Ministério da Saúde
Departamento de Informática do SUS
DATASUS

Segurança da Informação e Comunicação

SUS Ministério da Saúde BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Segurança da Informação

Conceitos :

- Disponibilidade

  Significa estar acessível e utilizável quando demandado

- Integridade

  Propriedade de salvaguarda da exatidão de informações

- Confidencialidade

  Garantia da proteção contra revelação não autorizada

- Autenticidade

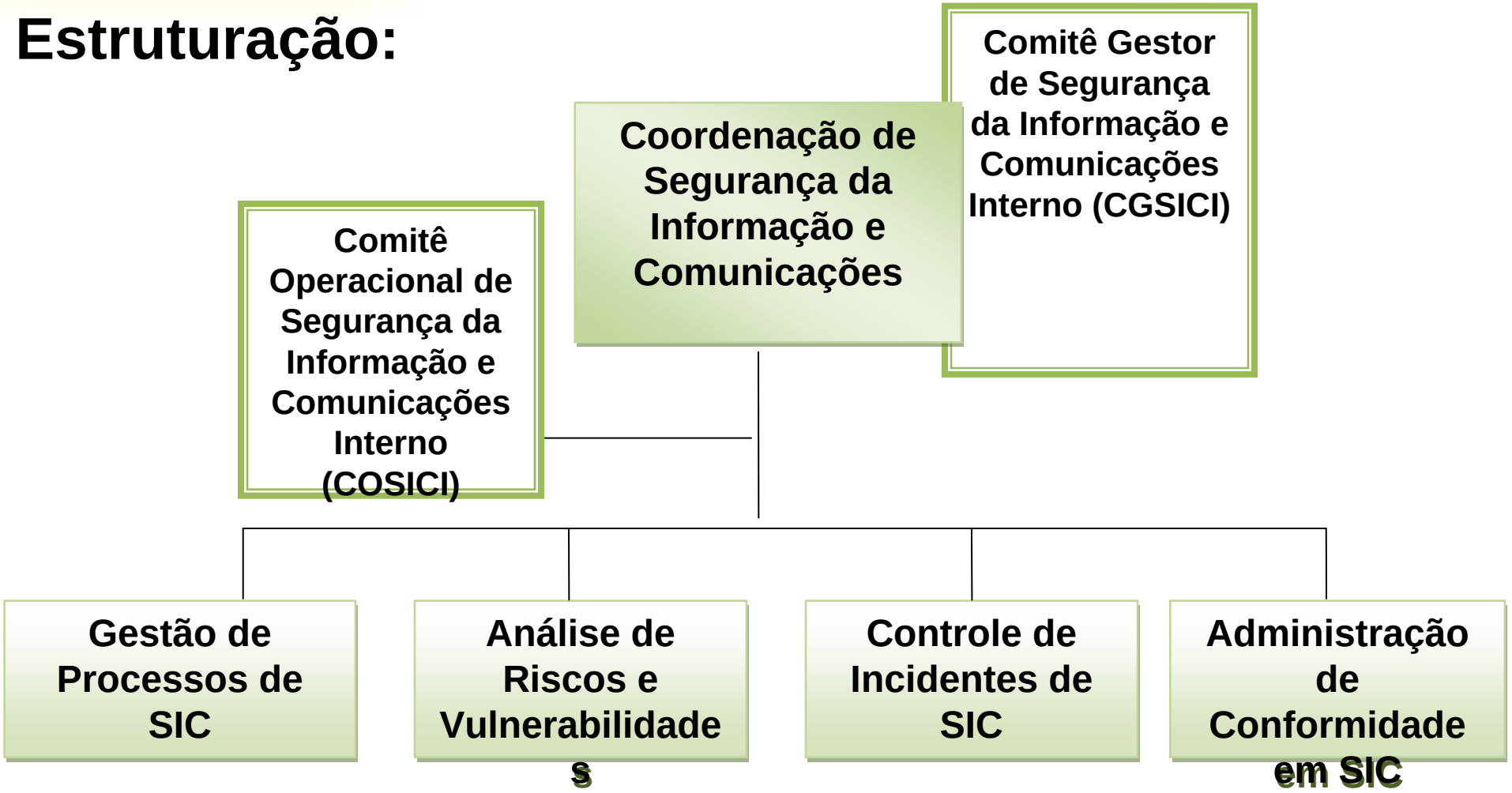
  Certeza absoluta de que a informação provém de fontes anunciadas e que não foi alvo de mutações ao longo da transmissão

Motivadores Legais:

- Decreto lei nº 3.505/2000
- Acórdão TCU 461/2004
- Instrução Normativa GSI/PR nº 01 de 2008
- Norma Complementar GSI/PR nº 02, 03, 04 e 05 de 2009
- Política Nacional de Informação e Informática em Saúde (PNIIS)

GESTÃO EM SEGURANÇA DA INFORMAÇÃO

Estruturação:



PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO

Instrumento norteador das medidas de segurança :

- Projetos de Estruturação e Normatização
- Projetos de Implementação do Ciclo de Gestão
- Projetos Específicos

PROJETOS:

- **Metodologia de Gestão Riscos**
- **Análise de Riscos**
- **Política de Segurança**
- **Modelo de Resposta Incidentes**
- **Preparação para certificação de Conformidade ISO-27001**
- **Classificação Informação**
- **Capacitação em SI**
- **Teste de Invasão**
- **Campanha de Conscientização em SI**
- **GCN - Gestão de Continuidade de Negocio**
- **Análise Código Fonte – DSS**
- **Solução de Criptografia**

Projetos são executados para dar continuidade às ações de segurança

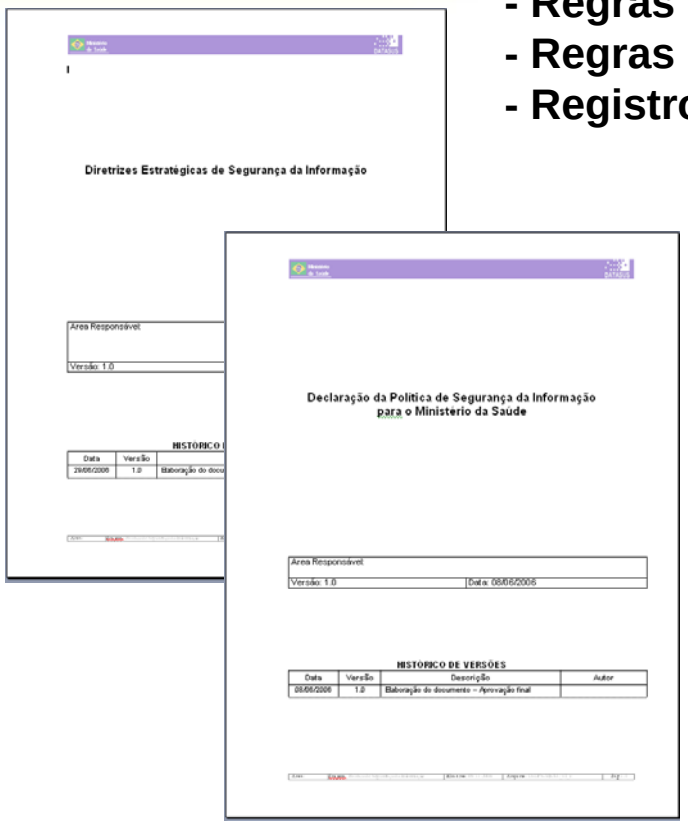
Principais Iniciativas – MS/SE/Datasus

Plano Diretor de Segurança da Informação

PDSI (2008/2011)

- Política de Segurança da Informação e Comunicações
- Campanha Conscientização e Treinamento em SI
- Análise de Riscos Corporativa
- Modelo de Gestão de Segurança da Informação
- Desenvolvimento Seguro de Software
- Maturidade em relação ao COBIT 4.1
- Gestão de Continuidade de Negócios : Estratégia e Testes

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



- Regras gerais de segurança da informação para usuários
- Regras gerais para criação e manutenção de contas e senhas
- Registro de eventos e trilhas de auditoria

SECRETARIA EXECUTIVA
DEPARTAMENTO DE INFORMÁTICA DO SUS

PORTARIA Nº 207, DE 9 DE JULHO DE 2008

O DIRETOR DO DEPARTAMENTO DE INFORMÁTICA DO SUS, no uso da atribuição que lhe confere a Portaria nº. 725, de 31 de julho de 2007, da Casa Civil da Presidência da República e com base na competência regimental estabelecida pelo Art. 7º, Inciso III, do Decreto nº. 5.974, de 29 de novembro de 2006 e no disposto no inciso XI do artigo 7º da Lei 8.080, de 19 de setembro de 1990, e

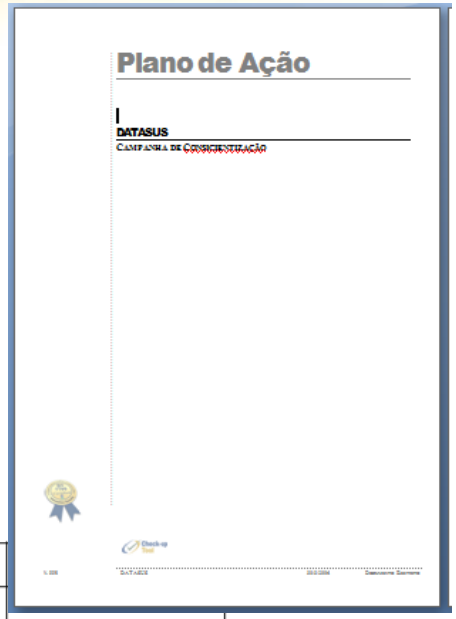
Política institucionalizada (Publicada no DOU), implementada, auditada e analisada para fins de melhoria

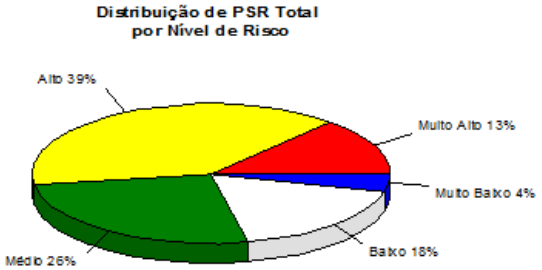
- Norma específica de segurança física de datacenters
- Cessão de base de dados confidencial custodiada pelo Ministério da Saúde
- Dicionário da Política de segurança da informação

SUS Ministério da Saúde BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Organizar, planejar e acompanhar campanha para sensibilizar e disseminar a cultura de segurança da informação.





Domínios de Segurança	% Security Index			
	Geral	Gestores	DF	RJ
Transporte físico	1,03	0	1,39	0
Incidentes de segurança	5,6	5,56	4,01	15,79
Identificação e autenticação	6,61	22,22	4,57	0
Infra-estrutura de segurança	6,87	7,26	5,48	10,51
Código malicioso	16,08	0	15,35	31,58
Direitos de privacidade	21,12	13,89	19,98	31,58
Recursos humanos e prestação de serviços	28,32	30,56	27,73	10,53
Ambiente de trabalho	29,06	43,89	26,92	37,37
Contas e senhas	30,95	32,57	31,61	32,22
Comunicação de dados e voz	35,07	40,99	41,44	41,78
Utilização adequada de recursos	43,36	55,56	44,36	31,58
Direitos de propriedade intelectual	43,5	47,83	40,32	60
Controle de acesso	51,02	64,99	53,27	54,75
Integridade de sistemas e dados	63,72	58,33	65,29	50

Universo total pesquisado	
Questionários respondidos	
Período da Pesquisa	07/03/2006 à 22/03/2006
Primeiro envio da Pesquisa	11.436 questionários
Segundo envio da Pesquisa	9.227 questionários
Terceiro envio da Pesquisa	130 questionários
Aviso de ausência	17
Aviso de caixa cheia	680
Aviso de caixa não encontrada	36
Aviso de retorno DATASUS_RJ – lista errada	1495
Mensagens respondidas por Eber e Marine	130
Mensagens enviadas por usuários no último dia	79

Temas da


Contas e Senhas
Controle de Acesso
Integridade de Sistema
Utilização Adequada dos Recursos
Classificação da Informação
Incidentes de Seguraça
Identificação e Autenticação
Ambiente de Trabalho

Capacitação em SI

Objetivo:

Elaborar e aplicar treinamentos que visem capacitar todos os envolvidos no processo de gestão da segurança da informação no Ministério da Saúde.

Realizado:

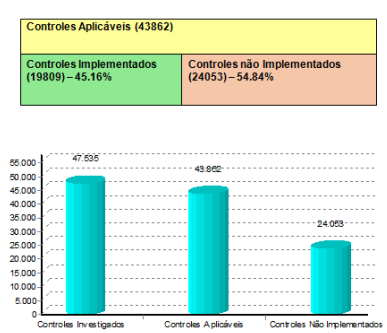
Treinadas 137 pessoas em segurança da informação.

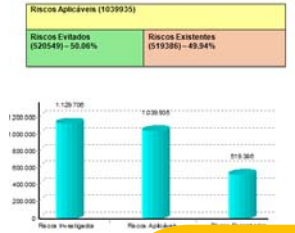
ANÁLISE DE RISCOS

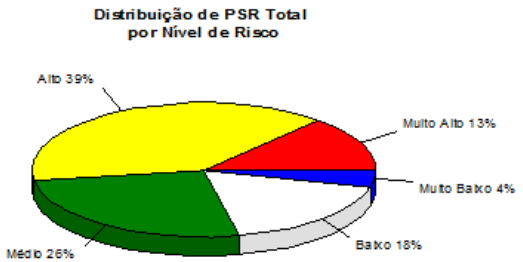
Análise de risco:

Uso sistemático de informações para identificar fontes e estimar o risco

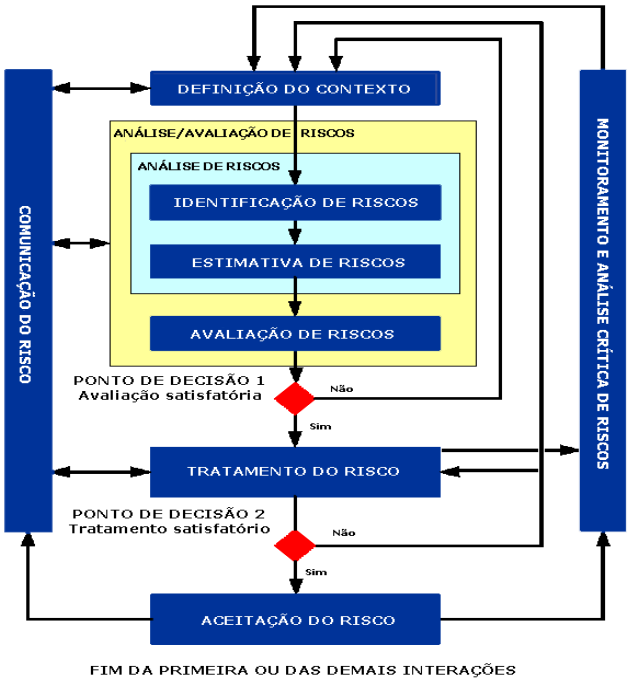
NBR ISO/IEC 27005

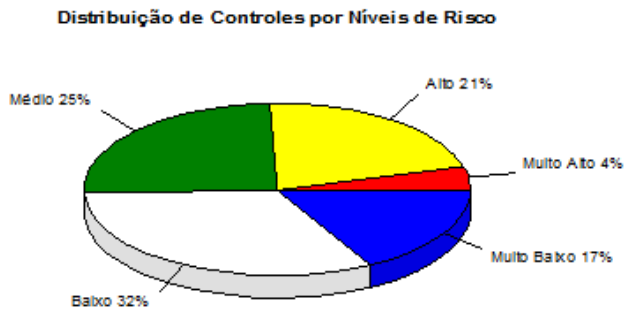






Riscos tratados e medidos periodicamente conforme Probabilidade, Severidade e Relevância





ANÁLISE DE RISCOS

Metodologia:

-Inventario dos ativos
-Identificação de Vulnerabilidades e Ameaças
-Análise dos riscos
-Avaliação dos riscos
-Relatório e comunicação de risco
-Tratamento de risco

Algumas análises de riscos realizadas:

•Alimentação Elétrica da SalaCofre
•Ativos de TI do DATA-CENTER
•Ativos de TI de regionais
•Ambientes críticos do DATASUS
•Contratos
•Sistema – SNT
•Sistema de Telefonia

GESTÃO DA CONTINUIDADE DE NEGÓCIOS

Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, fornecendo uma estrutura capaz de responder efetivamente e salvaguardar os interesses da organização
ABNT/NBR 15999

GESTÃO DA CONTINUIDADE DE NEGÓCIOS

Desafio para MS\DATASUS:

- *Continuidade das operações dos Data-centers de forma completa.*
- *Processos e planos para garantir a continuidade dos sistemas de informação de suporte aos processos de negócio críticos e vitais do Ministério da Saúde.*
- *Estruturação dos plano de continuidade: Recuperação de desastres e de Incidentes*

Estruturação dos plano de continuidade e recuperação e implementação da Gestão de Continuidade de Negócios

-Relatório de Estratégias de Continuidade
-Plano de recuperação de desastre
-Plano de recuperação de incidente
-Testes para validação dos planos

Classificação da Informação

DECRETO Nº 4.553, DE 27 DE DEZEMBRO DE 2002

Ações:

- Critérios para classificação da informação.
- Norma de classificação da informação.
- Fluxo de classificação e tratamento das informações.
- Implementação da norma de classificação como piloto no SNT(relatório e resultado).

Certificação Digital

Medida provisória nº 2.200-2, de 24 de agosto de 2001

- "Art. 1o Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras."

Certificação Digital

Ações:

- Estudo de viabilidade para implantação da ACSaúde – Autoridade Certificadora da Saúde vinculada à ICP-Brasil.
- Piloto de assinatura digital piloto no GESCON – FNS
- Estudo de viabilidade de certificação digital no SISCEL – DST/AIDS

Resposta a incidentes

O que é Incidente?

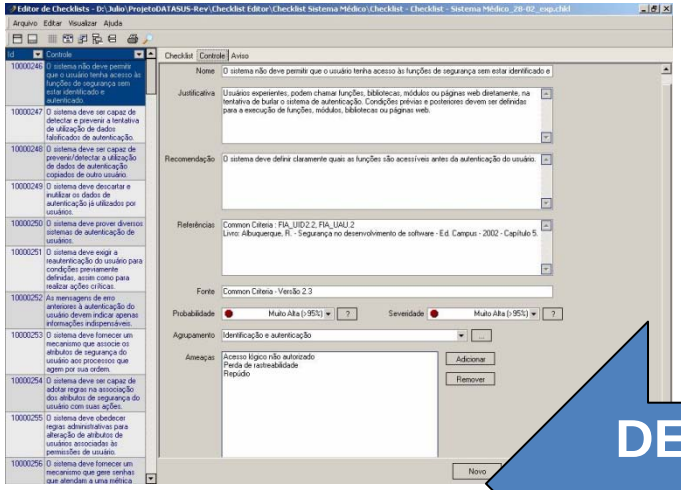
Um evento de segurança da informação indesejado ou inesperado

Desafio:

Aumentar a capacidade de resposta analítica, melhorando a eficiência do atendimento a incidentes de segurança e diminuindo o tempo de reação nas investigações computacionais ocorridas no âmbito do Ministério da Saúde.

DESENVOLVIMENTO SEGURO DE SISTEMAS

Verificar o nível de conformidade dos Sistemas Principais sob o critério da norma ISO/IEC 15408.



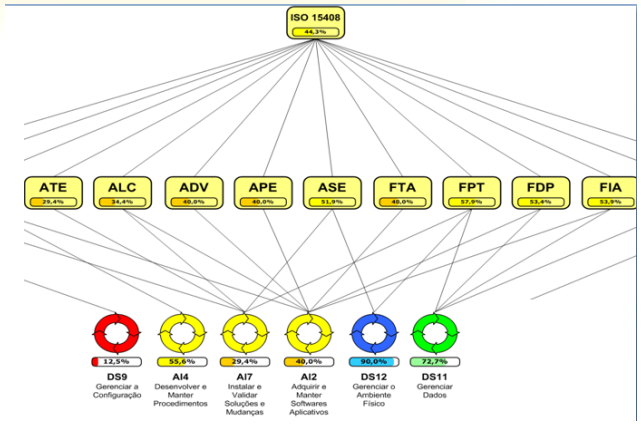
DESENVOLVIMENTO SEGURO

- **Bases de conhecimento**
- **Desenvolvimento**
- **Teste**
- **Homologação**

- **Perfil de segurança**
- **Premissas organizacionais**
- **Classificação dos sistemas**
- **Requisitos não funcionais de segurança**
- **Requisitos funcionais de segurança (Médico, Gerencial, Apoio)**

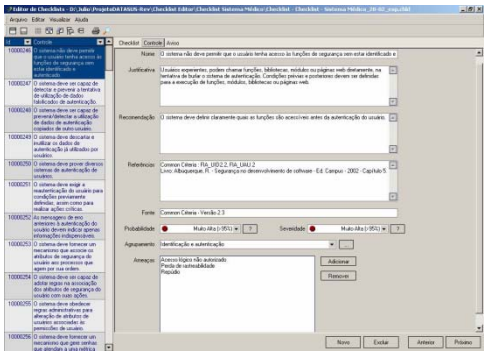
Metodologia divulgada e implementada e o legado analisado

AVALIAÇÃO DE MATURIDADE COBIT



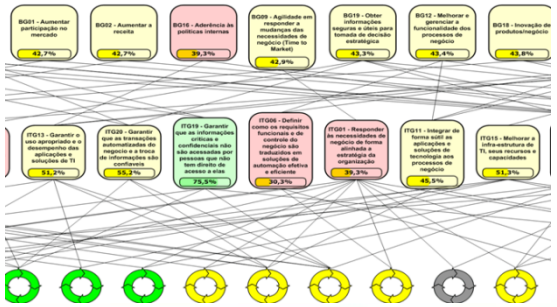
COBIT - Objetivos de Controle para Informações e Tecnologia relacionada

- Bases de conhecimento
- **Desenvolvimento (SUS, Gerencial, Apoio)**
- **Teste (SUS, Gerencial, Apoio)**
- **Homologação**



A Governança de TI deve ser efetivamente implementada

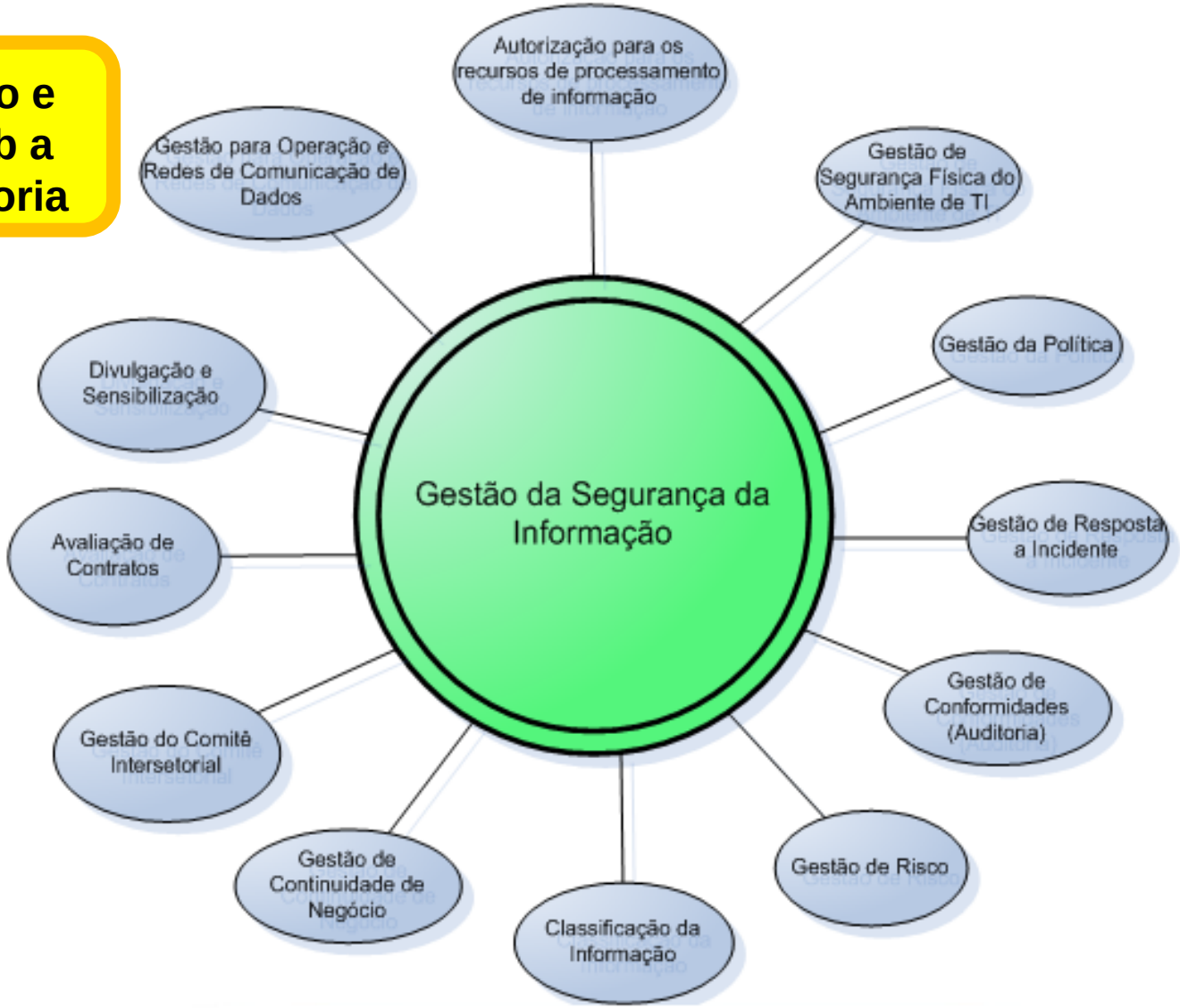
- Relatório de Gap Analysis
- **Maturidade**
- **Conformidade**
- **Recomendações**



- Conformidade com a ISO 27002 (mapeamento)
- Conformidade com a ISO 15408 (mapeamento)

MODELO DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO

Implementado e analisado sob a ótica de melhoria



AUDITORIA TCU
ACÓRDÃO Nº 1603 – 15/08/08 – TCU

- **48% não possui procedimentos de controle de acesso**
- **64% não tem política de segurança da informação**
- **64% não tem área específica de segurança da informação**
- **75% não adota análise de riscos**
- **76% não tem gestão de incidentes**
- **80% não classifica as informações**
- **84% não utiliza gestão de capacidade**
- **88% não usa gestão de mudanças**
- **88% não tem Plano de Continuidade de Negócio**

Adelino.correia@saude.gov.br
Coordenador de Gestão de Redes e Telecomunicações - CREDT

Obrigado.

datasus.csic@saude.gov.br