TRIBUNAL DE CONTAS DA UNIÃO

Avaliação da Segurança da Informação no âmbito da APF

Pedro Coutinho Filho
Sefti

Brasília, 17 de maio de 2013

www.tcu.gov.br/fiscalizacaoti

Agenda

- **Levantamento IGovTI**
  - **Objetivos**
  - **Principais resultados obtidos na área de Segurança da Informação**
  - **Evolução de alguns indicadores**
- **TMS Gestão e Uso e TMS ERP –**
  - **Objetivos e entidades alvo**
  - **Principais critérios utilizados na área de Segurança da Informação**
  - **Principais achados**
- **Acórdão 1233/2012 - NC GSI 5 e 8**
- **Cartilha de Boas Práticas em SI – Link e Indicação dos principais acórdãos**

Motivação dos Levantamentos GovTI

- ❑ Mapear riscos relevantes
- ❑ Identificar os melhores resultados e as boas práticas
- ❑ Dar transparência da situação de governança de TI na APF

Governança de TI

Definição

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

ABNT NBR ISO/IEC 38500

busca assegurar que o uso da TI

agregue valor ao negócio ...

... com riscos aceitáveis

Acórdão 2585/2012 – Voto e Declaração de Voto

Governança de TI

Responsabilidade

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

ABNT NBR ISO/IEC 38500, Cobit

Levantamentos de Governança de TI (iGovTI)

1º em 2007

- 255 Organizações
- 39 perguntas
  - 32 sim/não
- Evidências

2º em 2010

- 301 jurisdicionados
- 30 perguntas
  - 152 itens
- 7 dimensões do GesPública
  - Liderança
  - Estratégias e planos
  - Cidadãos
  - Sociedade
  - Informações e conhecimento
  - Pessoas
  - Processos

3º em 2012

- 338 jurisdicionados
- 36 perguntas
  - 494 itens
- Cobit 4.1
  - Governança
  - Gestão
- 7 dimensões do GesPública + Resultados

Metodologia Levantamento 2012

- 30 questões
  - Subdivididas em 152 itens;
  - Organizadas segundo 7 dimensões do Gespública (liderança; estratégias e planos; cidadãos; sociedade; informações e conhecimento; pessoas e processos);
- Instrumentos de apoio
  - Perguntas frequentes – FAQ;
  - Objetivos de cada questão;
  - Glossário.

Metodologia Levantamento 2012

- Análise das informações – definição de grupos
  - EXE-Dest (Empresas estatais)
  - EXE-Sisp (Sistema de Administração dos Recursos de Informação e Informática)
  - Judiciário
  - Legislativo
  - MPU

Feedback

Índice de Governança de TI da Instituição (iGovTI)

Nome Instituição: COMPANHIA

Tipo Instituição: Soc. econ. mista ou empresa pública **Segmento:** EXE-Dest

1.Liderança	2.Estrat. Planos	6.Pessoas	7.Processos	iGovTI	Estágio de Gov. de TI
0,29	0,29	0,25	0,29	0,28	Inicial

Acórdão 1.603/2008-TCU-Plenário

Deficiências

57% NÃO tinham carreira específica para TI

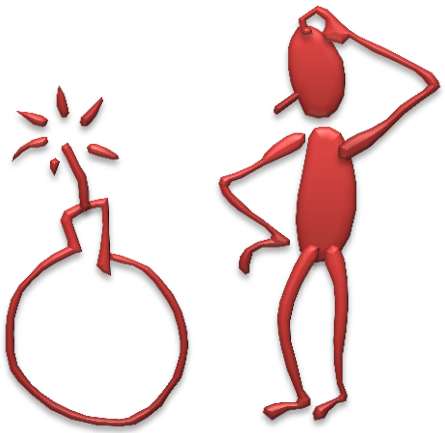
59% NÃO tinham planejamento estratégico em vigor

64% NÃO tinham política de segurança da informação

75% NÃO faziam análise de riscos de TI

80% NÃO faziam classificação da informação

88% NÃO tinham plano de continuidade de negócios



Acórdão 1.603/2008-TCU-Plenário

Orientações

9.1.3. orientem sobre a **importância do gerenciamento da segurança da informação**, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a **gestão da continuidade do negócio**, a **gestão de mudanças**, a **gestão de capacidade**, a **classificação da informação**, a **gerência de incidentes**, a **análise de riscos de TI**, a **área específica para gerenciamento da segurança da informação**, a **política de segurança da informação** e os **procedimentos de controle de acesso**.

Acórdão 1.603/2008-TCU-Plenário

Orientações

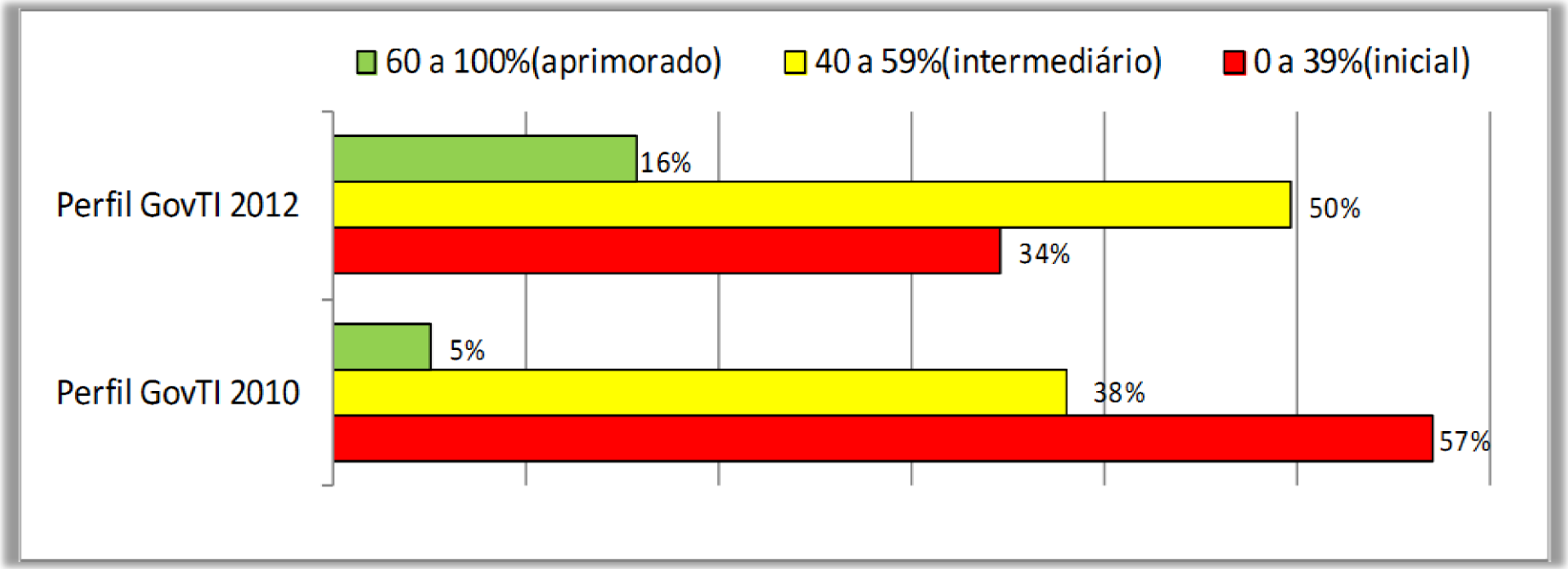
9.2. recomendar ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR que **oriente os órgãos/entidades da Administração Pública Federal** sobre a importância do **gerenciamento da segurança da informação**, promovendo, inclusive **mediante orientação normativa**, ações que visem estabelecer e/ou aperfeiçoar a gestão da **continuidade do negócio**, a gestão de **mudanças**, a gestão de **capacidade**, a **classificação da informação**, a gerência de **incidentes**, a **análise de riscos de TI**, a **área específica para gerenciamento da segurança da informação**, a **política de segurança da informação** e os **procedimentos de controle de acesso**.

TCU e a Sefti

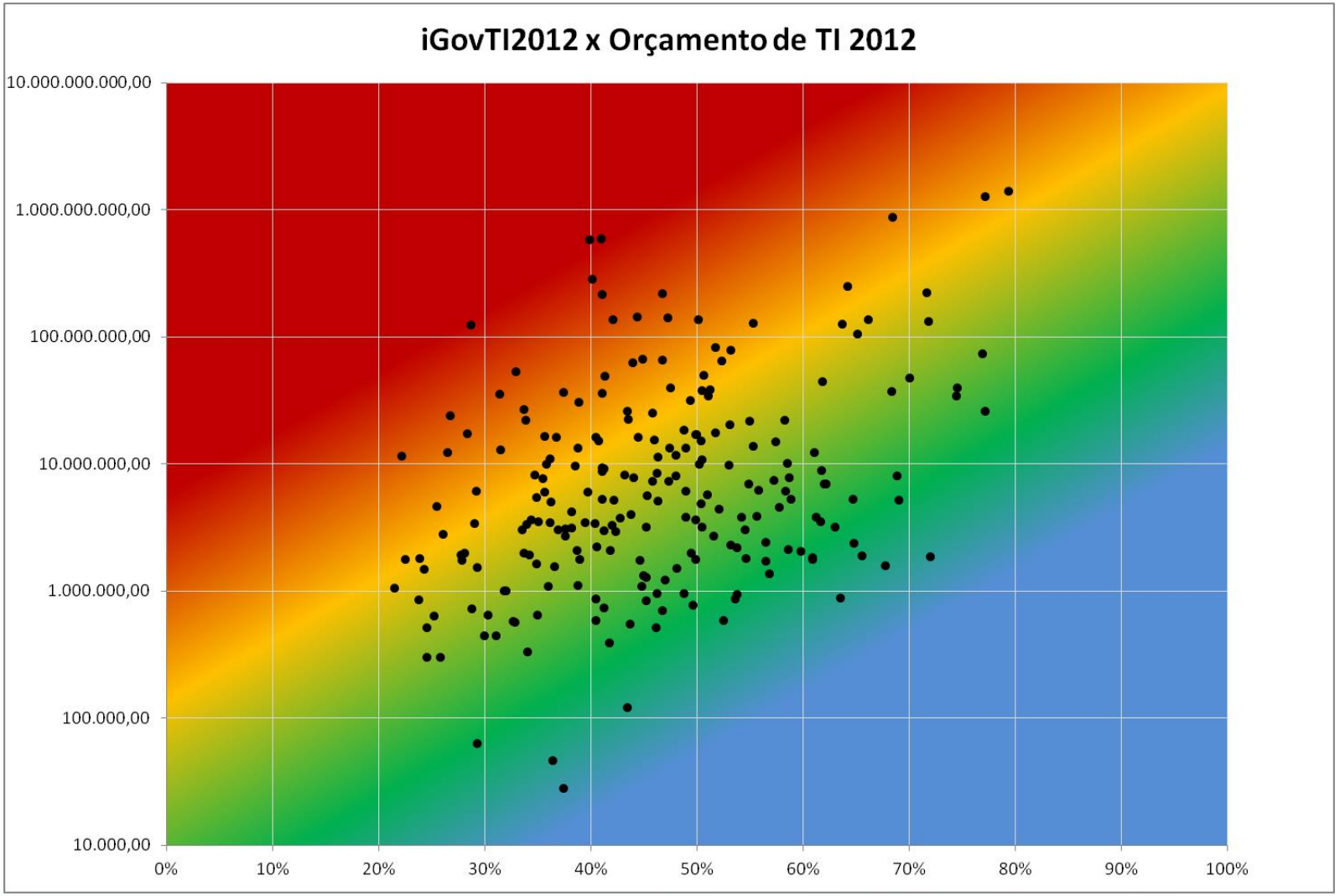
- Governança e Gestão
  - Levantamentos de Governança de TI
    - Acórdãos 1.603/2008, 2.308/2010 e 2.585/2012, todos do Plenário do TCU
  - Atuação em conjunto com os OGS
    - Acórdão 1.145/2011-TCU-Plenário, item 9.1: “ampliem a divulgação, inclusive por meio da realização de eventos, das **orientações e normas elaboradas para aprimoramento da governança de TI**, de modo a tentar obter, com maior celeridade, os resultados desejados com aquelas medidas”

iGovTI2012

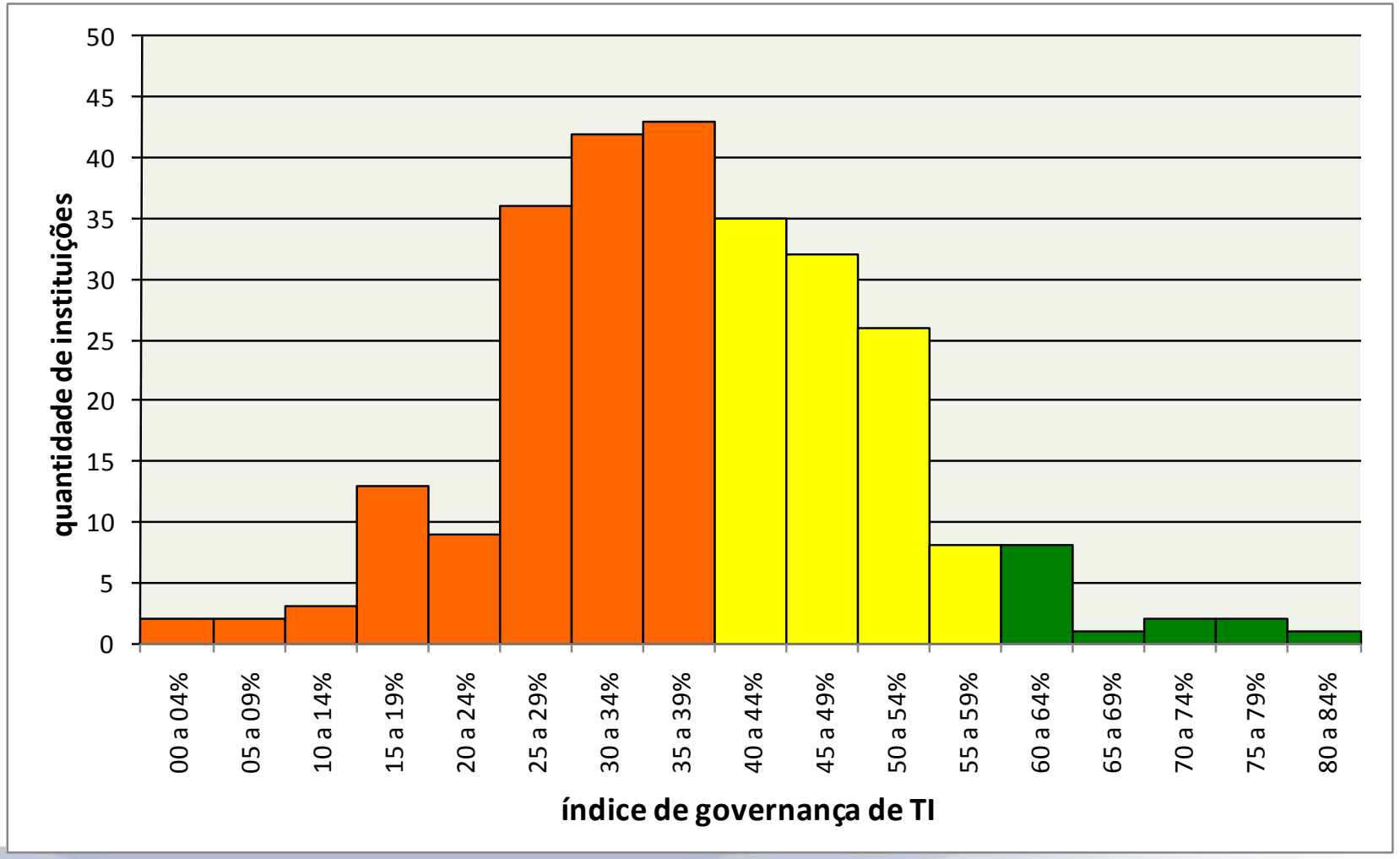
Distribuição das Instituições por estágio do iGovTI



Levantamento de Governança de TI 2012: Mapeamento de Riscos



Levantamento de Governança de TI 2012: Distribuição



Acórdão 2.585/2012-TCU-Plenário: Aspectos que demandam atenção

Liderança da Alta Administração

63% NÃO estabeleceram indicadores de desempenho de TI

Segurança da Informação

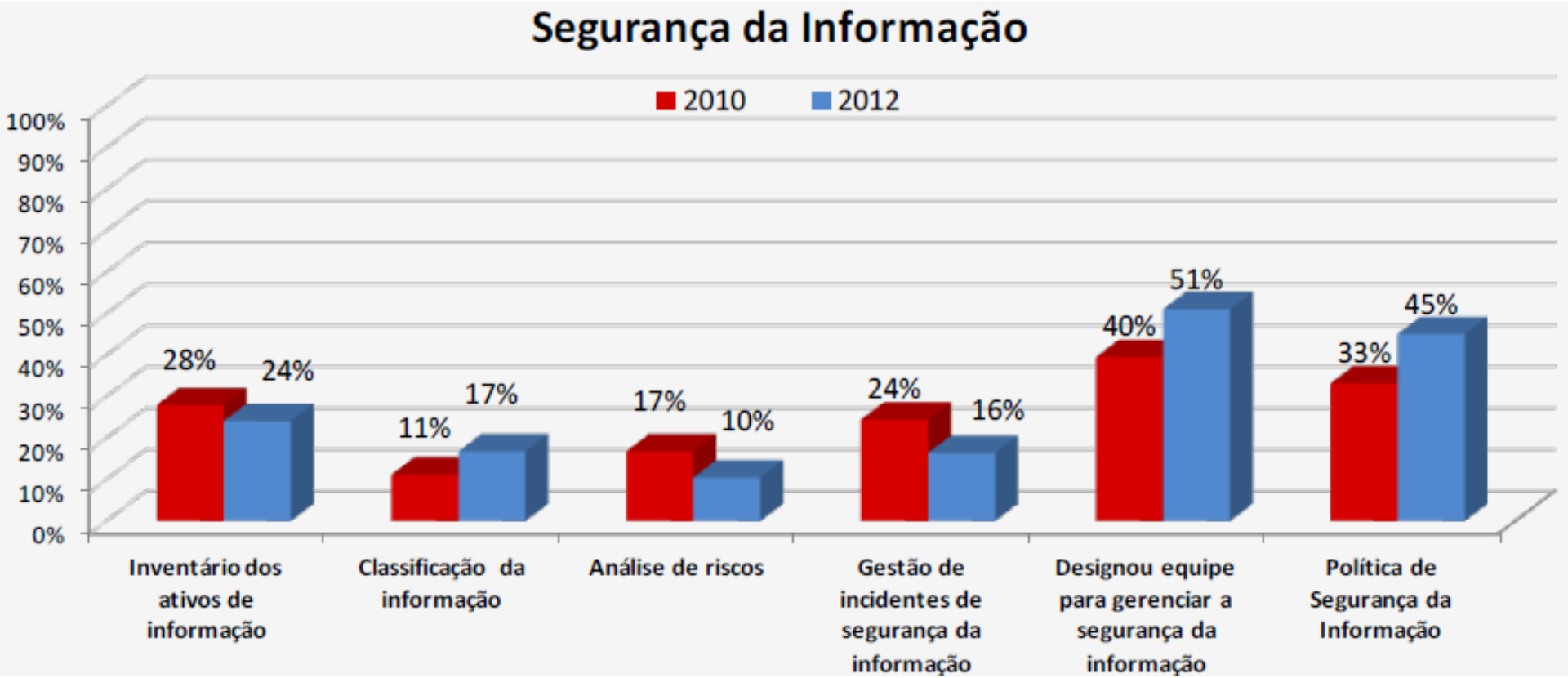
55% NÃO possuem política corporativa de segurança da informação

83% NÃO classificam a informação para o negócio

84% NÃO gerenciam os incidentes de segurança da informação

90% NÃO analisam os riscos aos quais a informação está submetida

Acórdão 2.585/2012-TCU-Plenário: Baixos sinais de evolução em SI



Acórdão 2.585/2012-TCU-Plenário: Recomendações

- Ausência de PSI
  - Procedimentos não padronizados de SI;
  - Deficiências nos controles de segurança;
  - Dificuldade de responsabilização em incidentes de segurança;
  - Risco de acesso não autorizado e vazamento de informações;
- Classificação de Informações
  - Lei 12.527/2011;
- Níveis baixos em análise riscos, inventário de ativos de informação e gestão de incidentes.

Acórdão 2.585/2012-TCU-Plenário: Recomendações

- definam e formalizem metas de governança, como parte do plano diretor de tecnologia da informação da instituição, baseadas em parâmetros de governança, necessidades de negócio e riscos relevantes, atentando para as metas legais de cumprimento obrigatório e as orientações da ABNT NBR ISO/IEC 31000
- à SOF/MP que desenvolva estudos para colocar em prática critérios de alocação de recursos públicos para TI segundo a real capacidade das instituições de converter tais recursos nos benefícios pretendidos, mensurada com base em métricas de risco, levando em consideração os planos de melhoria de governança de TI elaborados pelas instituições que apresentam maiores riscos

Acórdão 2.585/2012
Declaração de Voto

Enfim, vejo que a situação é desafiadora, e não tenho a ilusão de que seja fácil construir a cultura da governança de TI, mas há uma direção a seguir, e os alicerces estão sendo construídos. Por isso, pelo TCU, prosseguiremos nesse esforço, incrementando auditorias, promovendo ações e eventos de divulgação, induzindo a gestão de riscos e controles e incentivando o aperfeiçoamento da governança de TI.

Min. Augusto Nardes – Presidente do TCU

Temas de Maior Significância

Auditorias

- TMS Gestão e Uso – Foco da auditoria em SI
  - Equipe de tratamento e resposta a incidentes em redes computacionais ;
  - Política de Segurança da Informação e Comunicações;
  - Comitê de Segurança da Informação e Comunicações;
  - Inventário dos ativos de informação;
  - Processo de gestão de riscos de segurança da informação;
  - Classificação da informação.

Temas de Maior Significância

Auditorias

- TMS Gestão e Uso – Resultados em SI
  - Informação da APF, apesar da atuação do GSI/PR e CNJ continua exposta a riscos de segurança em larga medida;
  - Trabalhos de campo demonstraram:
    - possibilidade de acesso/alteração indevidamente;
    - ausência de segregação de funções em sistemas;
    - compartilhamento de senhas;
    - contratação de "pacotes" de políticas e SI;
    - execução de despesas sem o aperfeiçoamento de SI;

Temas de Maior Significância

Auditorias

- TMS Gestão e Uso (Ac. 1233/2012-Plenário)
  - Recomendação ao GSI/PR
    - 9.8.1. em atenção à Lei 10.168/2003, art. 6º, IV, articule-se com as escolas de governo, notadamente à Enap, a fim de **ampliar a oferta de ações de capacitação em segurança da informação** para os entes sob sua jurisdição (subitem II.8);
    - 9.8.2. em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição 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 (subitem II.8).

Temas de Maior Significância

Auditorias

- TMS ERP– Foco da auditoria em SI
  - Política de Segurança da Informação e Comunicações;
  - Processo de gestão de riscos;
  - Continuidade de negócios;
  - Procedimentos formais para backup e recuperação de dados, aplicativos e documentação;
  - Controles físicos ao ambiente de produção do ERP;
  - Política de controle de acesso (rastreabilidade, revisão periódica de usuários);
  - Controle de atividades conflitantes.

Temas de Maior Significância

Auditorias

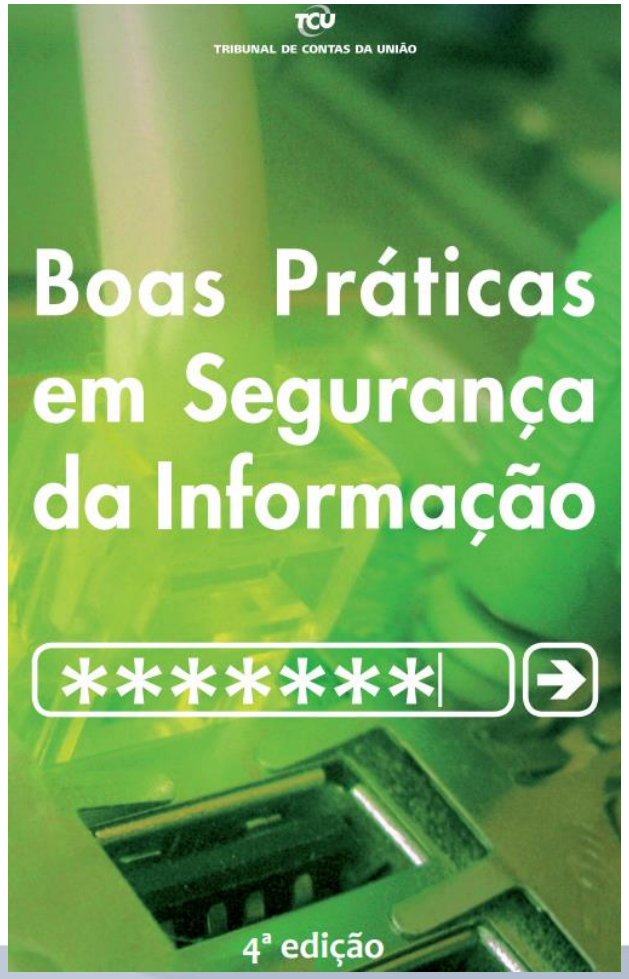
- TMS ERP – Resultados em SI
  - Inexistência de plano de continuidade;
  - Ausência de formalização de PSI ou inexistência de PSI;
  - Política de controle de acesso em desconformidade com as boas práticas;
  - Permissão dadas sem revogação posterior;
  - Ausência de mapeamento de atividades conflitantes;
  - Falhas nos controles físicos.

Temas de Maior Significância

Auditorias

- TMS ERP (Ac. 2523/2012-Plenário)
  - Determinação ao Dest, para que exija dos órgãos e entidades sob sua jurisdição, para ERP já implantados ou com implantação planejada
    - 9.1.1**. política de segurança da informação** formalmente aprovada, em obediência à IN 1/2008, art 5º, inciso VII, do GSI/PR, observando as diretrizes da NC 3/IN01/DSIC/GSIPR, as práticas dos itens 5.1.1 e 5.1.2 da NBR ISO/IEC 27002:2005, e à semelhança das orientações do objetivo de controle DS5.2 do Cobit 4.1;
    - 9.1.2. **política de controle de acesso** formalmente aprovada, em obediência à NC 7, item 2.6, do Gabinete de Segurança Institucional da Presidência da República, observando as diretrizes e recomendações dessa norma e do item 11.1.1 da NBR ISO/IEC 27002:2005;

Boas práticas em Segurança da Informação



- Portal TCU > Comunidades > Fiscalização de tecnologia da informação > Documentos e trabalhos
- http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF
- Política de Segurança da Informação; Controles de acesso lógico; Plano de continuidade de negócios; e TCU e a NBR ISO/IEC 27002:2005

TRIBUNAL DE CONTAS DA UNIÃO

Obrigado!

Pedro Coutinho Filho
Sefti
www.tcu.gov.br/fiscalizacaoti
Brasília, 17 de maio de 2013