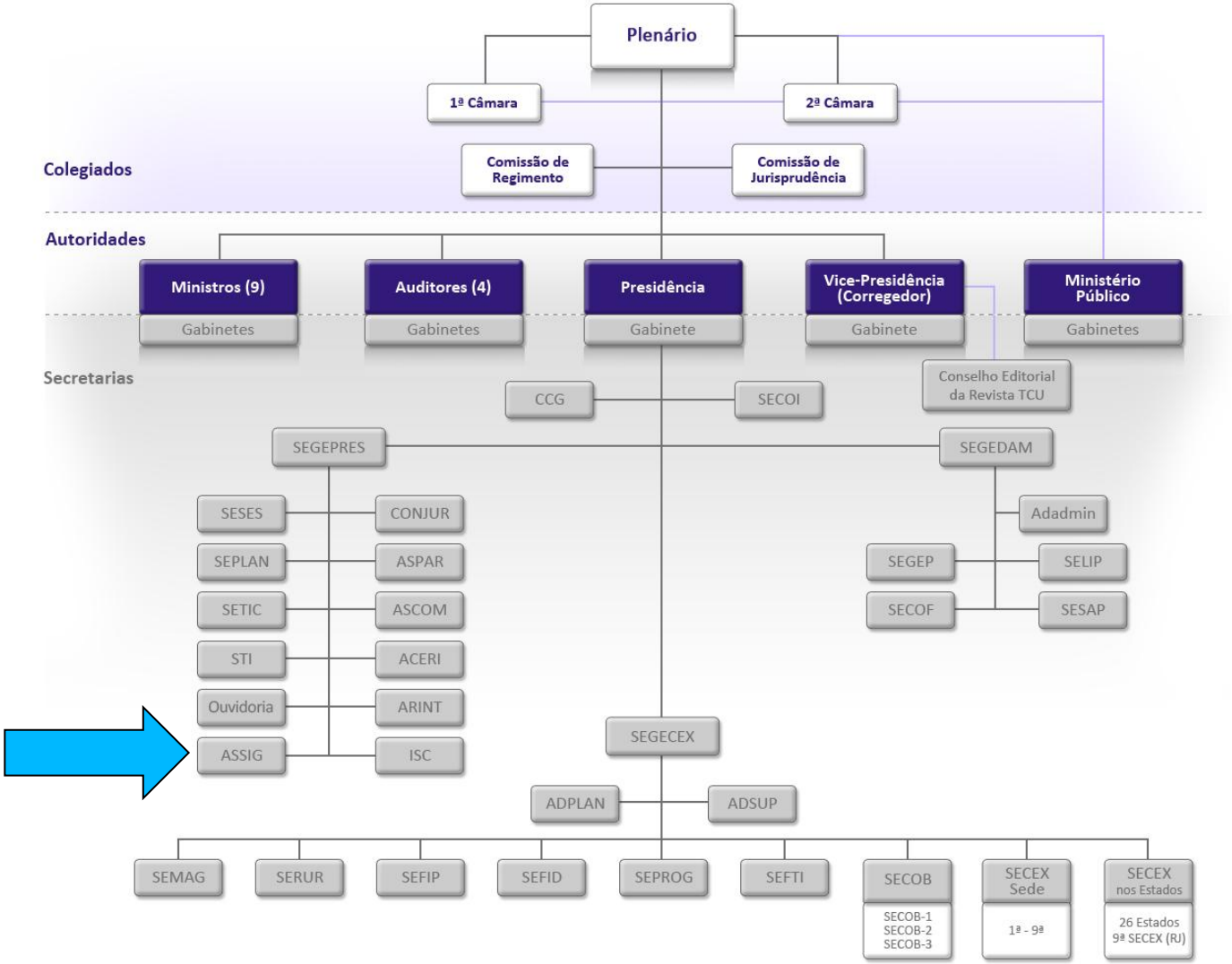
TRIBUNAL DE CONTAS DA UNIÃO

Como o TCU vem implantando a governança de TI

Assessoria de Segurança da Informação e Governança de TI
- Assig -

Marisa Alho
Chefe de Assessoria

Assessoria de Segurança da Informação e Governança de TI

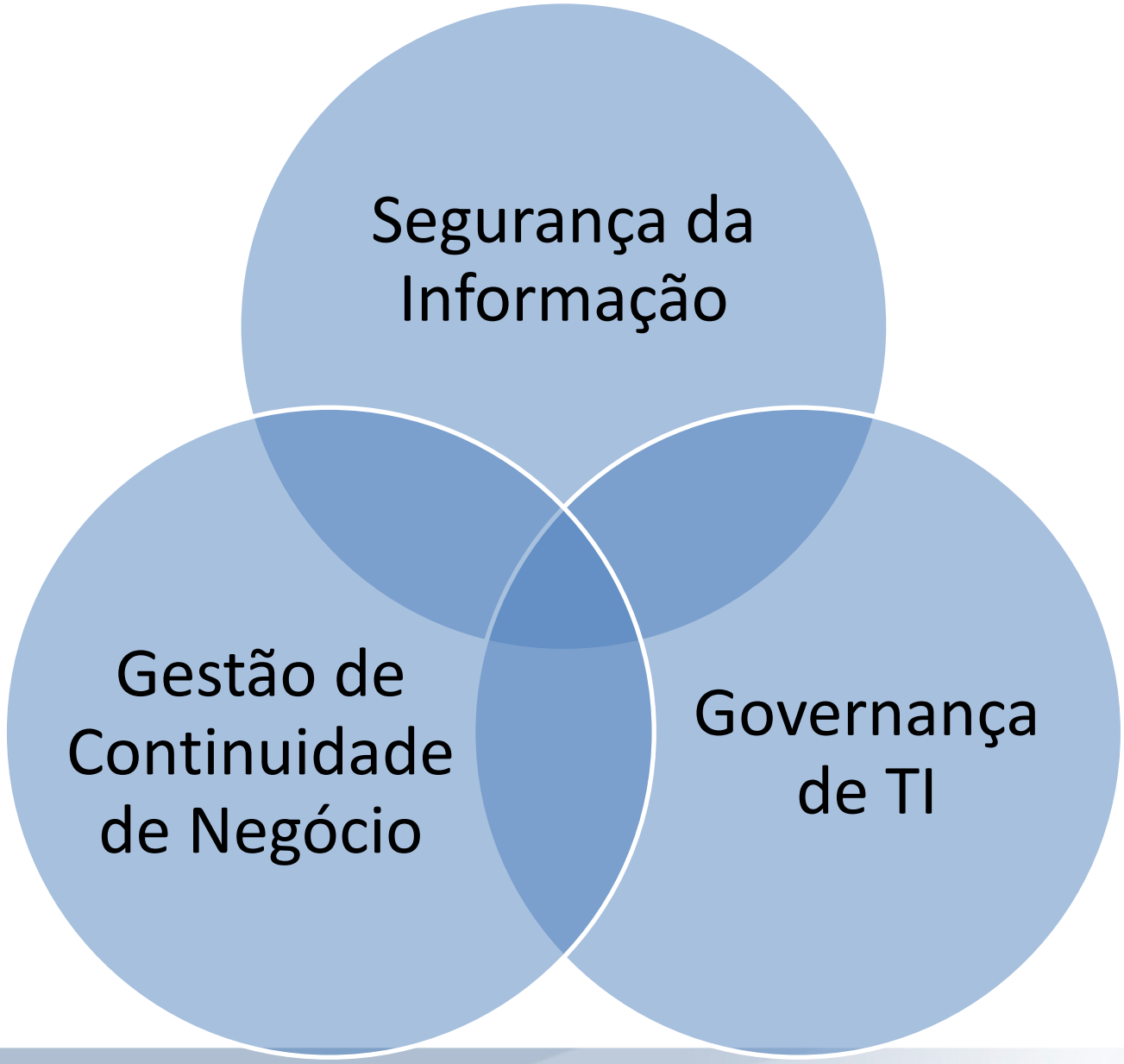


Missão da Assig:

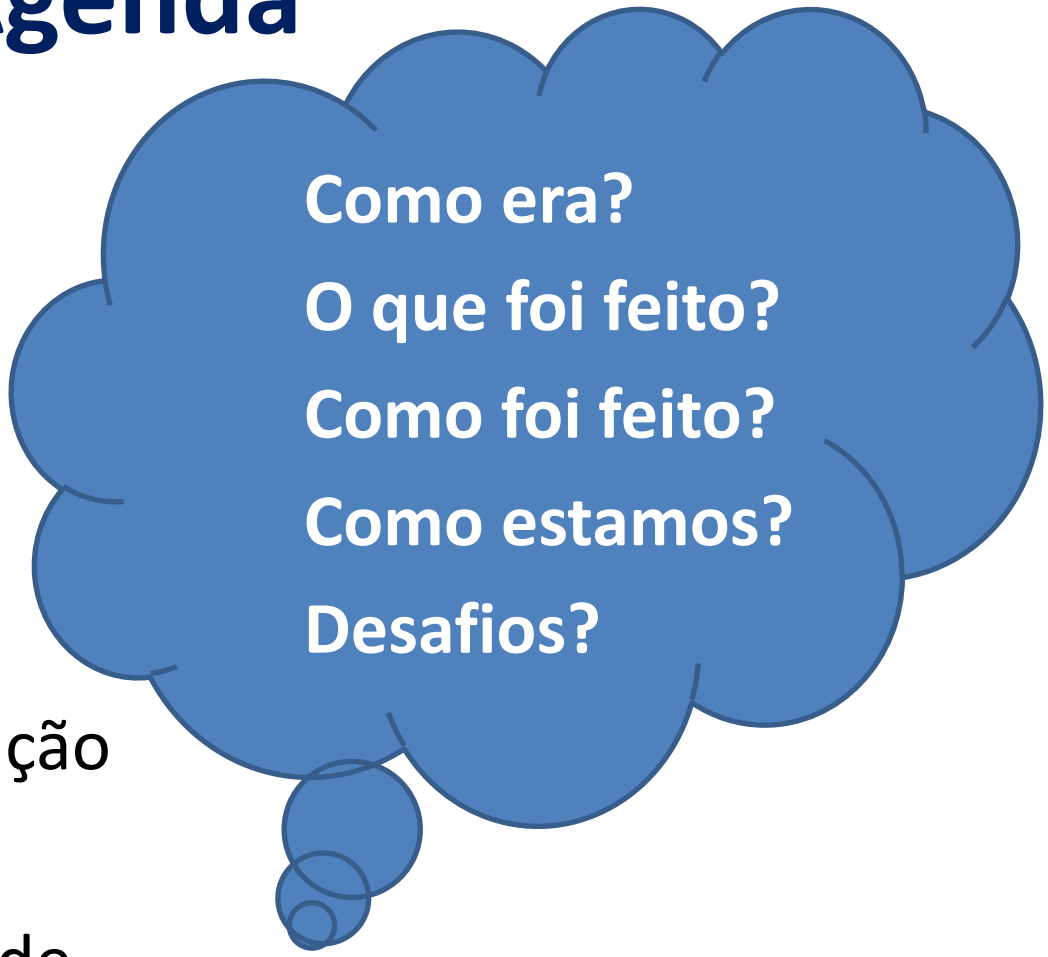
"Promover a segurança da informação, a governança de TI e a continuidade dos processos críticos, para viabilizar o uso adequado da informação e aperfeiçoar a governança institucional."

Missão do TCU:

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

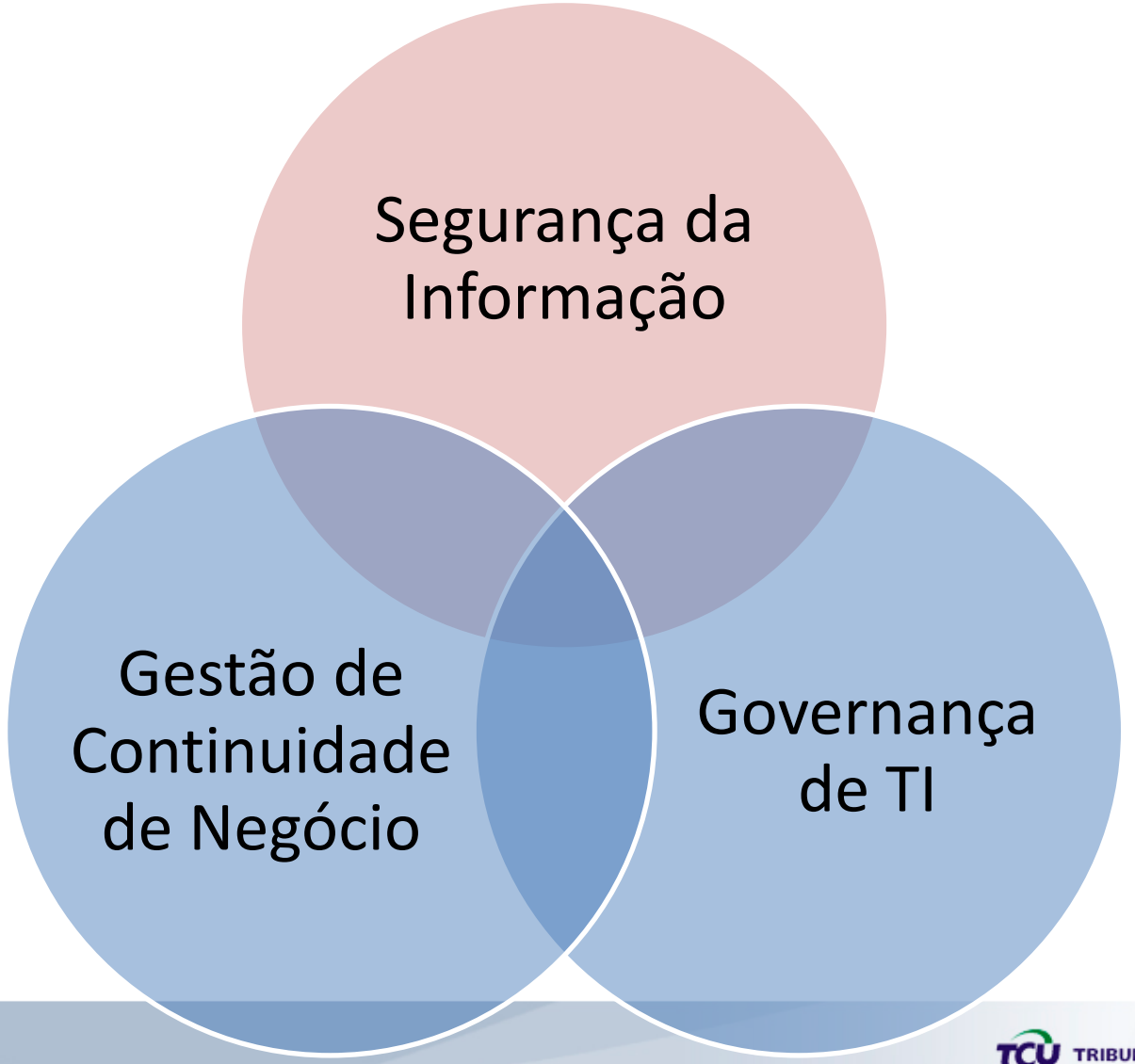

Segurança da Informação
Gestão de Continuidade de Negócio
Governança de TI

Agenda



- Segurança da Informação
- Governança de TI
- Gestão de Continuidade de Negócio

TCU e a Segurança da Informação



Por que Segurança da Informação no TCU?

Prestações de contas

Solicitações CN

Denúncias

Documentos gerais

Recursos

Bases de dados

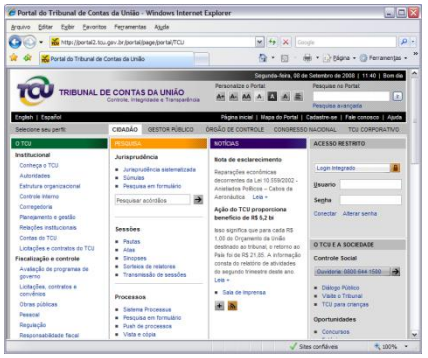
Pareceres e relatórios

Tramitações

Sistemas de informação

Papéis de trabalho

Bases de dados



Acórdãos

Vistas

Publicações TCU

Informações para o CN

Segurança da Informação

Como era em 2008?

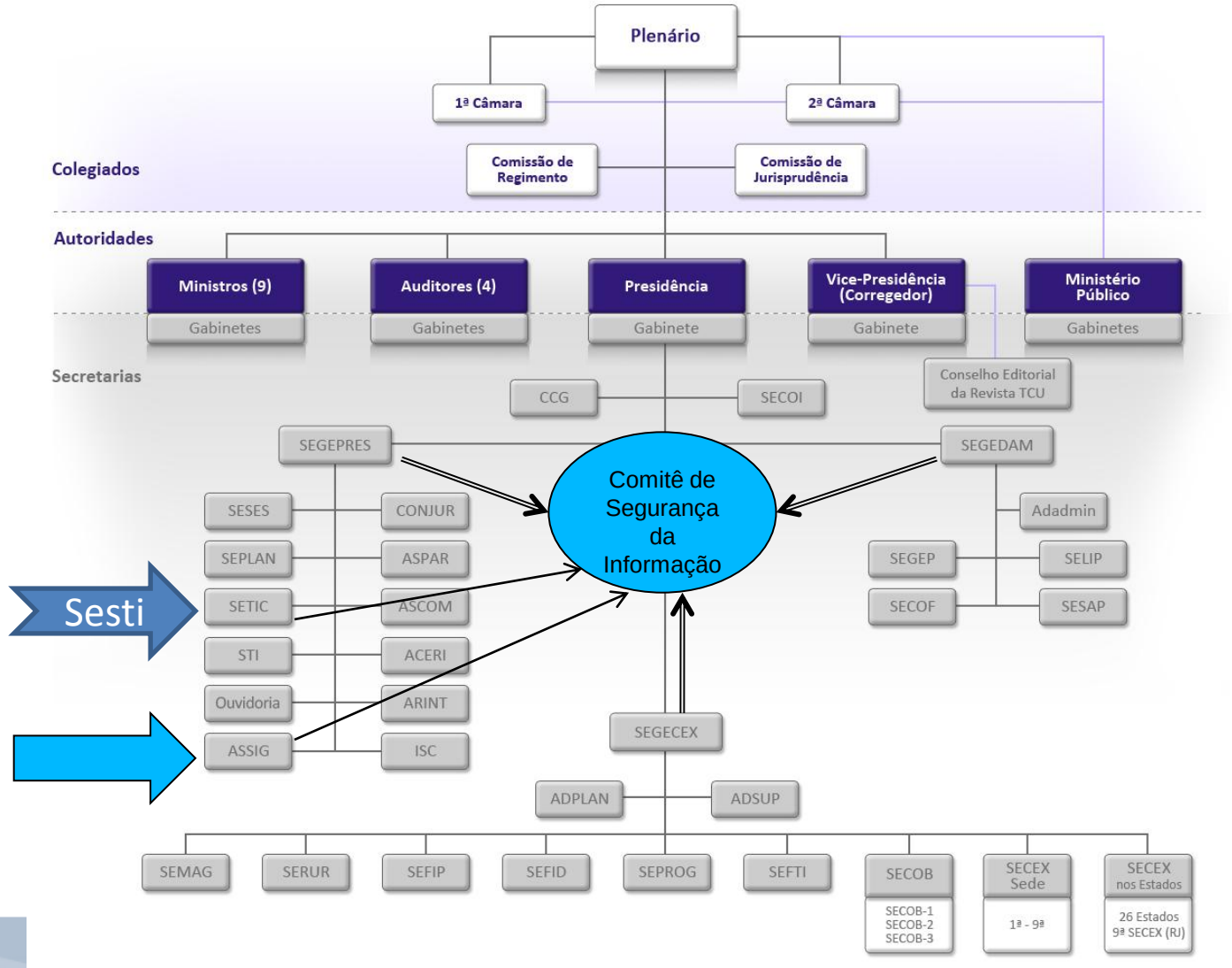
- Política de Segurança da Informação
  - 1999
  - Foco excessivo em aspectos tecnológicos
- Organização da Segurança da Informação
  - Inexistente
- Demais processos ISO 27000
  - Inexistentes

Segurança da Informação

O que foi feito?

- Organização da Segurança da Informação
  - Criação da Assessoria de Segurança da Informação e Governança de TI – Assig (2008)
  - Criação do Comitê de Segurança da Informação (2008)
  - Criação do Serviço de Segurança da Informação em TI (2009)

Organização da Segurança da Informação



Segurança da Informação

O que foi feito?

- Política de Segurança da Informação
  - Revisada e reeditada (2008)
  - Foco em princípios e diretrizes
  - Abordagem holística (processos, pessoas e tecnologia)
  - Atribui responsabilidades
  - Aspectos tecnológicos em normativos adicionais

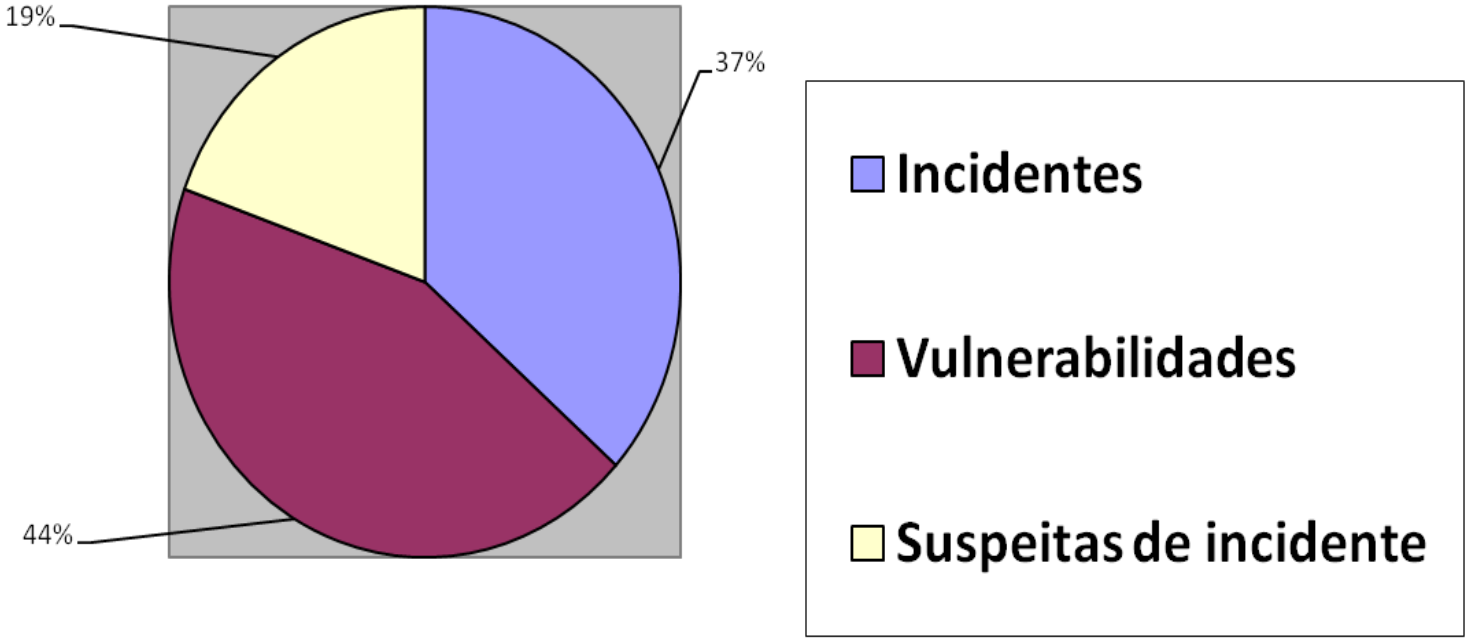
Segurança da Informação

O que foi feito?

- Demais processos ISO 27000
  - Classificação da Informação (2009)
  - Gestão de Incidentes de Segurança da Informação (2010)
  - Gestão de Riscos em Segurança da Informação (2011)
- Conscientização
  - Processo contínuo (desde 2008)

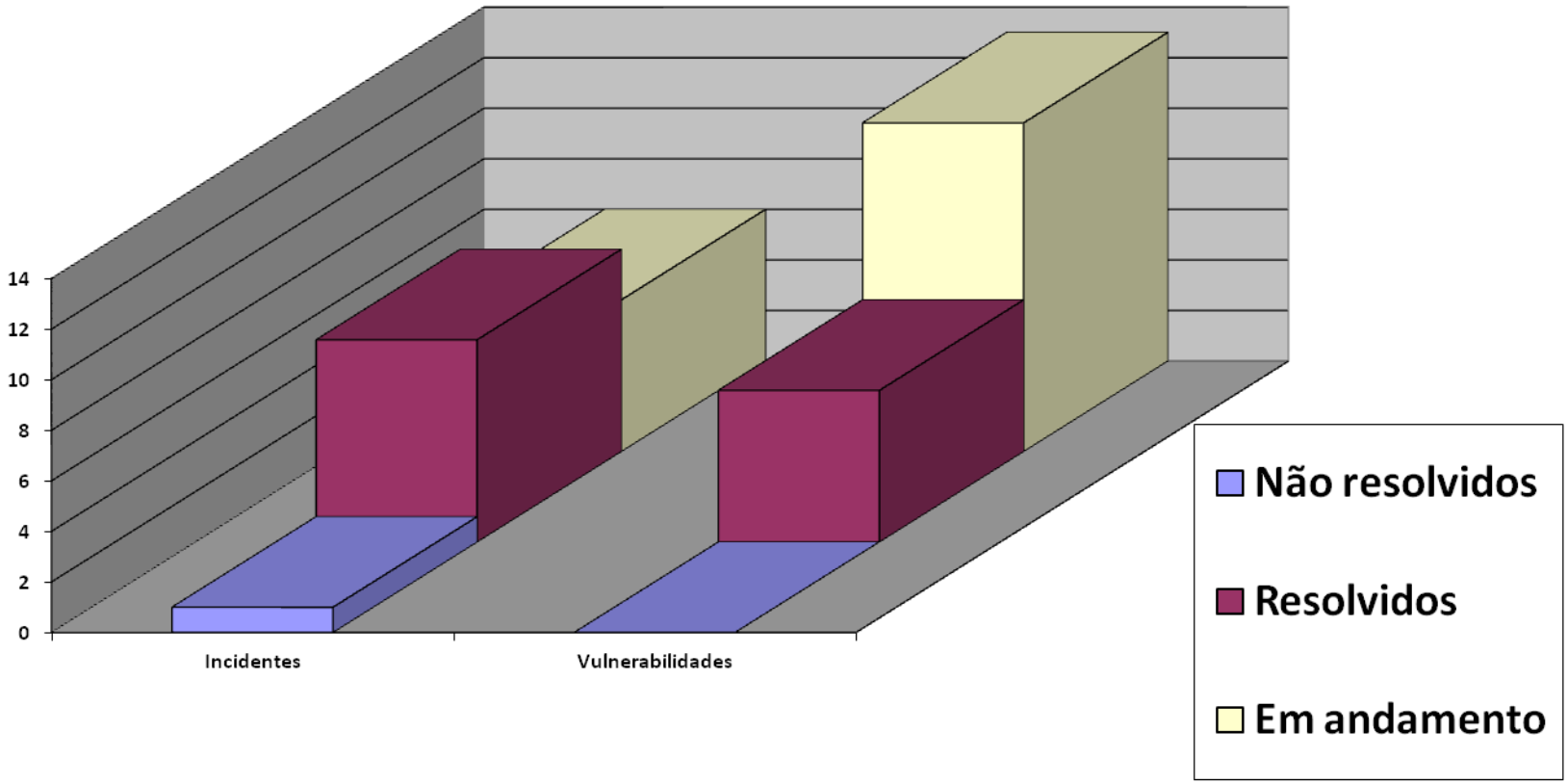
Gestão de Incidentes de Segurança da Informação

Dados de 2011:



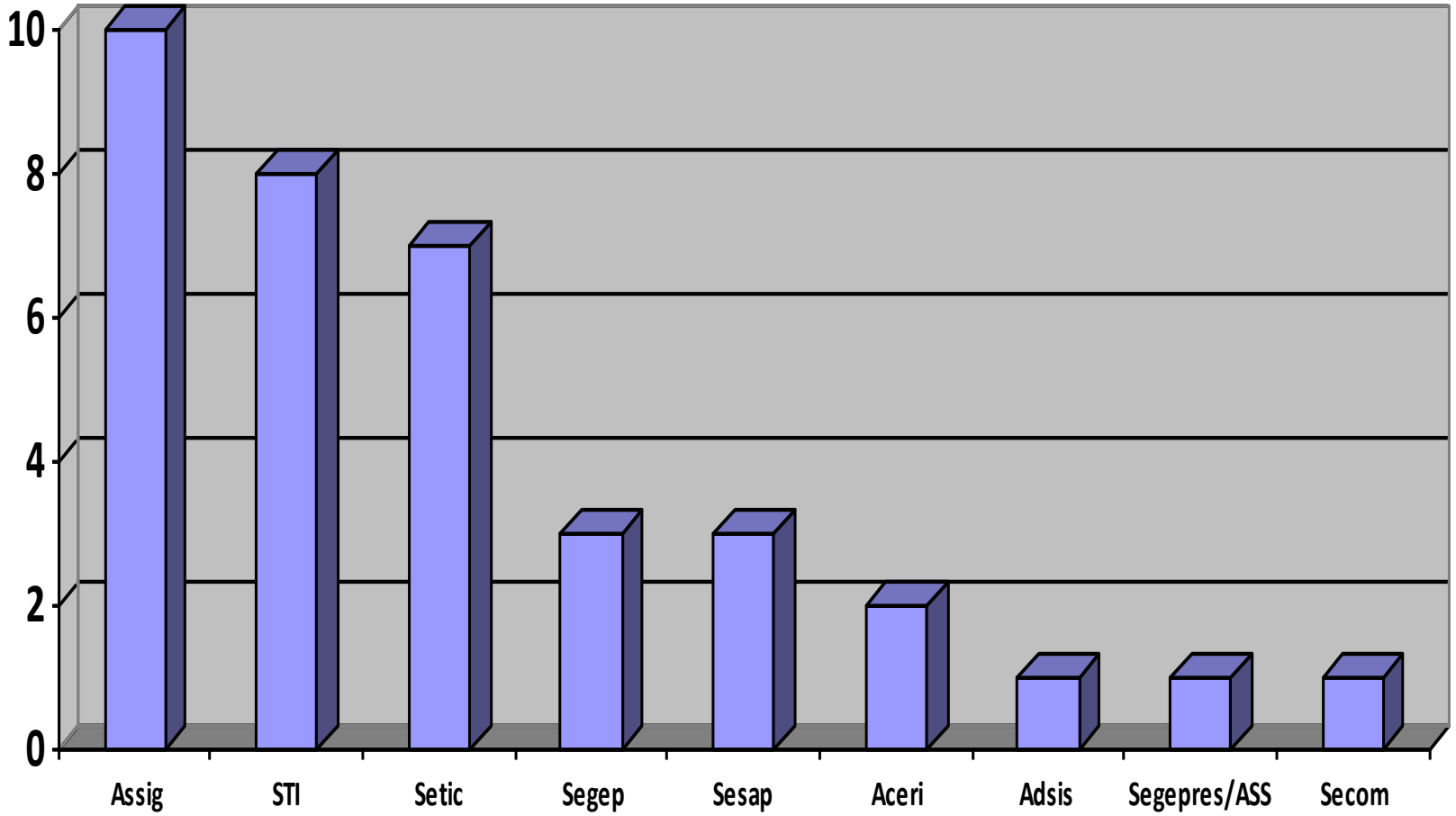
Gestão de incidentes em dez/2011: ocorrências reportadas por tipo

Gestão de Incidentes de Segurança da Informação



Gestão de incidentes em dez/2011: estado das ocorrências

Gestão de Incidentes de Segurança da Informação



Gestão de incidentes em 2011: unidades envolvidas na resolução

Gestão de Riscos de Segurança da Informação

- 2011
  - Início do processo (ISO 27005)
  - 1 edição
- 2012
  - Revisão do método
    - Método simplificado, baseado no FRAAP
  - 2 edições
- 2013
  - Demandas por mais duas edições

Conscientização em Segurança da Informação

- Participação em treinamentos institucionais
- Dicas semanais no jornal interno (União)
- Coluna “Aprendendo com a Notícia”
- Dia da Segurança da Informação
- Quiz em Segurança da Informação
- Cartilha “Boas Práticas de Segurança da Informação em Auditorias”
- Portal TCU – comunidade de SI

Conscientização em Segurança da Informação

Evento	Participantes
Auditores (curso)	502
Coordenadores de auditoria (curso)	148
Supervisores de auditoria (curso)	75
Inteligência no Controle (curso)	90
Dia da Segurança da Informação 2011	305
Dia da Segurança da Informação 2012	138
Gestores de Soluções de TI (mini-curso)	41
TOTAL	**1299**

Dados acumulados de jan/2011 a out/2012

Conscientização em Segurança da Informação

Ações de conscientização	Quantidade
Cartilhas publicadas e distribuídas no TCU	3
Apresentações realizadas	65
Visitas recebidas de outros órgãos	11
Dicas no União	70
Coluna “Aprendendo com a Notícia”	19

Dados acumulados de jan/2011 a out/2012

ASSIG - Toda terça-feira, uma dica de segurança para você.

E-mail pessoal e e-mail corporativo

Embora algumas vezes não seja fácil separar nossas vidas pessoal e profissional, é fundamental que tenhamos uma caixa de e-mail corporativa separada de caixas de e-mail pessoais.

A Portaria-TCU nº 169, de 2006, permite o acesso a caixa de e-mail pessoal via web (webmail) pela rede do TCU, desde que o uso não prejudique o desempenho e a segurança da rede de computadores do TCU, nem a produtividade pessoal.

Portanto, sua caixa de e-mail corporativa deve ser usada para assuntos de interesse profissional. No entanto, utilize sempre um e-mail pessoal, por exemplo, para cadastro em sites de compras coletivas, lojas online e listas de distribuição de propagandas.

Em caso de Dúvidas ou sugestões entre em contato com a ASSIG.

Conheça mais nossa página.

União • Ano XXVI • nº 121 • Terça-feira, 12/7/2011

ASSIG

Aprendendo com a Notícia

Folha de S. Paulo

"Usuários se enfurecem com Sony após invasão à rede do *PlayStation*"

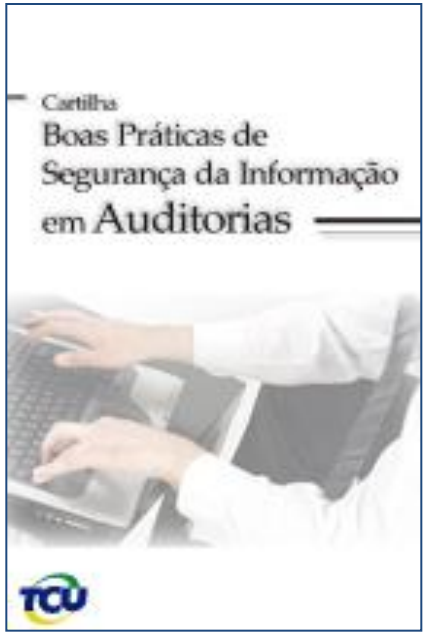
No decorrer da última semana, noticiou-se no jornal Folha de S. Paulo e em diversos veículos da imprensa nacional e internacional a ocorrência de invasão à rede de jogos *PlayStation Network*, pertencente à empresa de produtos eletrônicos Sony. A invasão ocorreu entre os dias 17 e 19 de abril, levando à indisponibilidade da aludida rede e ao acesso, por pessoa não autorizada, de informações pessoais de mais de 77 milhões de usuários, incluindo números de cartões de crédito e de senhas de acesso. Após o fato, contratou-se "empresa de segurança reconhecida" para investigar a violação dos dados.

A ocorrência de falhas como essa foge ao controle dos usuários, mas cuidados relacionados à segurança da informação podem minimizar bastante o risco de incidentes e os prejuízos deles advindos. No exemplo em questão, usuários que tinham *login* e/ou senha de acesso exatamente iguais em outros sites podem ter tido suas informações utilizadas por um terceiro mal intencionado, potencializando os prejuízos à pessoa ou a outras organizações. Da mesma forma, os dados de cartão de crédito armazenados automaticamente no site para que não fosse necessária sua digitação em eventuais compras futuras podem ter sido acessados por pessoa não autorizada, gerando prejuízos financeiros para o titular das informações.

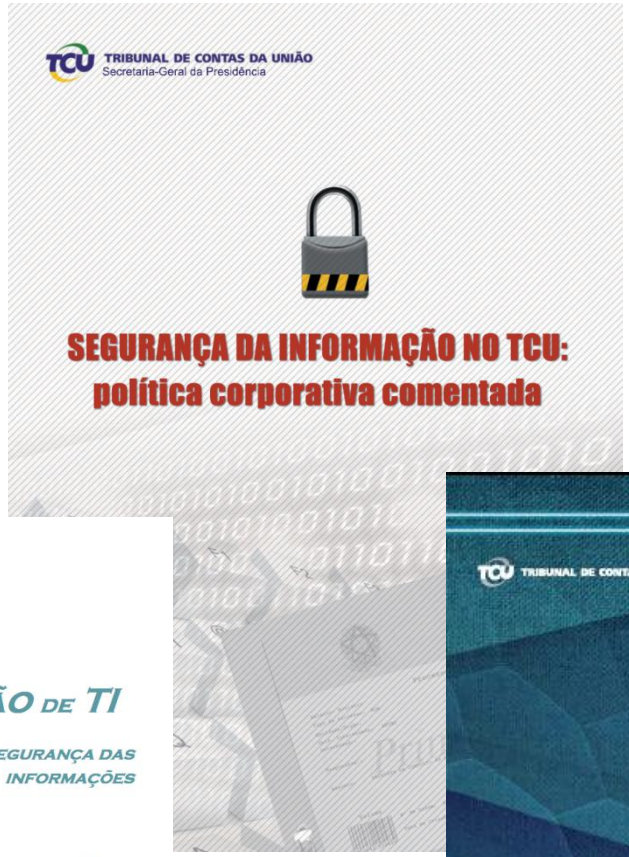
Assim, uma boa prática em segurança da informação é evitar o reaproveitamento de *login e/ou* senha em ambientes com necessidades de segurança diversas (ex: dados de autenticação idênticos para um *webmail* e para o Portal TCU). Adicionalmente, evitar o armazenamento automático de informações sensíveis (como dados de cartões de crédito em sites ou senhas em navegadores), apesar do trabalho adicional de digitação em acessos futuros, minimiza o risco de uso indevido dessas informações.

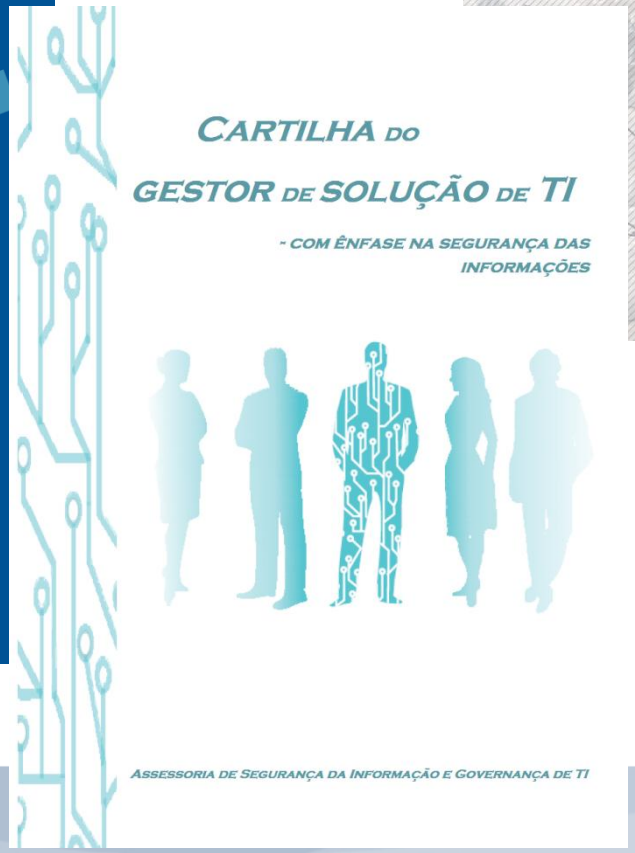
Conheça as boas práticas em segurança da informação no TCU: clique aqui.

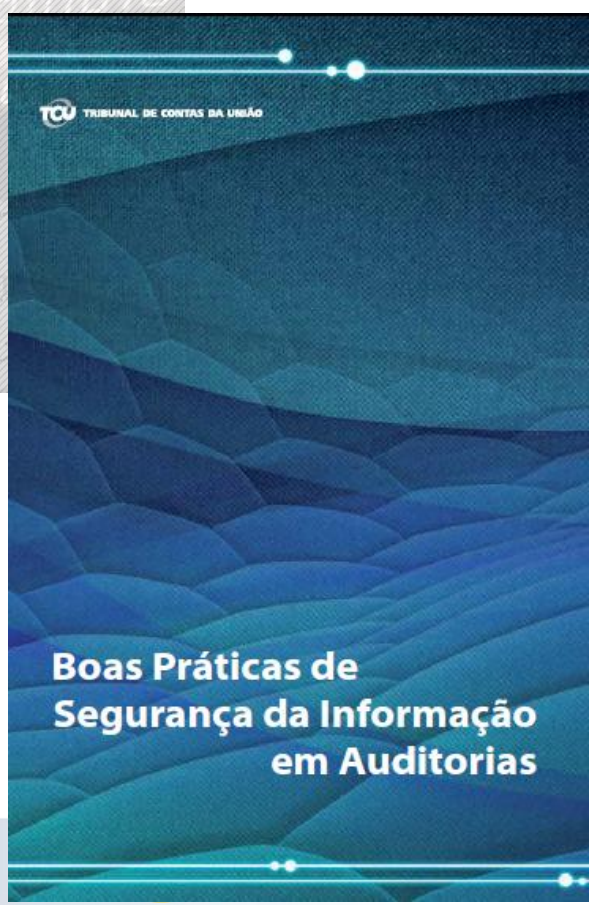
Conscientização em Segurança da Informação



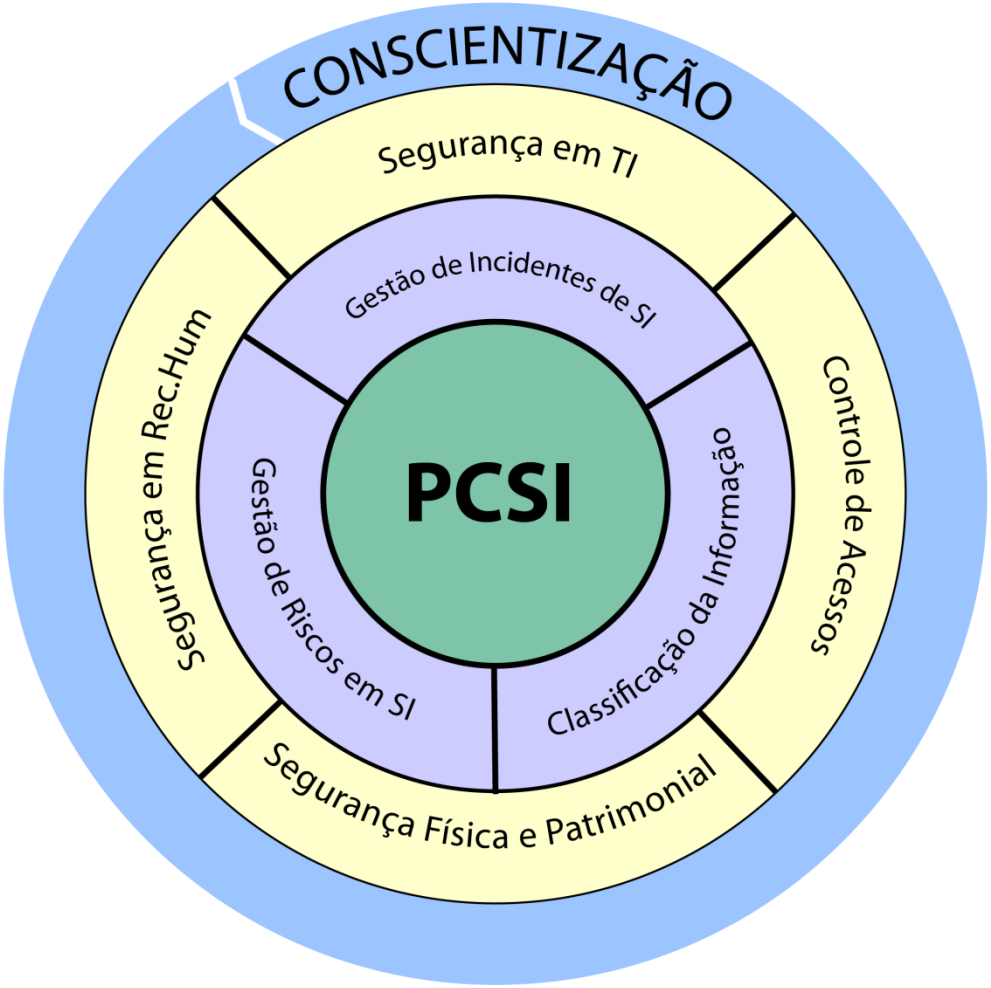

SAIBA MAIS SOBRE A SUA FRAG MENTA DORA
TCU


TRIBUNAL DE CONTAS DA UNIÃO
Secretaria-Geral da Presidência
SEGURANÇA DA INFORMAÇÃO NO TCU:
política corporativa comentada


CARTILHA DO
GESTOR DE SOLUÇÃO DE TI
- COM ÊNFASE NA SEGURANÇA DAS INFORMAÇÕES
ASSESSORIA DE SEGURANÇA DA INFORMAÇÃO E GOVERNANÇA DE TI


TRIBUNAL DE CONTAS DA UNIÃO
Boas Práticas de
Segurança da Informação
em Auditorias

Segurança da Informação – Como estamos?



SGSI/TCU – Sistema de Gestão da Segurança da Informação do TCU

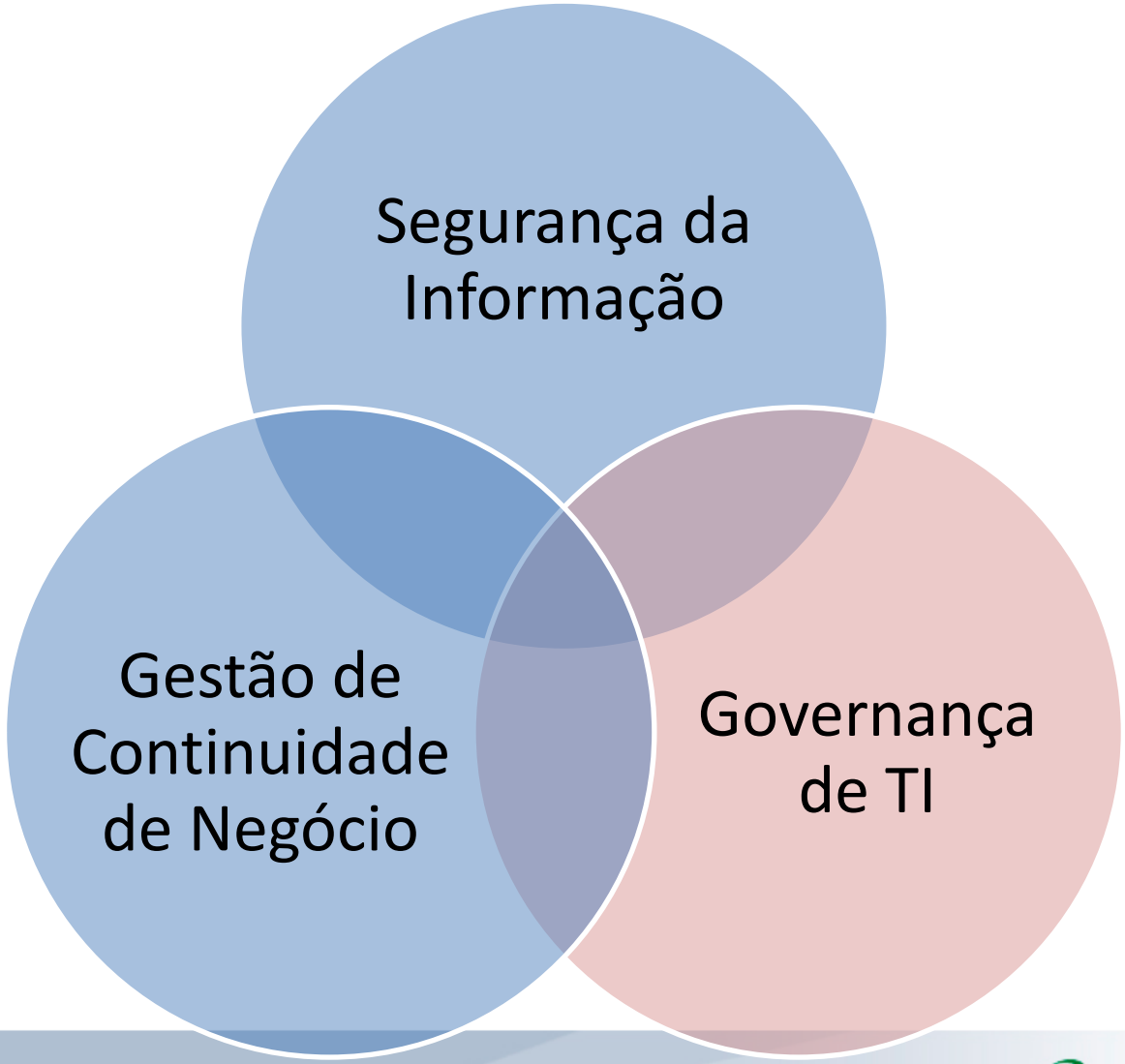
Segurança da Informação – Desafios

- Política Corporativa de Segurança da Informação
  - Revisar: 4 anos da última edição
  - Como abordar:
    - Dispositivos móveis
    - Dispositivos pessoais
    - Cloud
    - Redes Sociais
- Política de Classificação da Informação
  - Revisar: Lei 12.527/2011 – Lei de Acesso à Informação
  - Implantar / Divulgar / Conscientizar

Segurança da Informação – Desafios

- Gestão de Riscos em Segurança da Informação
  - Normatizar
  - Desenvolver ferramenta de apoio
- Gestão de Incidentes de Segurança da Informação
  - Normatizar
  - Desenvolver ferramenta de apoio
- Controle de Acesso
  - Integrar mecanismos de acesso físico e lógico
  - Definir política corporativa e integrada
- Treinar, divulgar, conscientizar – sempre!

TCU e a Governança de TI



Por que Governança de TI no TCU?

Prestações de contas

Solicitações CN

Denúncias

Documentos gerais

Recursos

Bases de dados

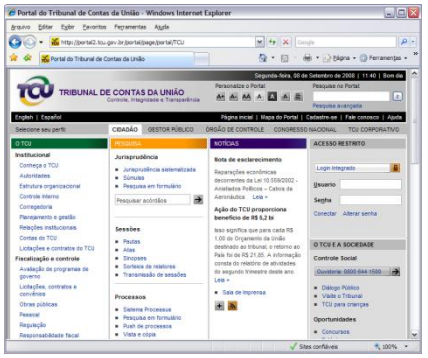
Pareceres e relatórios

Tramitações

Sistemas de informação

Papéis de trabalho

Bases de dados



Acórdãos

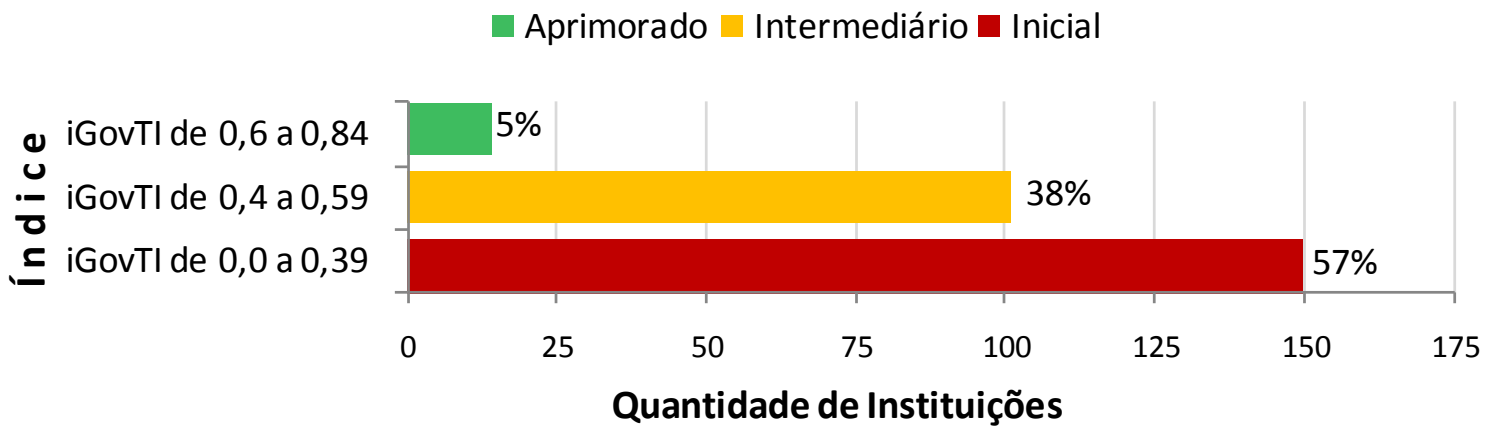
Vistas

Publicações TCU

Informações para o CN

2010 - iGovTI

INSTITUIÇÕES x ESTÁGIOS DO iGovTI



Governança de TI no TCU

Como era em 2008/2010?

Índice de Governança de TI da Instituição (iGovTI)

Nome Instituição: TRIBUNAL DE CONTAS DA UNIÃO

Tipo Instituição: Legislativo **Segmento:** LEG

1.Liderança	2.Estrat. Planos	6.Pessoas	7.Processos	iGovTI	Estágio de Gov. de TI
0,34	0,57	0,78	0,44	0,51	Intermediário

Obs. Desequilíbrio entre as dimensões.

1.1. Em relação à estrutura de governança, a Alta Administração da instituição:

- [x] se responsabiliza pelo estabelecimento e pelo cumprimento das políticas de gestão e uso corporativos de TI.
- [x] designou formalmente um Comitê de TI para **auxiliá-la nas decisões** relativas à gestão e ao uso corporativos de TI.
- [x] designou representantes de todas as áreas relevantes para o negócio institucional para compor o Comitê de TI.
- [x] monitora regularmente o funcionamento do Comitê de TI.
- [ ] nenhuma das opções anteriores descreve a situação desta instituição.

1.2. Em relação ao desempenho organizacional na gestão e no uso de TI, a Alta Administração da instituição:

- [x] estabeleceu objetivos (diretrizes) de desempenho de gestão e de uso corporativos de TI.
- [x] estabeleceu indicadores de desempenho de gestão e de uso corporativos de TI.
- [x] recebe e avalia regularmente informações sobre o desempenho relativo à gestão e ao uso corporativos de TI.
- [ ] acompanha os indicadores de benefício dos principais sistemas de informação e toma decisões a respeito quando as metas de benefício não são atingidas.
- [ ] nenhuma das opções anteriores descreve a situação desta instituição.

2.2. Em relação ao processo de planejamento estratégico de TI, marque a opção que melhor descreve a sua instituição:

- ○ a instituição não executa um processo de planejamento estratégico de TI.
- ○ a instituição desenvolve alguns planos estratégicos de TI, mas não de maneira periódica.
- ◉ a instituição executa um processo periódico de planejamento, embora este não esteja formalmente instituído.
- ● o processo de planejamento estratégico de TI é formalmente (aprovado e publicado) instituído.
- ○ o processo de planejamento estratégico de TI formal é acompanhado segundo indicadores e metas estabelecidos.
- ○ o processo de planejamento estratégico de TI formal é aperfeiçoado continuamente com base na análise de seus indicadores.

7.1. A instituição implementou formalmente (aprovou e publicou) os processos corporativos de segurança da informação abaixo relacionados?

- ☐ Inventariar todos os ativos de informação (dados, hardware, software e instalações).
- ☒ Classificar a informação para o negócio (p.ex. divulgação ostensiva ou restrita).
- ☐ Analisar os riscos aos quais a informação crítica para o negócio está submetida, considerando, pelo menos, confidencialidade, integridade e disponibilidade.
- ☒ Gerenciar os incidentes de segurança da informação.

7.3. Em que nível de capacidade/maturidade melhor se enquadra o seu atual processo de software?

Obs.: com base na ABNT NBR ISO/IEC 15.504

- ○ *Ad hoc* (não há processo e nem conceito de qualidade do processo).
- ◉ Inicial (não há processo nem seu controle, mas já há conceitos de qualidade de processo em implantação).
- ● Gerenciado (há um processo informal repetido várias vezes e que implementa conceitos de qualidade de processo).
- ○ Definido (há um processo formal – aprovado e publicado – e obrigatório).
- ○ Mensurado (o processo é controlado por meio de mensurações e há metas de processo a cumprir).
- ○ Em otimização (o processo é periodicamente revisado e melhorado com base nas suas mensurações).

7.6. A instituição implementou corporativamente os processos de gestão de serviços de TI abaixo relacionados?

Obs.: conceitos baseados na biblioteca ITIL v.3

- ☒ gestão de mudanças ..... ☒ se sim, constituiu um comitê técnico de gestão de mudanças
- ☐ gestão de capacidade
- ☐ gestão de nível de serviço
- ☒ gestão de problemas ..... ☒ se sim, tem base de conhecimento de apoio à gestão de problemas e incidentes
- ☒ gestão de incidentes
- ☐ gestão de configuração ..... ☐ se sim, tem base de dados de gestão da configuração do ambiente computacional
- ☐ gestão financeira
- ☐ gestão de disponibilidade
- ☐ gestão de continuidade ..... ☐ se sim, tem plano de continuidade de negócio em vigor (aprovado e publicado)
- ☒ gestão de liberação

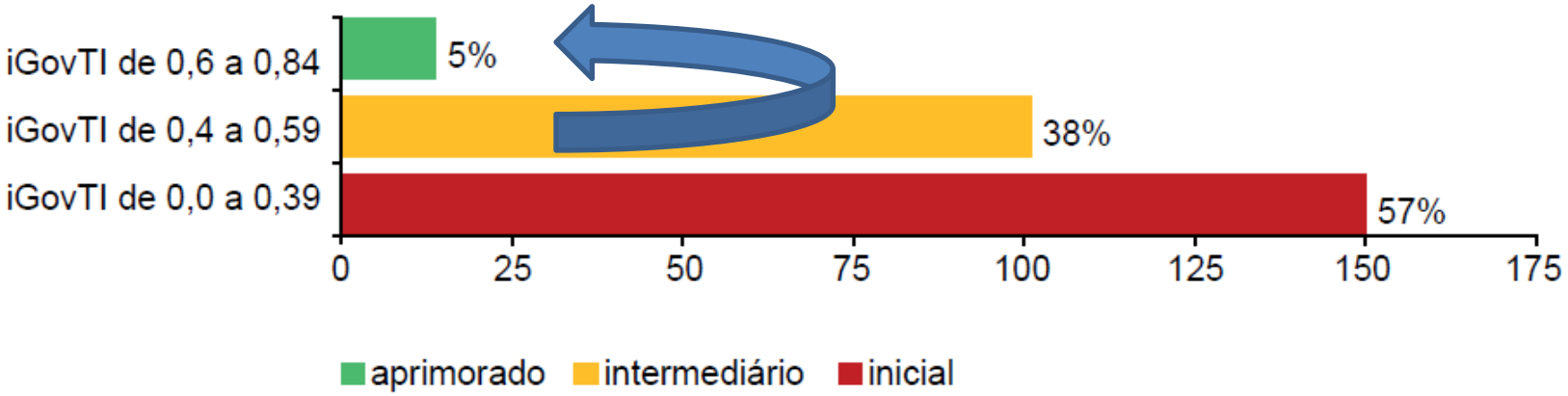
7.7. Em relação à gestão de nível de serviço de TI:

- Não há um portfólio formal (aprovado e publicado) dos serviços oferecidos aos clientes.
- Há um portfólio formal e atualizado dos serviços oferecidos aos clientes.
- Além do item anterior, os níveis dos serviços oferecidos nesse portfólio são monitorados pela área de TI.
- Além do item anterior, são feitos Acordos de Nível de Serviço (ANS) formais com as áreas de negócio clientes.
- Além do item anterior, os ANS são monitorados formalmente e seus resultados relatados periodicamente aos clientes.
- Além do item anterior, os resultados do monitoramento são usados para melhorar os ANS.

7.11. Em relação à fase de gestão dos contratos de TI, em qual das descrições abaixo a instituição se encaixa melhor?

- As diretrizes legais são observadas, mas há grande variação nos procedimentos adotados.
- As diretrizes legais são observadas e os procedimentos reconhecidos como boas práticas são disseminados internamente e praticados.
- Além do item anterior, o processo de gestão de contratos é formalizado (aprovado e publicado) em norma própria e de cumprimento obrigatório.
- Além do item anterior, o cumprimento do processo de gestão de contratos publicado é medido e controlado.
- Além do item anterior, o processo de gestão de contratos é melhorado com base nas mensurações obtidas.

Rumo ao iGovTI 2012



Governança de TI

Como foi feito?

- Questionário do iGov como diagnóstico
  - O que deve ser aprimorado?
  - Que itens nossa cultura interna potencializa?
- Foco principal nas dimensões
  - Liderança
  - Processos
- Parceria com áreas envolvidas
- Meta no Plano de Diretrizes do TCU
  - 0,60 (aprimorado)

Governança de TI

O que foi feito?

- Publicação da Política de Governança de TI (PGTI)
- Mudanças no Comitê Gestor de TI
  - Representantes das áreas de negócio
- Estabelecimento de indicadores de desempenho
- Instituição de plano de treinamento de pessoal de TI
- Implantação de processos ITIL (em andamento)
- Desenho e formalização do processo de gestão de contratos de TI
- Outras ações...

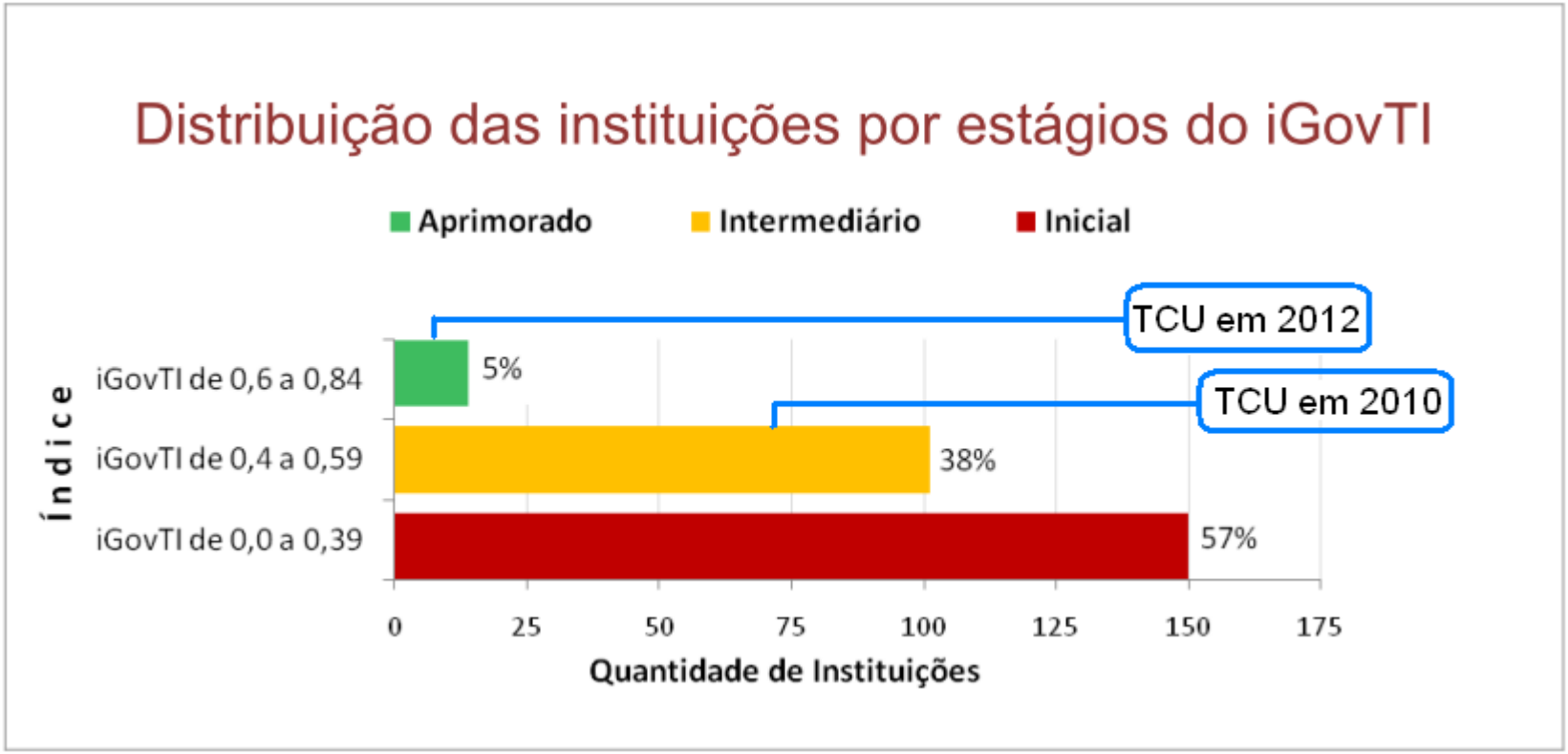
Estrutura Decisória no TCU

	Princípios de TI		Arquitetura de TI		Infraestrutura de TI		Necessidades de Negócio das Soluções de TI		Investimento e priorização em TI	
Contribui	CGTI						UOT		UOT, CGTI	
Decide		CCG		STI e Setic		Setic		UGS		CCG

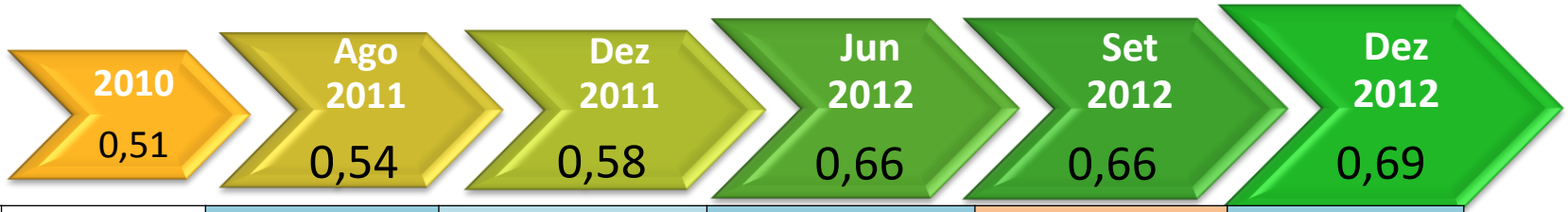
Legenda:
CCG – Comissão de Coordenação Geral
CGTI – Comitê Gestor de TI
UOT – Unidades organizacionais do Tribunal (todas, inclusive as unidades de TI)
UGS – Unidade Gestora de Solução de TI

Obs.: mapeamento baseado em modelo desenvolvido pelo Center for Information System Research (CISR/MIT)

Governança de TI – Como estamos?



Governança de TI – Como evoluimos?



	2010	Ago 2011	Dez 2011	Jun 2012	Set 2012	Dez 2012
LIDERANÇA:	0,34	0,46	0,46	0,58	0,58	0,64
ESTRATÉGIA E PLANOS:	0,61	0,61	0,61	0,70	0,70	0,70
PESSOAS:	0,71	0,71	0,89	0,89	0,89	0,89
PROCESSOS:	0,44	0,45	0,45	0,57	0,57	0,61

Governança de TI – Como evoluimos?

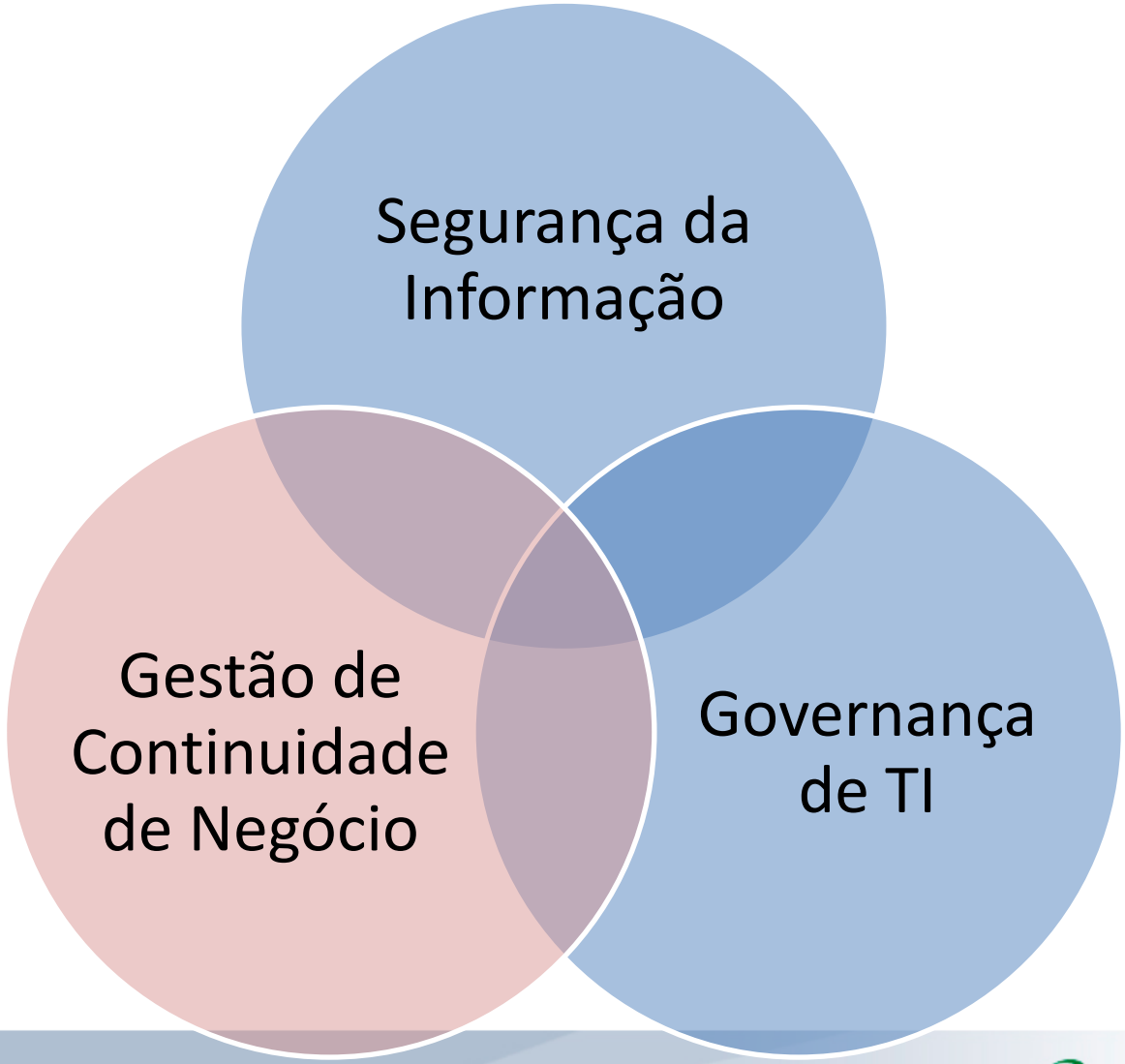
	LIDERANÇA	ESTRAT. E PLANOS	PESSOAS	PROCESSOS
Dez/2012:	0,64	0,70	0,89	0,61
Set/2012:	0,58	0,70	0,89	0,57
Maio/2010:	0,34	0,57	0,78	0,44

Governança de TI

Próximos desafios

- Monitoramento, pela Alta Gestão, do funcionamento do Comitê de TI
- Monitoramento, pela Alta Gestão, do desempenho da gestão e do uso corporativos de TI
- Portfólio de serviços de TI atualizado com Acordos de Nível de Serviço (ANS) internos
- Norma própria que regula as contratações de TI
- Implantação da Gestão de projetos de TI

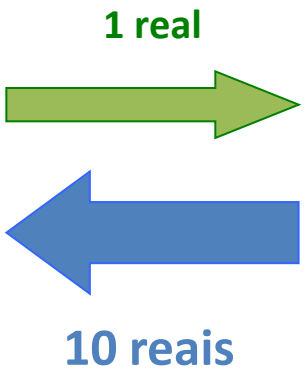
TCU e a Gestão de Continuidade de Negócio



Por que a GCN no TCU?

E se um evento de grandes proporções atingisse o TCU?

- Danos financeiros, de imagem e de conformidade



25/01/2012 20h54 - Atualizado em 26/01/2012 01h44

Prédio desaba no Centro do Rio

Segundo a Defesa Civil, a tragédia deixou 11 vítimas, entre mortos e feridos. Prédio fica na Rua Treze de Maio, perto do Teatro Municipal.

Do G1 RJ, com informações da Globo News

131 comentários | Tweetar 953 | Recomendar 6 mil

Um desabamento atingiu pelo menos dois prédios no Centro do Rio, na altura da Avenida Treze de Maio. De acordo com a empresária Zilene Bernardino, que trabalha no local, desabaram um prédio de dez andares na Rua Manuel de Carvalho, esquina com Treze de Maio, e outro de 21 andares na própria Treze de Maio. A Defesa Civil Estadual informou que o desabamento deixou 11 vítimas, entre mortos e feridos, um deles retirado do meio dos escombros.

Uma moradora de um prédio vizinho relatou que três andares do prédio desabado passavam por reforma. "De repente, ouvimos um grande barulho e começou a voar tudo, e os 18 andares caíram", contou a argentina Devora Galavardo, que mora há seis meses em frente ao prédio que desabou.

Gestão de Continuidade de Negócio no TCU

Como era em 2008?

- Inexistente

GCN no TCU – O que foi feito?

Jan-Nov/2010	Jan-Dez/2011	Jan-Dez/2012
Fase 1: Projeto Piloto **Produtos:** Acordo de Cooperação CEF; Capacitação da Equipe (DRI); Análise de Impacto Simplificada; Escolha de processos críticos;		
	Fase 2: Entendendo a organização **Produtos:** Ratificação dos processos críticos; Análise de Impacto Detalhada por processo; Escolha das Estratégias;	
		Fase 3: Implementação **Produtos:** Preparação da Estratégia; Confecção dos planos; Análise de novos processos;

GCN no TCU

Como foi feito?

- Benchmarking / Acordo de Cooperação
- Desenvolvimento da metodologia
- BIA no processo crítico e não na organização
- Uso de cenários de indisponibilidade
  - de TI
  - de Acesso Físico
  - de Pessoas
- Assig assumiu a responsabilidade pela elaboração

GCN – processos críticos escolhidos

- Após a fase piloto, decidiu-se iniciar a implementação efetiva da GCN abrangendo 2 processos críticos:
  - A realização das sessões colegiadas
  - A instrução eletrônica de processos de controle externo

GCN – Resultados da Análise de Impacto

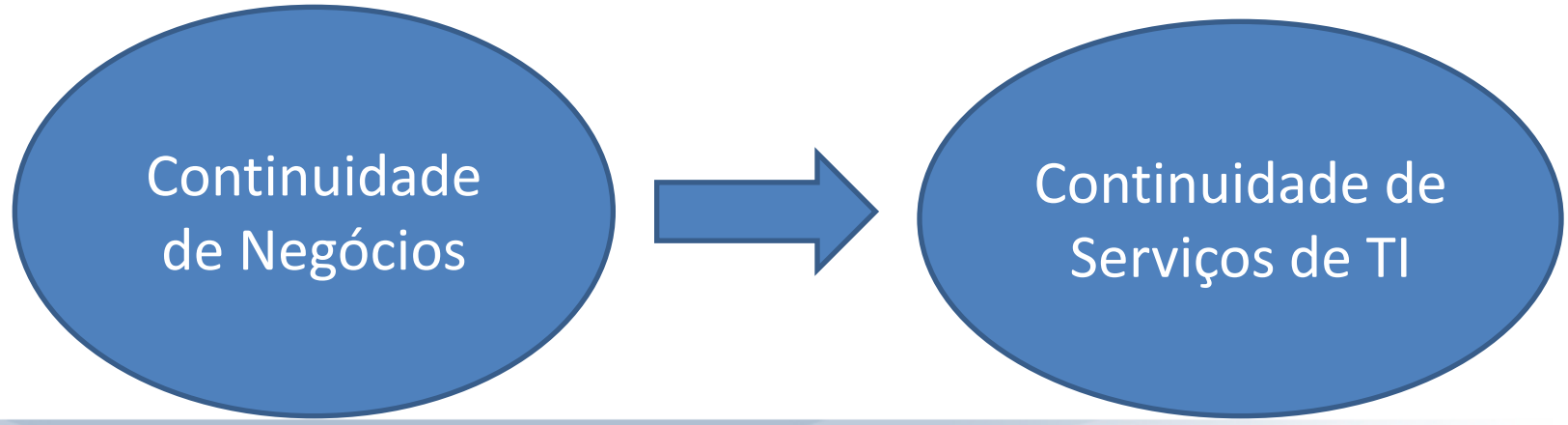
- Realização das Sessões Colegiadas
  - Levantamento com a Secretaria das Sessões
  - 5 atividades críticas encontradas
  - Cenário de maior risco: **Indisponibilidade de acesso físico**
  - Tempo máximo de retorno: 7 dias
- Instrução Eletrônica de Controle Externo
  - Levantamento com 11 unidades (Brasília e Estados)
  - 6 subprocessos e 4 atividades críticas encontrados
  - Cenário de maior risco: **Indisponibilidade de TI**
  - Tempo máximo de retorno: varia por subprocesso

GCN – Estratégias Definidas

- Local físico alternativo próprio (ISC)
  - Menor custo, estruturas de TI prontas e em uso
- Teletrabalho
- Trabalho Off-line (em qualquer dos locais físicos)
- Datacenter de contingência

Continuidade de serviços de TI

- Requisitos de serviços de TI derivados dos relatórios de Análise de Impacto no Negócio
  - Tempos máximos de retorno
  - Serviços críticos a serem retomados no Datacenter alternativo



GCN no TCU – Como estamos?

- Planos de continuidade – encaminhados para aprovação da Alta Gestão
  - Abarcam os três cenários de interrupção
  - Interação com áreas provedoras de recursos para operacionalização (TI, Comunicação Social, Engenharia)
- Planos para uso em Emergências – encaminhados para aprovação da Alta Gestão
  - Plano de Resposta à Emergência
  - Plano de Comunicação em Emergência
- Trabalhos iniciados em dois novos processos críticos
  - Publicação da Relação de Inelegíveis
  - Consultoria Jurídica (resposta a demandas judiciais)

GCN no TCU – Desafios

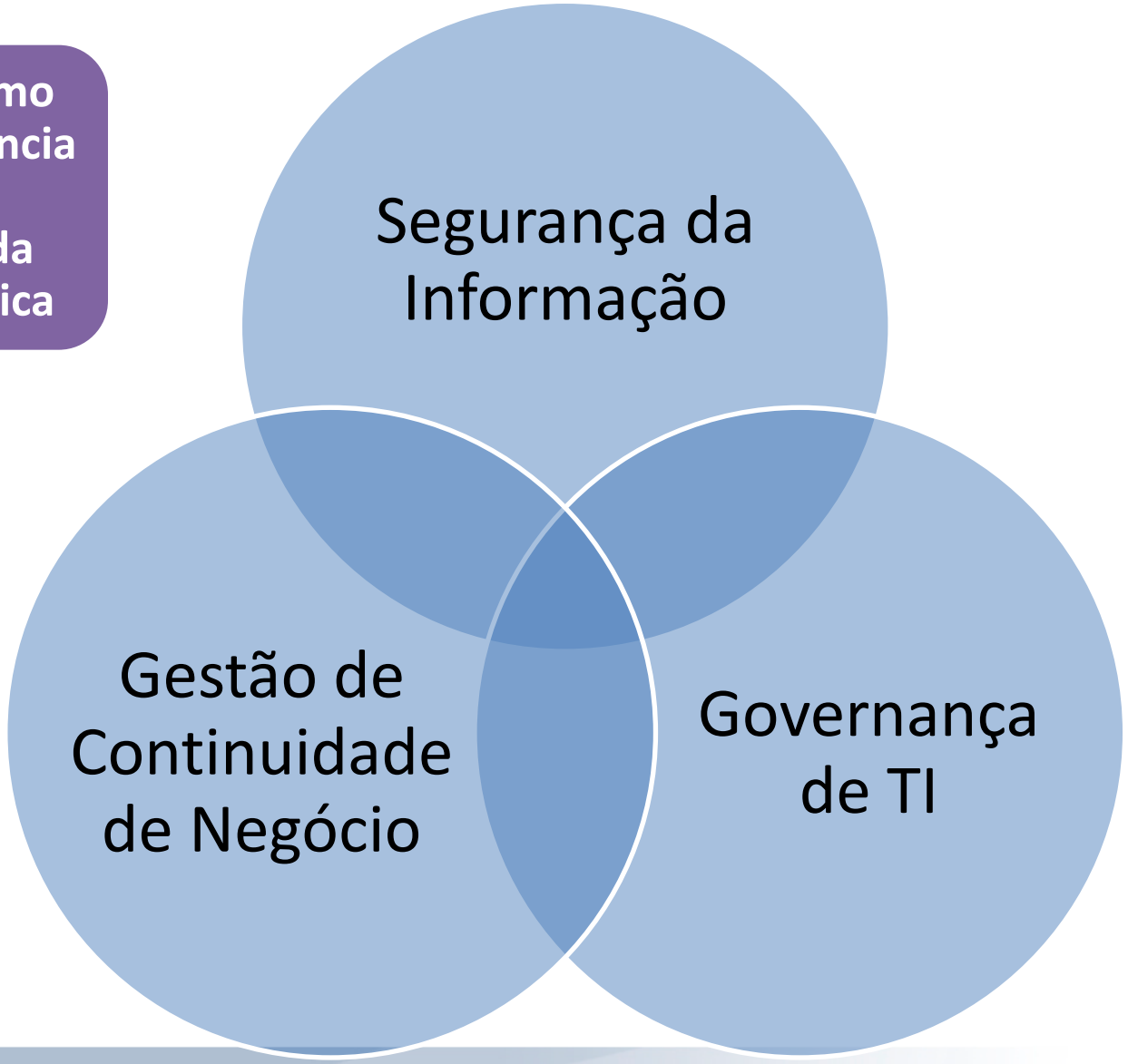
- Planejamento e implementação de testes
  - Aumento gradativo de complexidade
- Elaboração de Política de GCN
- Implantação da Continuidade de TI
  - Plano deve estar aprovado em 2013
- Divulgação da GCN entre os servidores
  - Modificar cultura organizacional

Resultado da Pesquisa de Clima 2012

Pergunta	Comparativo (%)	
	2007 - 2010	2010 - 2012
Os sistemas informatizados do TCU são de fácil utilização	9,33%	20,70%
Os sistemas informatizados do TCU atendem às necessidades do meu trabalho		22,09%
O suporte oferecido ao uso das soluções de informática satisfaz as necessidades do meu trabalho	30,38%	19,76%
As condições dos equipamentos de informática são adequadas para a realização do meu trabalho	16,65%	0,22%
As ferramentas de processo eletrônico (mesa de trabalho, Sagas, Fiscalis, Sisdoc) contribuem para a otimização do meu trabalho		7,32%

Visão do TCU:

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



Obrigada

Marisa Alho

Tribunal de Contas da União

Assessoria de Segurança da Informação e

Governança de Tecnologia da Informação (Assig)

assig@tcu.gov.br

"*Promover a segurança da informação, a governança de TI e a continuidade dos processos críticos, para viabilizar o uso adequado da informação e aperfeiçoar a governança institucional*."