Gestão e Uso da TI na APF

Renato Braga, CISA, CIA, CGAP, CCI

Brasília, 05 de novembro de 2012

“Feliz aquele que transfere o que sabe e aprende o que ensina”

Cora Coralina,

poeta goiana.

Objetivo

- Apresentar a auditoria realizada pelo TCU para avaliar a gestão e o uso dos recursos de tecnologia da informação pela Administração Pública Federal (APF), os principais resultados da avaliação e as medidas estruturantes propostas.

Na íntegra:
Acórdão 1.233/2012-TCU-Plenário

Relator:

Exmº Ministro Aroldo Cedraz

Agenda

- Por que TI é importante na APF?
- Como foi feita a avaliação?
- Resultados da avaliação
- Aspectos legais nas contratações de TI
- Governança Corporativa x Governança de TI

Evolução dos gastos com TI

- 2006 – R$ 6 bilhões (executado)
  - OFSS + OI
- 2012 – R$ 14,8 bi (previsão)
  - R$ 7,0 bi (OFSS)
  - R$ 7,8 bi (OI)

Impacto da TI na gestão pública

Criticidade (Se o sistema parar, o negócio...)	Maturidade inicial	Maturidade intermediária	Maturidade aprimorada	Total	
... para imediatamente.	82	63	9	154	51%
... para em uma semana.	12	6	3	21	7%
... para em um mês.	5	1	-	6	2%
... é afetado, mas não para.	27	13	3	43	14%
... não é afetado.	50	26	1	77	26%
Total	176	109	16	301	100%

Fonte: dados da fiscalização do Acórdão 2.308/2010-TCU-Plenário

Agenda

- Por que TI é importante na APF?
- Como foi feita a avaliação?
- Resultados da avaliação
- Aspectos legais nas contratações de TI
- Governança Corporativa x Governança de TI

Tema de Maior Significância (TMS)

- *... consideram-se temas de maior significância aqueles identificados em função de fatores de risco, materialidade, relevância e oportunidade e que estejam em consonância com o Plano de Diretrizes do Tribunal.*

(Resolução TCU 185/2005, art. 4º, § 1º)

Objetivo Geral do TMS 6/2010

- Avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas da governança de TI.

Objetivos específicos do TMS

- Levantamento da situação da governança de TI na APF (perfil GovTI2010);
- Avaliação de controles gerais de TI em 14 jurisdicionados;
- Validação das respostas dos questionários perfil GovTI2010 (nos 14 jurisdicionados);
- Avaliação de 4 objetos específicos de TI;

Objetivos específicos do TMS

- Avaliação da atuação dos órgãos governantes superiores (SLTI/MP, GSI/PR, CGU/PR etc);
- Obtenção da (possível) relação de causa-efeito entre maturidade dos controles gerais de TI e desconformidades nos objetos específicos de TI;
- Obtenção da (possível) relação de causa-efeito entre a atuação dos órgãos governantes superiores e a situação da governança de TI na APF;

Objetivos específicos do TMS

- Ratificação ou retificação da situação da governança de TI declarada no perfil GovTI2010, em confronto com a que for evidenciada *in loco*;
- Disseminação no TCU da expertise para avaliação de controles gerais de TI.

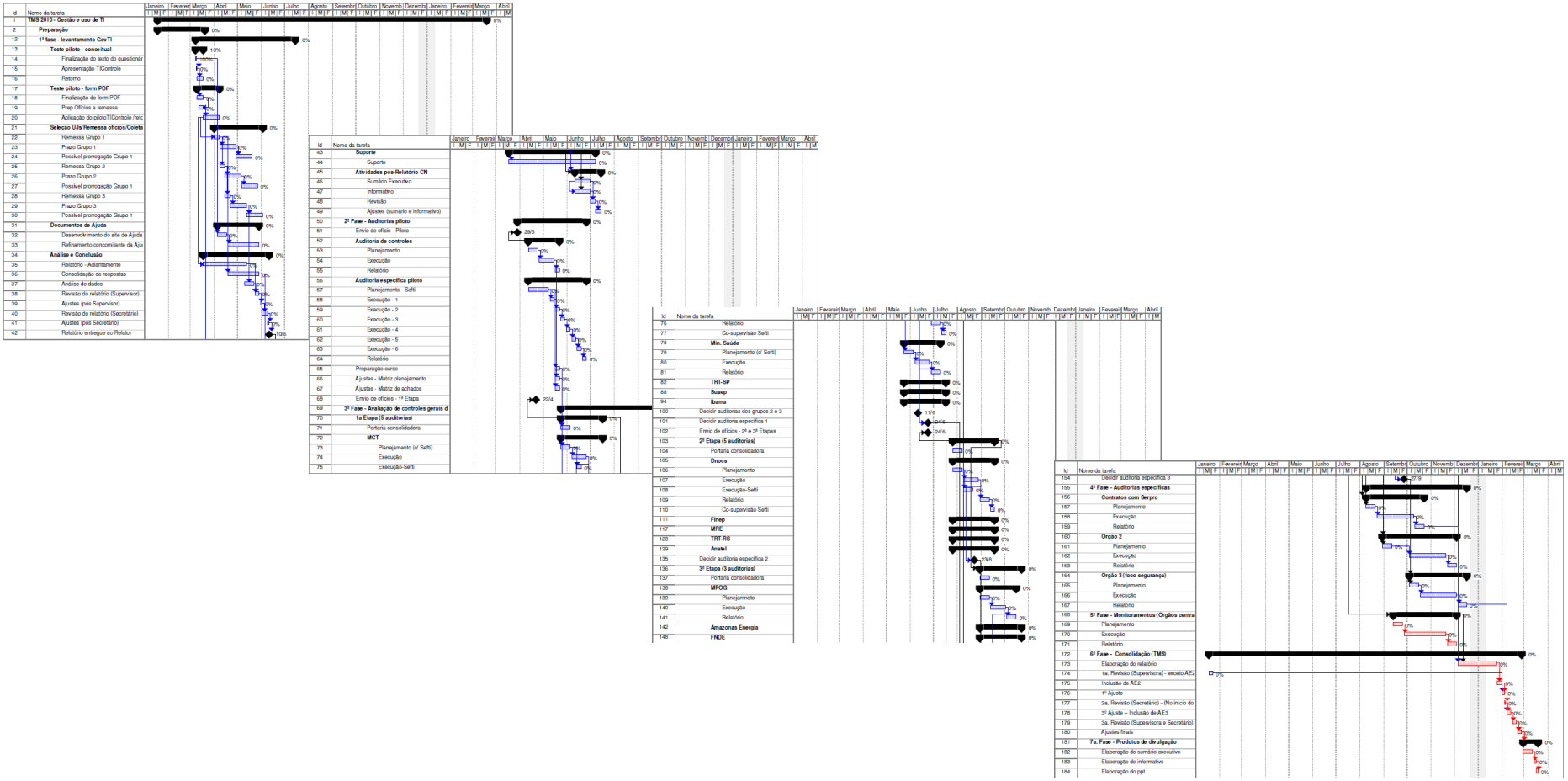
Fiscalizações integrantes do TMS

- 1 levantamento de auditoria (preparação);
- 1 levantamento de auditoria (perfil GovTI2010);
- 14 auditorias para avaliação de controles gerais de TI (FOC – Fiscalização de Orientação Centralizada);
- 4 auditorias em objetos específicos de TI;
- 1 monitoramento de deliberações com orientações aos OGS.

Preparação

- Projeto do TMS
- Dados orçamentários de TI
- Planejamento da FOC
  - Papéis de trabalho
    - Matriz de planejamento
    - Ofício de requisição inicial
    - ...
  - Material de treinamento

Projeto do TMS
(coordenando 21 fiscalizações...)



Perfil GovTI2010

- 321 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

Avaliação de controles gerais de TI (FOC)

- 14 auditorias, em 8 UF
  - 4 ministérios
  - 5 autarquias
  - 1 fundação
  - 2 tribunais
  - 1 empresa pública
  - 1 sociedade de economia mista
- Amostra não estatística, logo não há como fazer inferências

Avaliação de controles gerais de TI
(FOC)

- 12 temas, 12 questões de auditoria
- 54 possíveis achados
- Fiscalização integrada (conformidade e operacional)
- Execução iterativa e incremental
- 29 auditores treinados, sendo 24 auditores de processos de negócio
- VRF: R$ 47,6 bilhões

Temas

T1 – Planejamento estratégico institucional

T2 – Planejamento estratégico de TI

T3 – Estrutura de TI

T4 – Orçamentação de TI

T5 – Processo de software

T6 – Gerenciamento de projetos

Temas

T7 – Gestão de serviços

T8 – Segurança da informação

T9 – Capacitação de profissionais de TI

T10 – Monitoração do desempenho da gestão de TI

T11 – Contratação de soluções de TI

T12 – Gestão de contratos de soluções de TI

Acórdãos estruturantes monitorados

“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)

Órgãos Governantes Superiores (OGS)

OGS monitorados

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

Novos OGS identificados

- Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo
  - Decreto 7.478/2011
- Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal
  - Decreto 5.707/2006
- Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR)
  - Decreto 6.021/2007

Avaliação de objetos específicos

- Sistema de Acompanhamento de Contratos (Siac) de Autarquia
- Sistema informatizado que suporta o Sistema Nacional de Transplantes
- Contratos da APF com empresa pública prestadora de serviços de TI
- Contrato cujo objeto é consultoria em segurança da informação

Avaliações de qualidade do TMS

- Auditores do TCU que participaram da FOC
  - objetivo: avaliar a atuação da Sefti como unidade coordenadora dos trabalhos
  - 90% de satisfação
- Responsáveis pelos entes auditados
  - objetivo: verificar a satisfação do auditado com a auditoria
  - 94% de satisfação

Agenda

- Por que TI é importante na APF?
- Como foi feita a avaliação?
- Resultados da avaliação
- Aspectos legais nas contratações de TI
- Governança Corporativa x Governança de TI

Preliminar

- Percepção de que há desconhecimento de aspectos relevantes, como:
  - controle interno <> auditoria interna;
  - governança de TI <> gestão de TI;
  - governança <> gestão;
  - de quem é a responsabilidade pela governança;
  - controles positivados na legislação (especialmente os de segurança da informação – normas do GSI/PR).

Acórdão 1.233/2012-TCU-Plenário

- Determinar à Sefti que “promova a divulgação dos critérios de auditoria contidos no Apêndice VIII.4, a fim de continuar a atividade de orientação que vem desenvolvendo;”

T1 - Planejamento Estratégico Institucional

Evidências
(Plano de Ação Global - PAG)

- Em 13 dos 37 órgãos com status de Ministério, o Regimento Interno não se refere a qualquer documento de planejamento institucional
- Para os outros 24 órgãos:
  - não há definição do que é o PAG
  - 17 (71%) não possui PAG
  - dos 7 que têm PAG:
    - 3 não não tem processo de trabalho para elaborá-lo;
    - 5 não dão lhe dão publicidade na Internet;
    - somente 1 foi aprovado pelo Ministro de Estado, conforme determinam os normativos.

Evidências

- Perfil GovTI2010
  - 21% declararam não executar processo de planejamento estratégico institucional
- Dos 14 auditados *in loco*, 1 passou pelos testes e:
  - 8 não possuíam plano
  - os outros 5 tinham falhas no plano ou falhas no processo de planejamento
  - no perfil govTI2010, 5 que declararam possuir o plano não o evidenciaram
- OGS
  - Só o CNJ atuou (Resolução 70/2009)

Acórdão 1.233/2012-TCU-Plenário

- Estabeleçam processo de planejamento estratégico institucional ... contemplando, pelo menos:
  - elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;
  - aprovação, pela mais alta autoridade da organização, do plano estratégico institucional;

Acórdão 1.233/2012-TCU-Plenário

- desdobramento do plano estratégico pelas unidades executoras;
- divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;
- acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;
- divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado.

T2 – Planejamento Estratégico de TI

Evidências

- Perfil GovTI2010
  - 61% declararam não executar processo de planejamento estratégico de TI
- Dos 14 auditados *in loco*:
  - 9 não possuiam plano
  - os outros 5 tinham falhas no plano ou falhas no processo de planejamento
  - no perfilgovTI, 2 que declararam possuir plano não o evidenciaram

Evidências

- OGS
  - CNJ (Resolução 99/2009)
  - SLTI (IN 4/2008)
    - Obriga a fazer, mas não orienta como fazer
- Exemplo de consequência:
  - Acórdão 2.023/2005-TCU-Plenário

Obs.: O PDTI ou PETI é documento da organização, não do setor de TI

Acórdão 1.233/2012-TCU-Plenário

- Estabeleçam processo de planejamento estratégico de TI... contemplando, pelo menos:
  - elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:
    - objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;
    - alocação de recursos (financeiros, humanos, materiais etc);
    - estratégia de terceirização

Acórdão 1.233/2012-TCU-Plenário

- aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;
- desdobramento do plano estratégico pelas unidades executoras;
- divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;
- acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;
- divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado.

T3 – Estrutura de TI

Avaliações

- Funcionamento dos comitês de TI;
- Definição e ocupação de papéis sensíveis dentro da TI;
- Forma de avaliação do quadro de pessoal de TI.

Comitês de TI

- Perfil GovTI2010
  - 68% declararam não possuir
- Nos 14 auditados *in loco*
  - 2 eram atuantes, 5 não atuavam e em 7 não havia
  - no perfilgovTI, 1 que declarou possuir comitê não o evidenciou

Acórdão 1.233/2012-TCU-Plenário

- Normatizem a obrigatoriedade do estabelecimento de comitês de TI.
- Orientem para que realizem avaliação quantitativa e qualitativa do pessoal do setor de TI.
- Disciplinem a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI.

T4 – Orçamentação de TI

Acórdão 1.233/2012-TCU-Plenário

- [SOF] normatize a obrigatoriedade de processo de trabalho formal para elaboração e acompanhamento da execução do orçamento, contemplando, pelo menos, a obrigatoriedade de que:
  - a solicitação do orçamento de TI seja feita com base nas estimativas de custos das atividades que pretendam executar, alinhadas aos objetivos do negócio da organização;
  - haja acompanhamento, ao longo do exercício financeiro, dos gastos efetuados especificamente com TI.
- [SOF e Dest] apresentem solução definitiva para transparência das informações orçamentárias

T5 – Processo de software

Acórdão 1.233/2012-TCU-Plenário

- Elaborem um modelo de processo de software para os entes sob sua jurisdição;

- Estabeleçam a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si.

Acórdão 1.233/2012-TCU-Plenário

- Orientem sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX.

Na mesma linha do tema T5, temos...

- T6 – Gerenciamento de projetos
- T7 – Gestão de serviços
  - Gestão de configuração
  - Gestão de incidentes
  - Gestão de mudanças

50

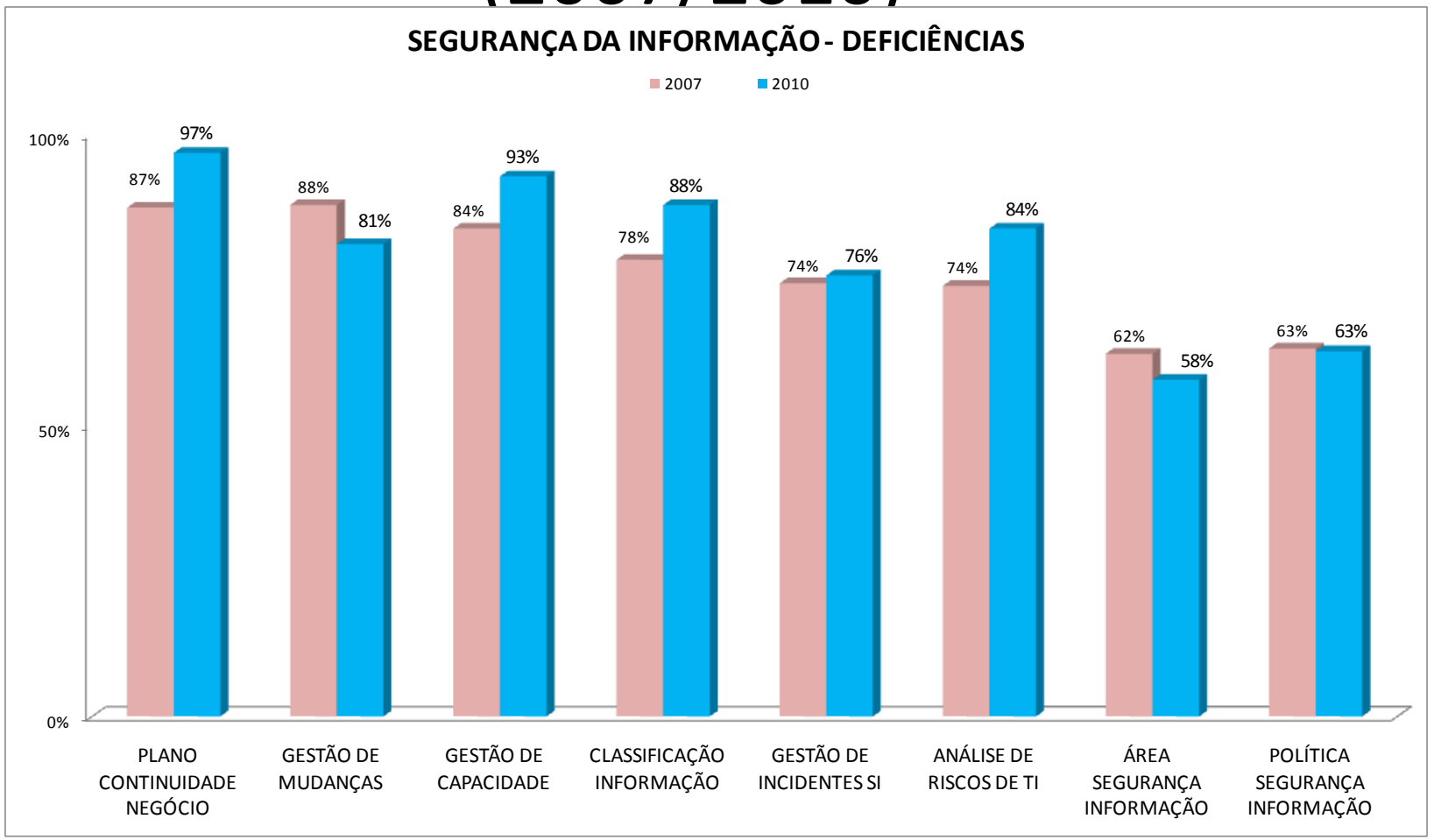
T8 – Segurança da informação

Avaliações

1. Existência de responsável pela segurança da informação;
2. Funcionamento do comitê de segurança da informação;
3. Política de segurança da informação;
4. Equipe de tratamento e resposta a incidentes em redes computacionais;
5. Inventário de ativos de informação;
6. Classificação da informação;
7. Gestão de riscos de segurança da informação.

52

Segurança da Informação (2007/2010)



fonte: Acórdão 2.308/2010-TCU-Plenário

Acórdão 1.233/2012-TCU-Plenário

- recomendar ao GSI/PR que:
  - ... articule-se com as escolas de governo, notadamente com a Enap, a fim de ampliar a oferta de ações de capacitação em segurança da informação;
  - ... oriente que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II.

54

Acórdão 1.233/2012-TCU-Plenário

- Demais OGS:
  - Normatizar obrigação de implantar os controles testados na auditoria (à semelhança do que fez o GSI/PR);
  - Criar procedimentos orientando como implantar tais controles.

T9 – Capacitação de profissionais de TI

Acórdão 1.233/2012-TCU-Plenário

- Recomendar ao Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal que:
  - oriente sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos do Decreto 5.707/2006, arts. 5º e 2º, c/c Portaria MP 208/2006, art. 2º, I, e art. 4º;
  - estabeleça, após consulta à SLTI, um programa de capacitação em governança e em gestão de tecnologia da informação.
- Recomendação análoga aos demais OGS

T11 – Contratação de soluções de TI
e
T12 – Gestão de contratos de soluções de TI

58

Avaliações

- Há controles que promovem:
  - cumprimento da IN - SLTI 4/2008 (vigente à época) ou
  - a realização dos obrigatórios estudos técnicos preliminares antes da elaboração do Termo de Referência ou Projeto Básico;
- A IN - SLTI 4/2008 é seguida, ou os estudos técnicos preliminares eram realizados;
- Conformidade nas contratações.

Avaliações

- Há controles que promovem a regular gestão contratual;
- Conformidade na gestão contratual.

Teses prospectadas e confirmadas

- Ausência de controles na contratação contribui para que o processo da IN - SLTI 4/2008 não seja cumprido ou os estudos técnicos preliminares não sejam realizados;
- Descumprimento do processo da IN - SLTI 4/2008 ou a não realização dos estudos técnicos preliminares contribui para desconformidades nas contratações;
- Ausência de controles na gestão contratual contribui para a sua desconformidade.

Acórdão 1.233/2012-TCU-Plenário

- Recomendar ao CNJ que:
  - a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, elabore um modelo de processo para contratação e gestão de soluções de tecnologia da informação para o Poder Judiciário ou, alternativamente, adote o modelo contido na IN - SLTI 4/2010;
  - promova a implementação do modelo mediante orientação normativa.
- Recomendação análoga à CGPAR e ao CNMP.

62

T10 – Monitoração do desempenho da gestão de TI

Avaliações

- A alta administração:
  - estabelece objetivos, indicadores e metas para a gestão de TI (Cobit 4.1, ME1.1 e PO1.4);
  - monitora a gestão de TI por meio de relatórios gerenciais (Cobit 4.1, ME1.5);
  - avalia a gestão de TI (Cobit 4.1, ME1.4);
  - determina ações corretivas, se for o caso (Cobit 4.1, ME1.6); e
  - utiliza a AI para apoiar a realização das três últimas tarefas acima (Cobit 4.1, ME2.2).

Evidências

(Acórdão 2.308/2010-TCU-Plenário)

- 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%)

A conclusão foi que há evidências de que...

- Alta administração geralmente não governa a TI
- AI geralmente não apoia a alta administração no monitoramento da TI

Acórdão 2.308/2010-TCU-Plenário

- OGS orientar devem orientar alta administração para que estabeleçam:
  - objetivos institucionais de TI
  - indicadores para cada objetivo
  - metas para cada indicador
  - mecanismos para acompanhar desempenho da TI

67

Acórdão 1.233/2012-TCU-Plenário

- OGS devem estabelecer normativamente a obrigatoriedade de a alta administração implantar uma estrutura de controles internos, mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades pelo menos no processos auditados.

68

Acórdão 1.233/2012-TCU-Plenário

- Recomendar ao CJN (CNMP) que estabeleça sistema de controle interno integrado para todo o Poder Judiciário (Ministério Público).

69

Acórdão 1.233/2012-TCU-Plenário

- Recomendar aos OGS que orientem as unidades de auditoria interna para que considerem os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (*e.g.*, IPPF 2110.A2, 2120.A1 e 2130.A1)

70

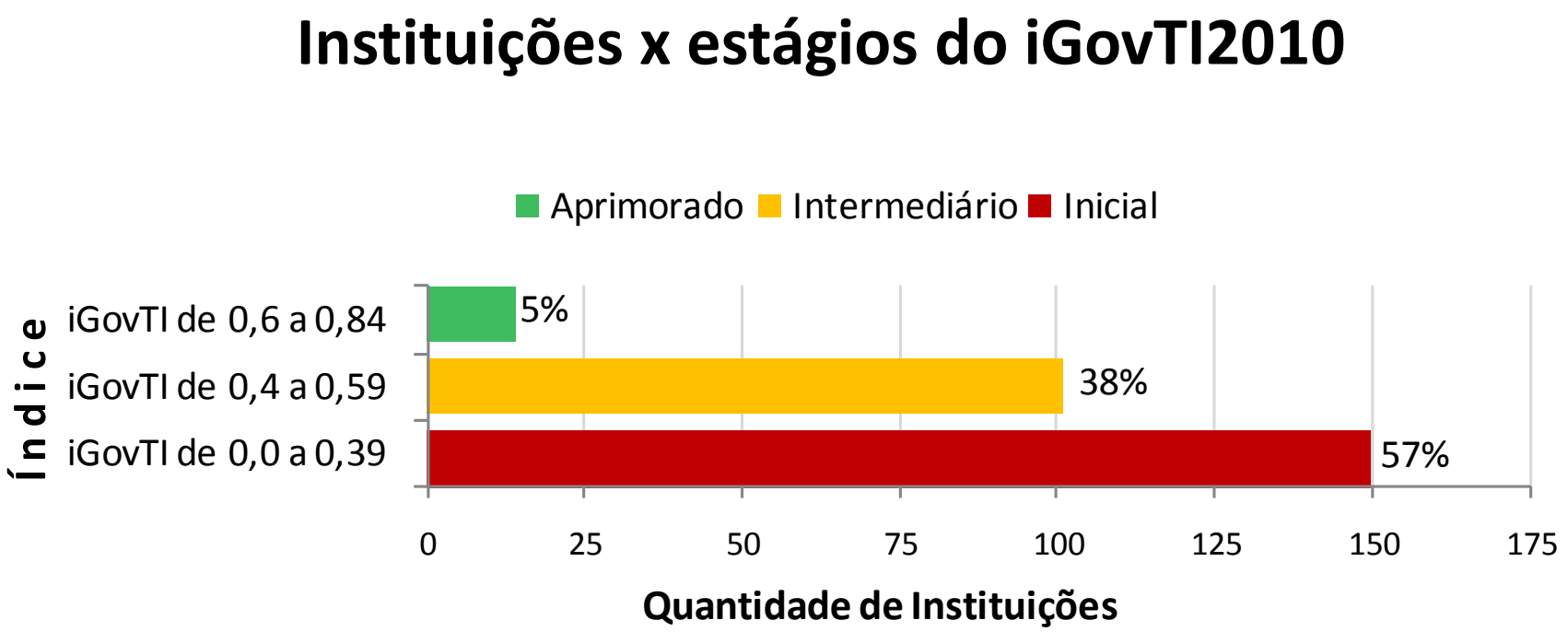
Acórdão 1.233/2012-TCU-Plenário

- *9.43. ...Tema de Maior Significância (TMS) com objetivo de avaliar a eficiência e eficácia dos sistemas de controles internos dos poderes da União, em especial como as unidades de auditoria interna atuam na avaliação da eficácia dos processos de gerenciamento de riscos, controle e governança dos órgãos e entidades da Administração Pública Federal, levando em consideração, inclusive, as boas práticas internacionais sobre o tema como o IPPF (International Professional Practices Framework) do Instituto de Auditores Internos;*

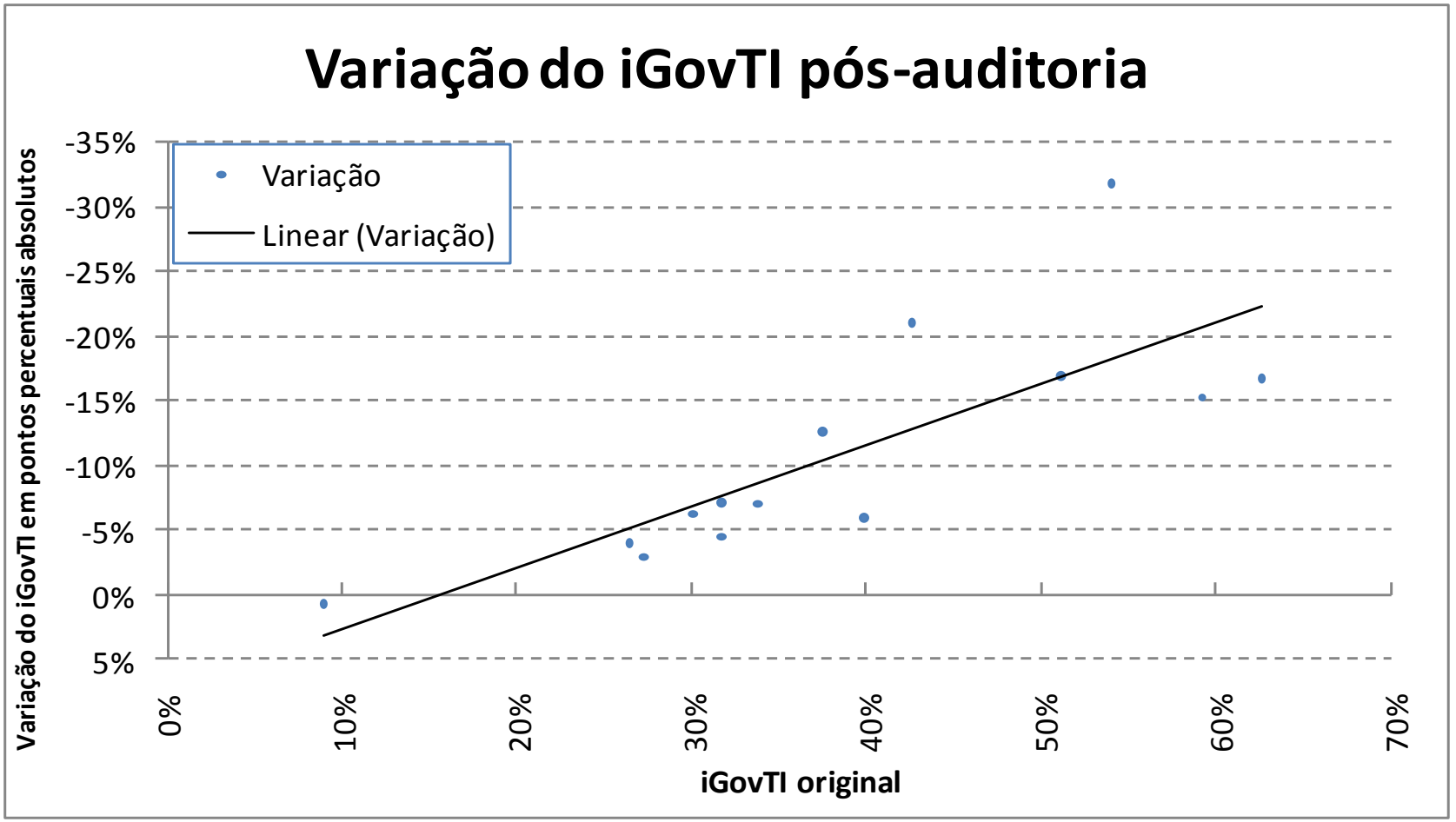
71

Considerações finais

Situação de govTI declarada não é boa ...



Situação pode ser pior do que a declarada...



Riscos poderiam ser mitigados...

- *Ausência de controles gerais de segurança da informação contribui para diversas vulnerabilidades na [Autarquia], inclusive já exploradas em sede de fraude no [Sistema], o qual gere R$ 24 bilhões em contratos ativos;*

Riscos poderiam ser mitigados...

- *A ausência de processo de software no [Ministério] contribui para que o código do sistema que suporta o [programa] não implemente as regras de negócio na forma prevista na legislação, com consequências que podem afetar inclusive a credibilidade do programa;*

Riscos poderiam ser mitigados...

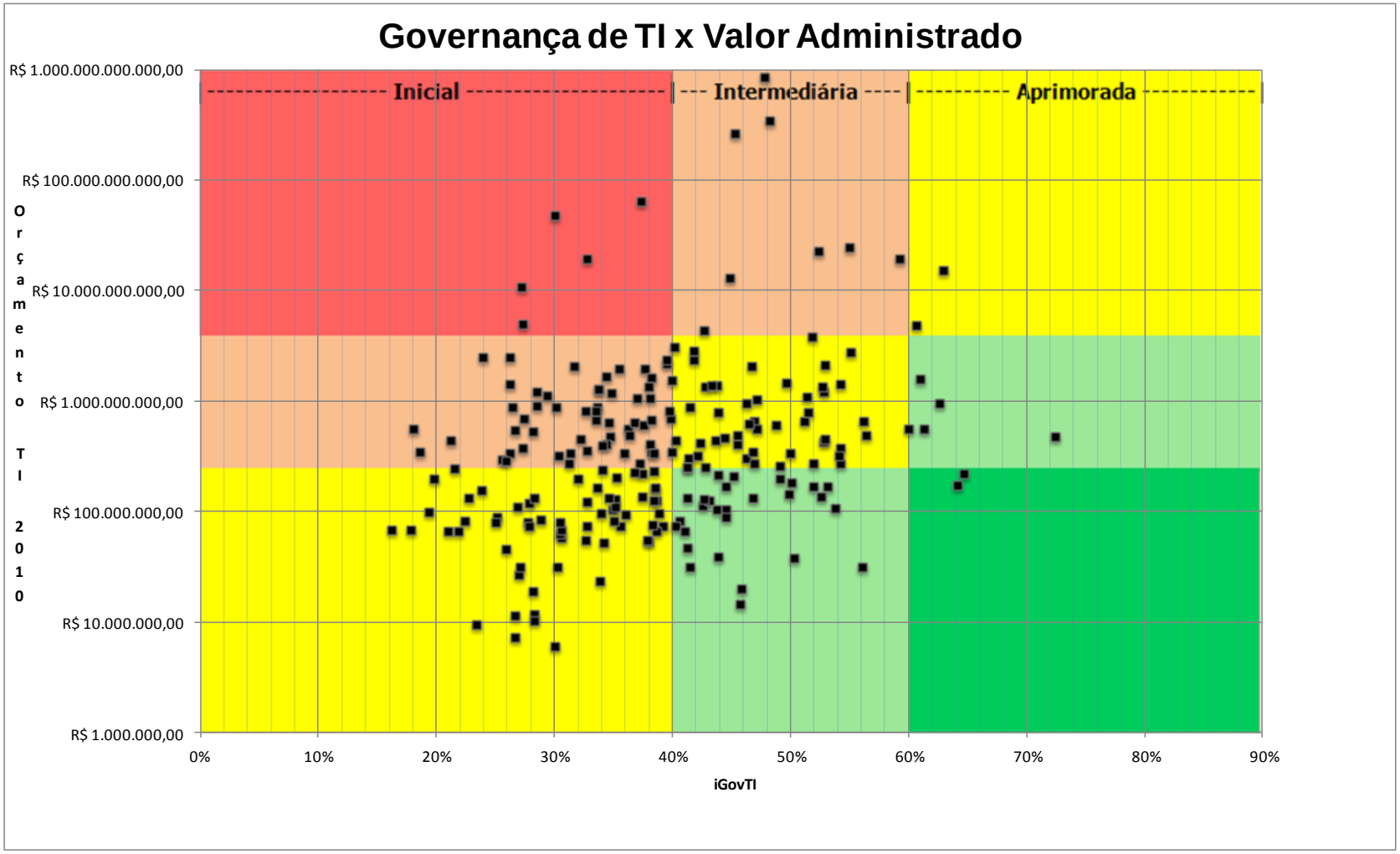
- *O não funcionamento do comitê de TI no [Ministério] impediu a avaliação de produtos de um contrato de consultoria para implantação de controles gerais de segurança da informação, acarretando, além de indícios de pagamento indevido (em apuração), ausência de benefício para o órgão devido a não implantação, até o fim da auditoria, dos controles.*

77

Atuação dos OGS

- *Identificou-se oportunidade de melhoria na atuação daqueles órgãos.*
- *Em especial, faz-se necessária maior atuação das auditorias internas, por meio da inclusão dos temas de TI nas suas matrizes de risco.*
- *...não se evidenciou melhora substantiva na situação de governança de TI nos entes da APF.*

Riscos para o negócio da APF



Acórdão 1.233/2012-TCU-Plenário

- Sefti deve promover *a divulgação, inclusive por meio de eventos, das recomendações e determinações dirigidas aos órgãos governantes superiores por meio do presente acórdão, como forma de mitigar os riscos da sua implementação;*

80

Agenda

- Por que TI é importante na APF?
- Como foi feita a avaliação?
- Resultados da avaliação
- Aspectos legais nas contratações de TI
- Governança Corporativa x Governança de TI

Trataremos das contratações dos entes públicos e do SRP na apresentação de amanhã ...

Agenda

- Por que TI é importante na APF?
- Como foi feita a avaliação?
- Resultados da avaliação
- Aspectos legais nas contratações de TI
- Governança Corporativa x Governança de TI

Também trataremos deste tema na apresentação de amanhã ...

Na íntegra:

Acórdão 1.233/2012-TCU-Plenário

Relator:

Exmº Ministro Aroldo Cedraz

Unidades do TCU participantes

- Secex-AM
- Secex-CE
- Secex-RJ
- Secex-RO
- Secex-RR
- Secex-RS
- Secex-SP
- Secex-1
- Secex-5
- Secex-6
- Secex-9
- Sefti

"A única coisa necessária para o triunfo do mal é que os homens bons não façam nada"

Edmund Burke,

estadista e filósofo britânico.

Grato pela atenção.

Renato Braga, CISA, CIA, CGAP, CCI

Missão da Sefti: *"Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública em benefício da sociedade."*

http://www.tcu.gov.br/fiscalizacaoti
sefti@tcu.gov.br