TI

Definição

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

  (NBR 38.500)

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

Governança de TI

Responsabilidade

A responsabilidade por prover uma boa governança de TI é da **alta administração** da organização

(NBR 38.500)

2. Situação da Governança de TI na Administração Pública Federal

Levantamento de Governança de TI 2010

- ✓ Órgãos/entidades da Administração Pública Federal pesquisados:
  - 265 no prazo, incorporados ao relatório (Acórdão 2308/2010-TCU-Plenário)
  - 301 (100% alcançado em junho de 2011)
- ✓ Questionário com 30 perguntas (152 subitens), divididas segundo 7 dimensões do Gespública:
  - Liderança
  - Estratégias e planos
  - Cidadãos
  - Sociedade
  - Informações e conhecimento
  - Pessoas
  - Processos

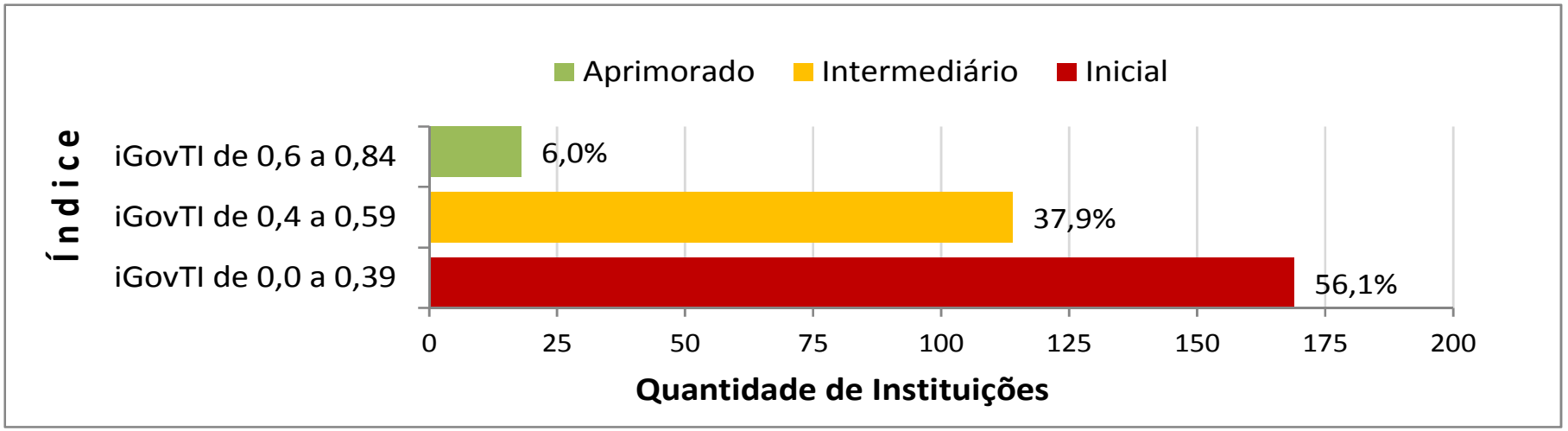
Melhorias observadas

Houve melhorias em relação ao levantamento de 2008?

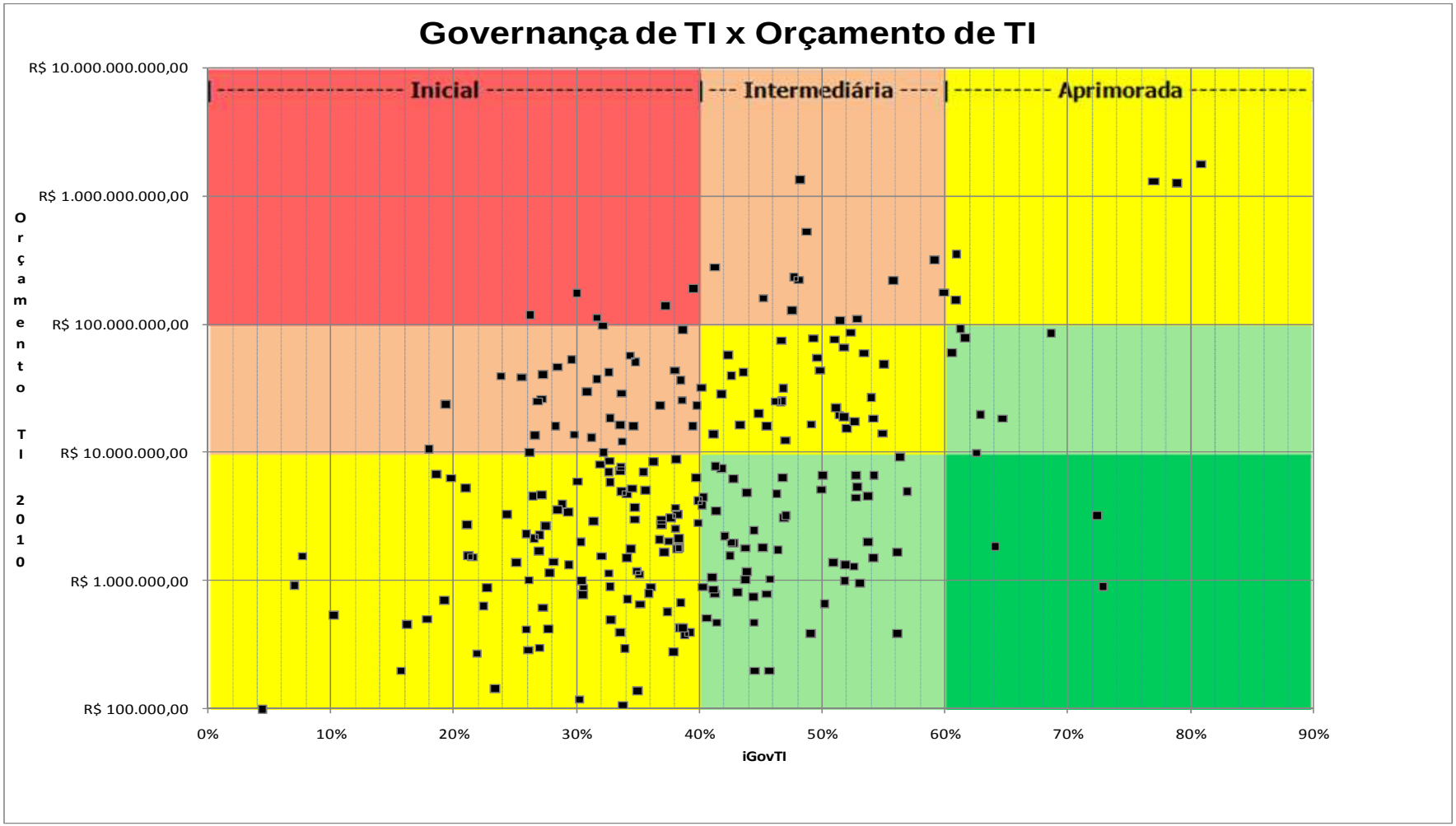
- ✓ Planejamento estratégico institucional
  - 2007 – 53%
  - 2010 – 79% (por ex. Res. CNJ 70/2009)
- ✓ Carreira de TI
  - 2007 – 43%
  - 2010 – 78% (por ex. SISP – ATI+GSISP)
  - ✓ Os indicativos de melhoria em planejamento e em quadro de pessoal sinalizam possibilidade de avanço em outras dimensões no futuro.

Índice de Governança de TI - iGovTI

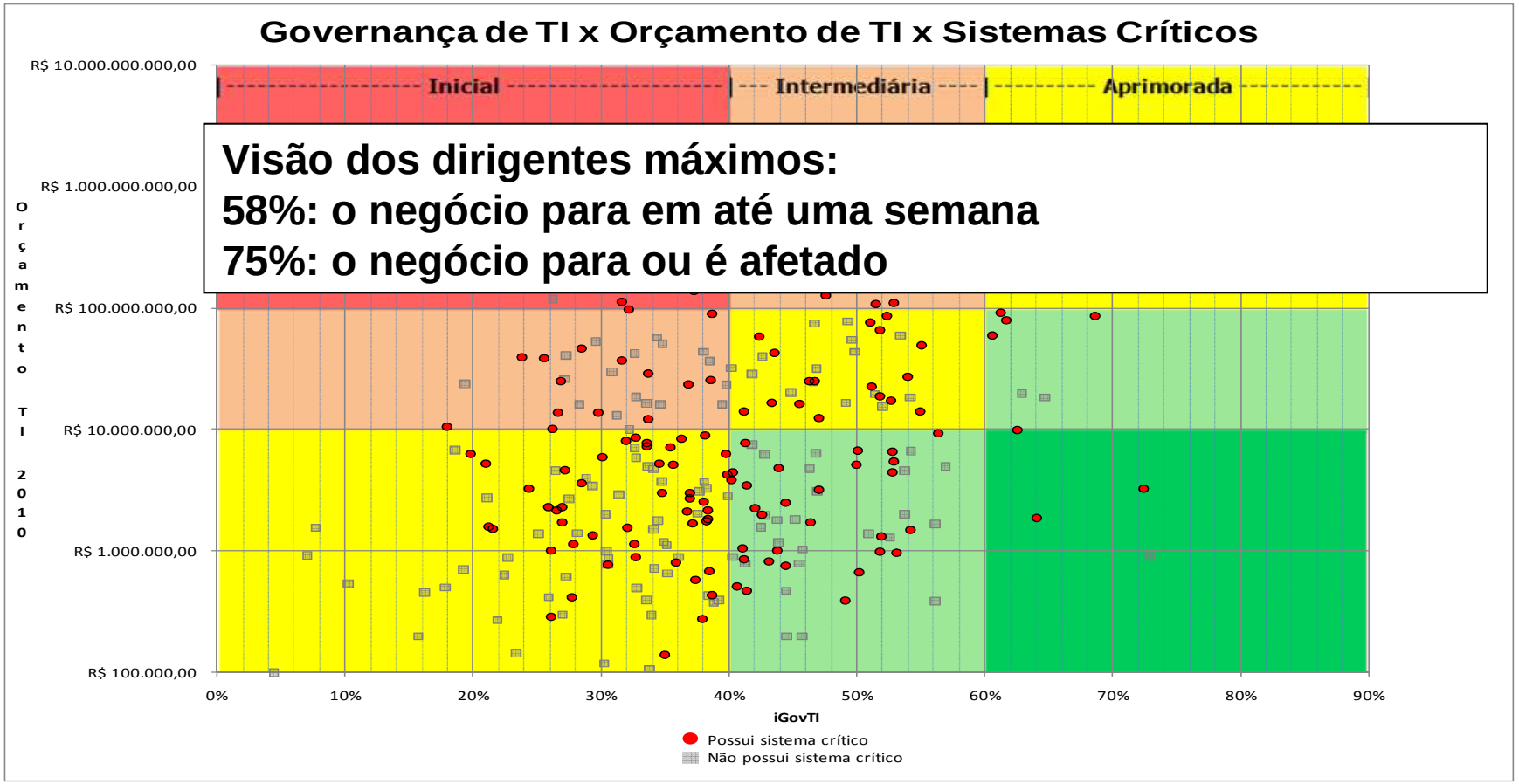
- ✓ Criado a partir de parâmetros do Cobit e das 7 dimensões do Gespública
- ✓ Instituições e estágios do iGovTI:



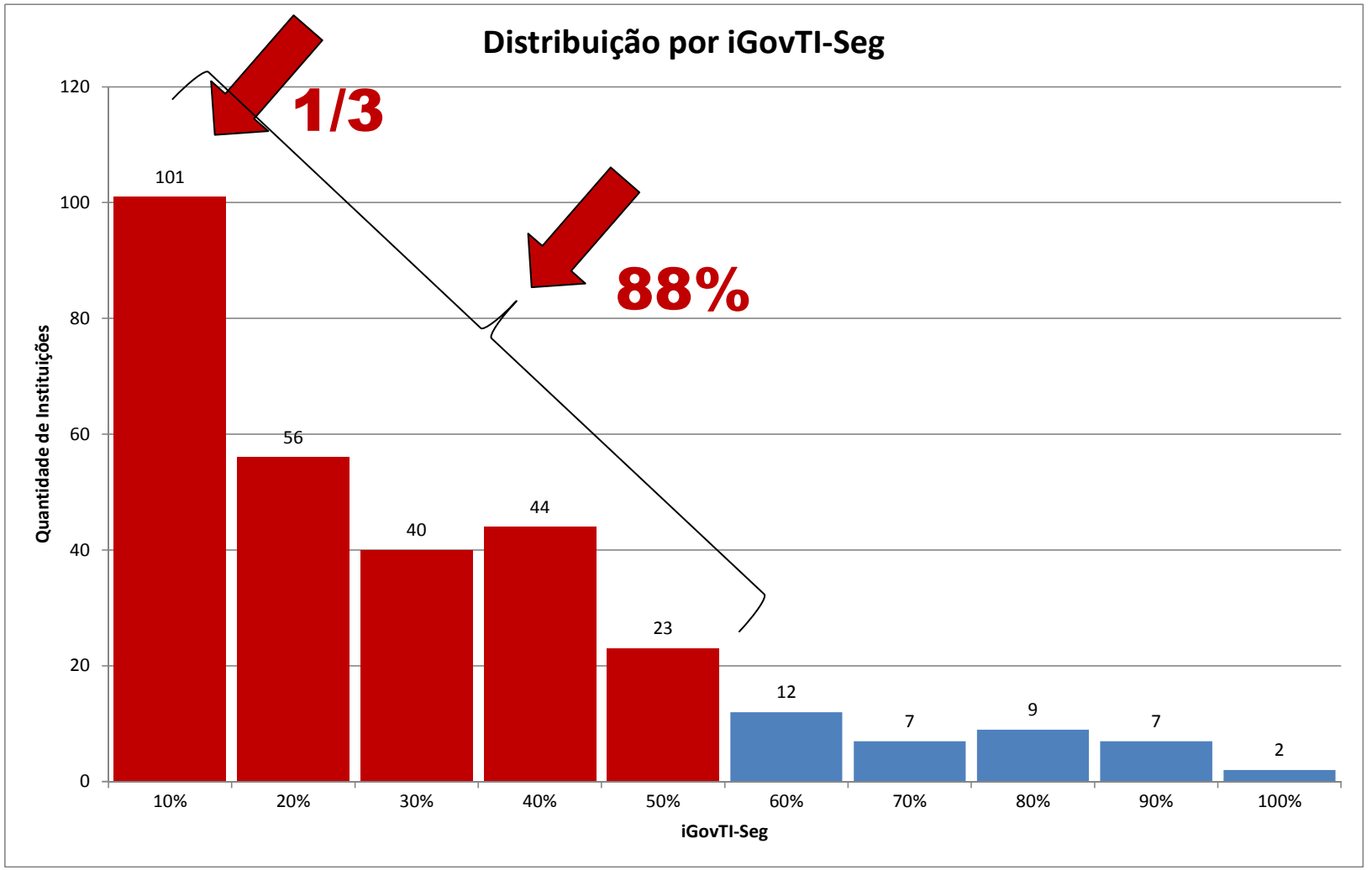
Risco de TI em função de iGovTI e Orçamento de TI



Risco de TI em função de iGovTI, Orçamento de TI e Sistemas Críticos



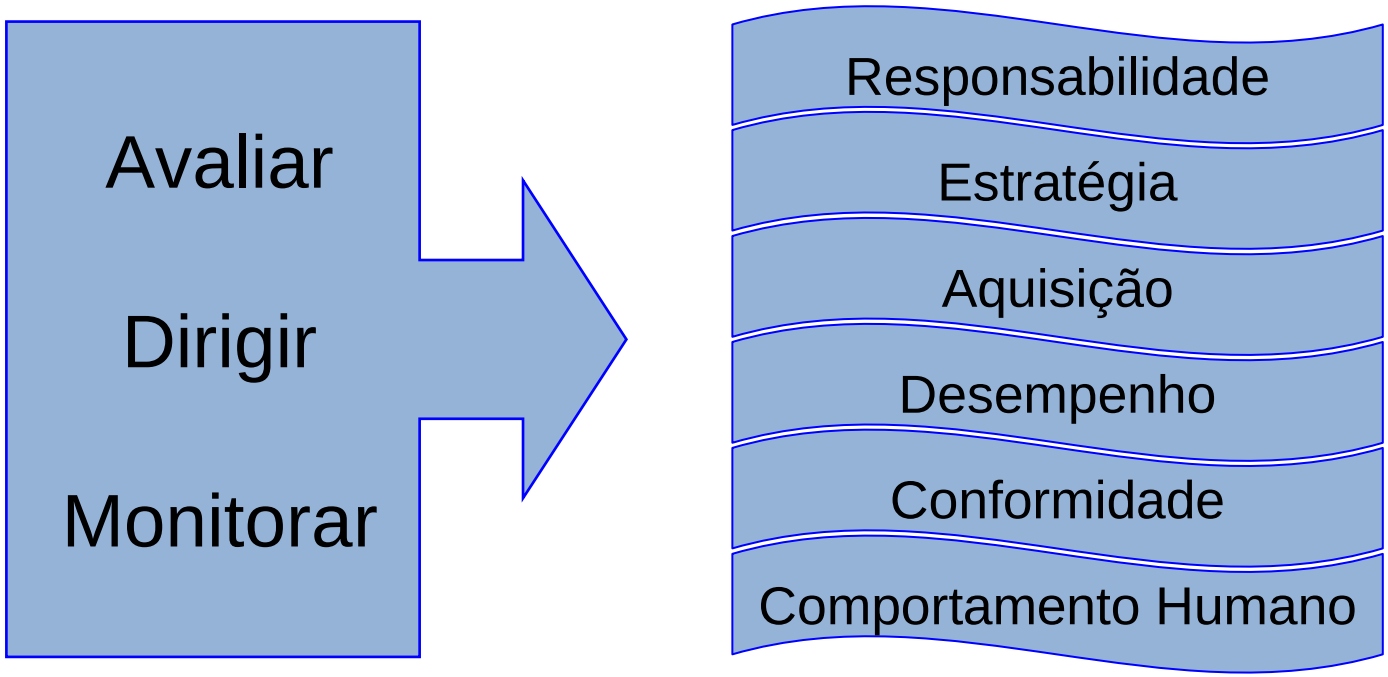
Riscos de TI:
IGovTI – Segurança da Informação



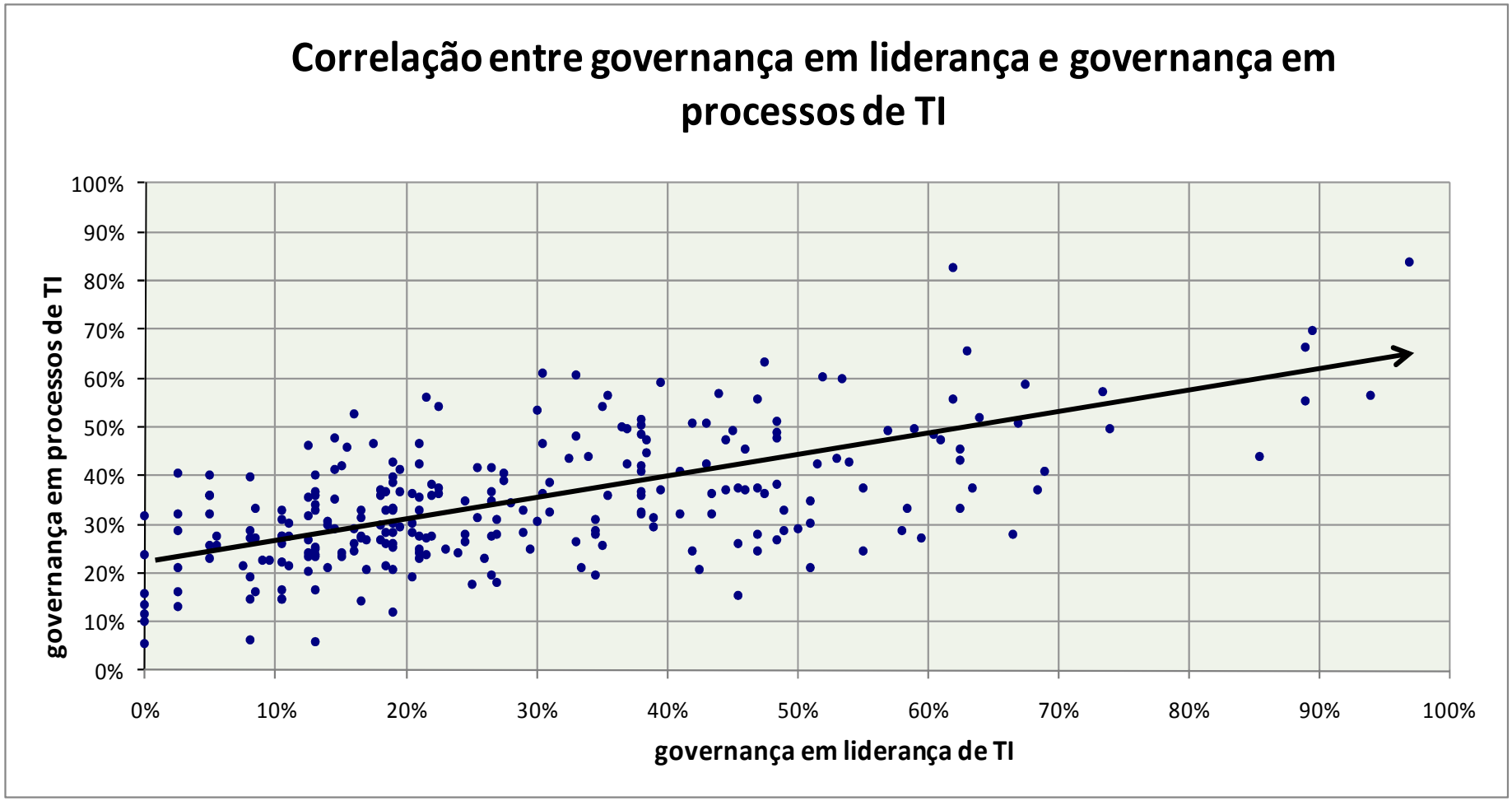
3. O Papel da Alta Administração na Governança de TI

Papel da Alta Administração

Baseado na NBR 38.500, governar a TI é:



Papel da liderança na Governança de TI



Coeficiente de correlação=0,60

Temas que merecem atenção

Resultados

(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 segurança da informação**

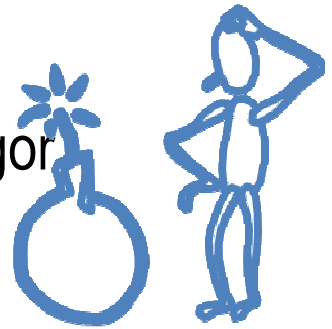
74% NÃO inventariam todos os **ativos de informação**

75% NÃO gerenciam os incidentes de segurança da informação

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



Temas que merecem atenção

Resultados

(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 de TI (**57%**)
- ✓ ... definiu indicadores de desempenho de gestão e uso de TI (**76%**)

Encaminhamento dos resultados

O relatório contendo os **resultados individuais** de cada instituição, incluindo **comparações por segmento**, foi encaminhado em setembro de 2010 e novamente em julho de 2011, sempre destinado ao **dirigente máximo**.

4. Problemas Advindos da Baixa Governança de TI

1º) Ausência de Plano de Continuidade de Negócio em vigor (97%)

✓ Situação:

- **Ausência** de Plano de Continuidade do Negócio
- **Falta/deficiência** de recursos ou planos de contingência

✓ Exemplos reais:

- Acórdão 172/2008-TCU-2ª Câmara
- Acórdão 1.330/2008-TCU-Plenário

1º) Ausência de Plano de Continuidade de Negócio em vigor (97%)

✓ Consequências:

- **Falha nos equipamentos de processamento centralizado** provocou (Acórdão 172/2008):
  - Paralisação do Banco **por mais de 20h**
  - Danos à imagem
  - Prejuízos financeiros
- **Vírus** gerou **paralisação da rede por mais de duas semanas** (Acórdão 1330/2008)

2º) Ausência de processo de software gerenciado - nível 2 da NBR 15.504 (53%)

- ✓ Exemplo Real: TC 031.963/2008-0
- ✓ Situação:
  - Edital e projeto básico **não possuíam indicadores de qualidade e desempenho** (níveis de serviço ou parâmetros de performance)
  - **Processo de homologação do produto sem viés técnico** e sem verificar a solução de TI em sua **integralidade**
    - Homologação focada só na usabilidade (ponto de vista do usuário)
    - Homologação focada no aceite de casos de uso individual (ausência de testes integrais)

2º) Ausência de processo de software gerenciado - nível 2 da NBR 15.504 (53%)

✓ Consequências:

- Produto **apresentou problemas de 2004 a 2007** (momento da entrega da solução completa)
- Procedimento de **homologação não garantiu a qualidade** do produto e não logrou exigir correções pela contratada
- **Não implantação do sistema**, apesar de ter sido **homologado e pago**

3º) Ausência de aprovação e publicação do PDTI interna ou externamente (63%)

- ✓ Exemplo Real: Acórdão 2.023/2005-TCU-Plenário
- ✓ Situação:
  - Planejamento deficiente
- ✓ Consequência:
  - **Desenvolvimento de sistema em 2000/2001**, considerado relevante e aprovado nos testes
  - **Ausência de infraestrutura necessária** à execução do sistema (infraestrutura de rede, servidores e equipamentos)
  - **Sistema não implantado até 2005**

4º) Ausência de política corporativa de segurança da informação (65%)

- ✓ Exemplo Real: Acórdão 71/2007-TCU-Plenário
- ✓ Situação:
  - **Sistema de âmbito nacional com informações confidenciais** e relevantes dos cidadãos
  - Minuta de Política de Segurança da Informação **(PSI) desatualizada e não formalmente aprovada**
  - **Política de Controle de Acesso** deficiente

4º) Ausência de política corporativa de segurança da informação (65%)

✓ Consequências:

- Dificuldade na **identificação de responsabilidades** quanto aos assuntos de segurança da informação
- **Grande vulnerabilidade** do sistema
- **Vazamento e mau uso de informações** privadas e confidenciais dos cidadãos
- **Atraso na implementação** total do sistema

5. Novo Modelo de Contratação de TI

Antigo modelo de contratação de TI

Consiste 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 CPD completo e terceirizado.

Antigo modelo de contratação de TI

Desvantagens desse Modelo

(Vide Acórdão 786/2006-TCU-Plenário):

- ✓ **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”

Necessidade de Novo Modelo

As significativas desvantagens do modelo de contratação de serviços de TI que vinha sendo praticado na Administração apontaram a necessidade de um **novo modelo**, um **novo paradigma !**

Atual Modelo de Contratação de TI

O atual modelo de contratação de TI se baseia:

- ✓ na **estruturação dos recursos humanos de TI** com servidores permanentes e capacitados na gestão de TI

(Acórdãos 786/2006-Plenário e 1.603/2008-Plenário)

- ✓ no **planejamento da contratação**
- ✓ no **parcelamento do objeto da licitação** em tantos itens quantos sejam tecnicamente possíveis e economicamente viáveis:
  - em **licitação independente** (ou adjudicação independente) para cada um dos itens
  - no estabelecimento de **exigências de habilitação e de avaliação da proposta técnica específicas para cada serviço**

Atual Modelo de Contratação de TI

O atual modelo de contratação de TI se baseia (continuação):

- ✓ na **prestação e pagamento por serviços mensurados por resultado alcançado e verificado**, e não por horas trabalhadas
- ✓ na **avaliação de qualidade** dos serviços
- ✓ no **controle efetivo da execução** dos serviços (aperfeiçoamento da gestão do contrato)

6. Como Implantar a Governança de TI na Administração Pública

Acórdão 2.308/2010-TCU-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)

Como implantar a Governança de TI na Administração Pública

- ✓ Passo 1: Obter, capacitar e valorizar **recursos humanos**
- ✓ Passo 2: Aprovar um **Plano Estratégico Institucional**
- ✓ Passo 3: Aprovar um **Plano Estratégico de TI**
- ✓ Passo 4: Criar um **Comitê de TI**
- ✓ Passo 5:
- ✓ Passo 6: Utilizar a **Auditoria Interna**
- ✓ Passo 7: **Monitorar** os **resultados**

Passo 1:
Priorizar Política de Recursos humanos

Obter, capacitar e valorizar os recursos humanos na área de TI:

"91.Todavia, deve-se ressaltar que esses resultados somente serão plenamente alcançados se os órgãos e entidades da Administração Pública estiverem preparados para ***executar as atividades estratégicas de planejar, definir, especificar, supervisionar e controlar a operação de seus setores de informática*** *de maneira independente das empresas prestadoras de serviço."*

(excerto do voto condutor do Acórdão 786/2006-TCU-Plenário)

Passo 2:
Aprovar Plano Estratégico Institucional (PEI)

- ✓ O que é?
  - Definir negócio, missão, visão, valores
  - Objetivos, indicadores, metas **do negócio**
  - Iniciativas, estratégias
  - Desdobramento
  - Divulgação
- ✓ Onde obter ajuda:
  - 79% dos pesquisados declararam que fazem (Acórdão 2.308/2010-TCU-Plenário)
  - Enap possui treinamento regular
  - C3S da SLTI/MP (SISP)

Passo 3:
Aprovar Plano Estratégico de TI (PETI)

- ✓ O que é?
  - Conteúdo semelhante ao PEI (objetivos, indicadores, metas **da TI**, iniciativas, estratégias, desdobramento, divulgação) e mais...
  - Alocação de **recursos** (financeiros, humanos, materiais)
  - **Alinhamento** com o negócio
  - Estratégia de **terceirização**
- ✓ Onde obter ajuda:
  - 37% dos pesquisados declararam que fazem (Acórdão 2.308/2010-TCU-Plenário)
  - Enap possui treinamento regular
  - C3S da SLTI/MP (SISP)

Passo 4:
Criar um comitê de TI

- ✓ O que é?
  - Instância (consultiva ou deliberativa) de **apoio à alta administração**
  - **Cobit 4.1**, objetivo de controle **PO4.3 Comitê Executivo de TI**: *"Estabelecer um comitê executivo composto pelas diretorias executiva, de negócios e de TI para:*
  - ***determinar prioridades dos programas de investimentos em TI*** *em linha com as estratégias e prioridades do negócio;*
  - ***monitorar o estado atual dos projetos*** *e resolver conflitos de recursos; e*
  - ***monitorar níveis de serviço*** *e suas melhorias."*
- ✓ Onde obter ajuda:
  - 32% dos pesquisados declararam que têm (Acórdão 2.308/2010)
  - C3S da SLTI/MP (SISP)

Passo 5:
Implantar Processo de Software

- ✓ O que é?
  - Definição de um processo, ou seja, uma sequência de passos realizados para um **aquisição, desenvolvimento ou manutenção de software** pela organização;
  - Envolve **métodos, técnicas, ferramentas e pessoas**;
  - Deve ser estabelecido uma **arquitetura** de alto nível do **ciclo de vida de software** que é construída a partir de um conjunto de processos e seus inter-relacionamentos;
- ✓ Onde obter ajuda
  - 47% dos pesquisados declararam que têm processo ao menos gerenciado (Acórdão 2.308/2010)
  - C3S da SLTI/MP (SISP)

Passo 6:
Utilizar a Auditoria Interna

- ✓ O que é?
  - *"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)
- ✓ Onde obter ajuda:
  - 10% dos pesquisados declararam que fazem auditoria de governança de TI

    (Acórdão 2.308/2010-TCU-Plenário)
  - Cursos do TCU/Sefti (IATI, Avaliação de Controles Gerais de TI)

Passo 7:
Monitorar os resultados

- ✓ O que é?
  - Acompanhar os **indicadores**
  - **Analisar riscos** (com base no impacto no negócio)
  - **Priorizar** ações
  - Acompanhar **ações críticas**
- ✓ Onde obter ajuda:
  - 23% dos pesquisados declararam que fazem (Acórdão 2.308/2010-TCU-Plenário)

Reforçando

Governar a TI é ação da Alta Administração, e não da área de TI.

Obrigado !

Ministro-Substituto Augusto Sherman