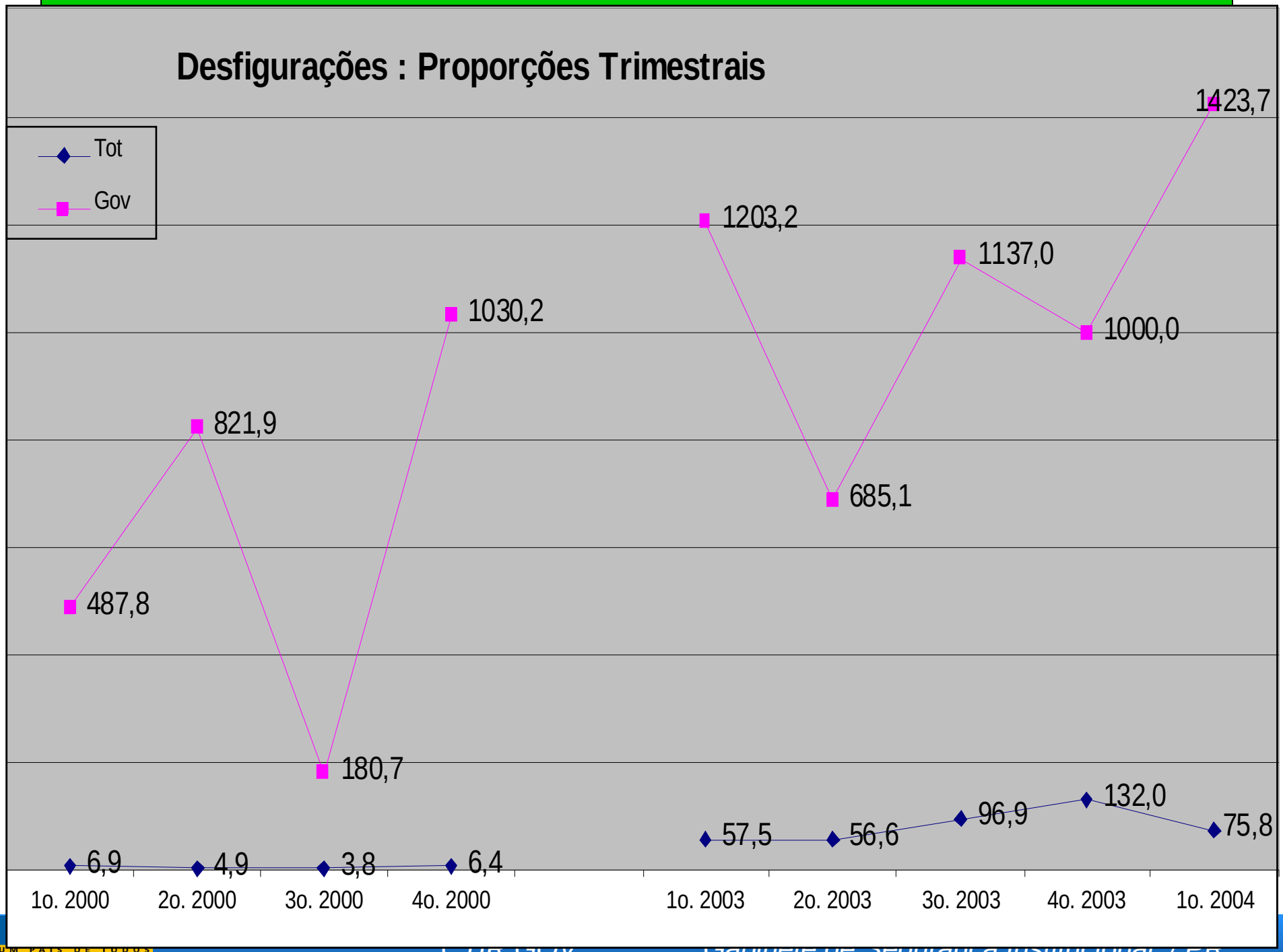
Centro de Tratamento de Incidentes em Redes de Computadores da Administração Pública Federal

CTIR Gov

SSI 2004

Sumário

1. Incidentes em Redes Gov.br
2. Histórico dos Grupos de Trabalho
3. Modelos de Centros
4. Articulação em Redes Gov
5. Interação nas Redes de Centros
6. O Projeto
7. Atendimento à Incidentes
8. Políticas
9. Procedimentos
10. Fases de Implantação do CTIR
11. Resultados


Desfigurações : Proporções Trimestrais
Tot
Gov
487,8
821,9
180,7
1030,2
1203,2
685,1
1137,0
1000,0
1423,7
6,9
4,9
3,8
6,4
57,5
56,6
96,9
132,0
75,8
1o. 2000
2o. 2000
3o. 2000
4o. 2000
1o. 2003
2o. 2003
3o. 2003
4o. 2003
1o. 2004

Histórico - CGSI

- Em 2001 e 2002
  - GT em Segurança de Redes Governamentais

- Em **2003** - Inserido no contexto de **7** Grupos
  - GT do **Centro de Emergência de Computação**
  - Relatório: *Centro de Tratamento de Incidentes de Segurança em Redes de Computadores*

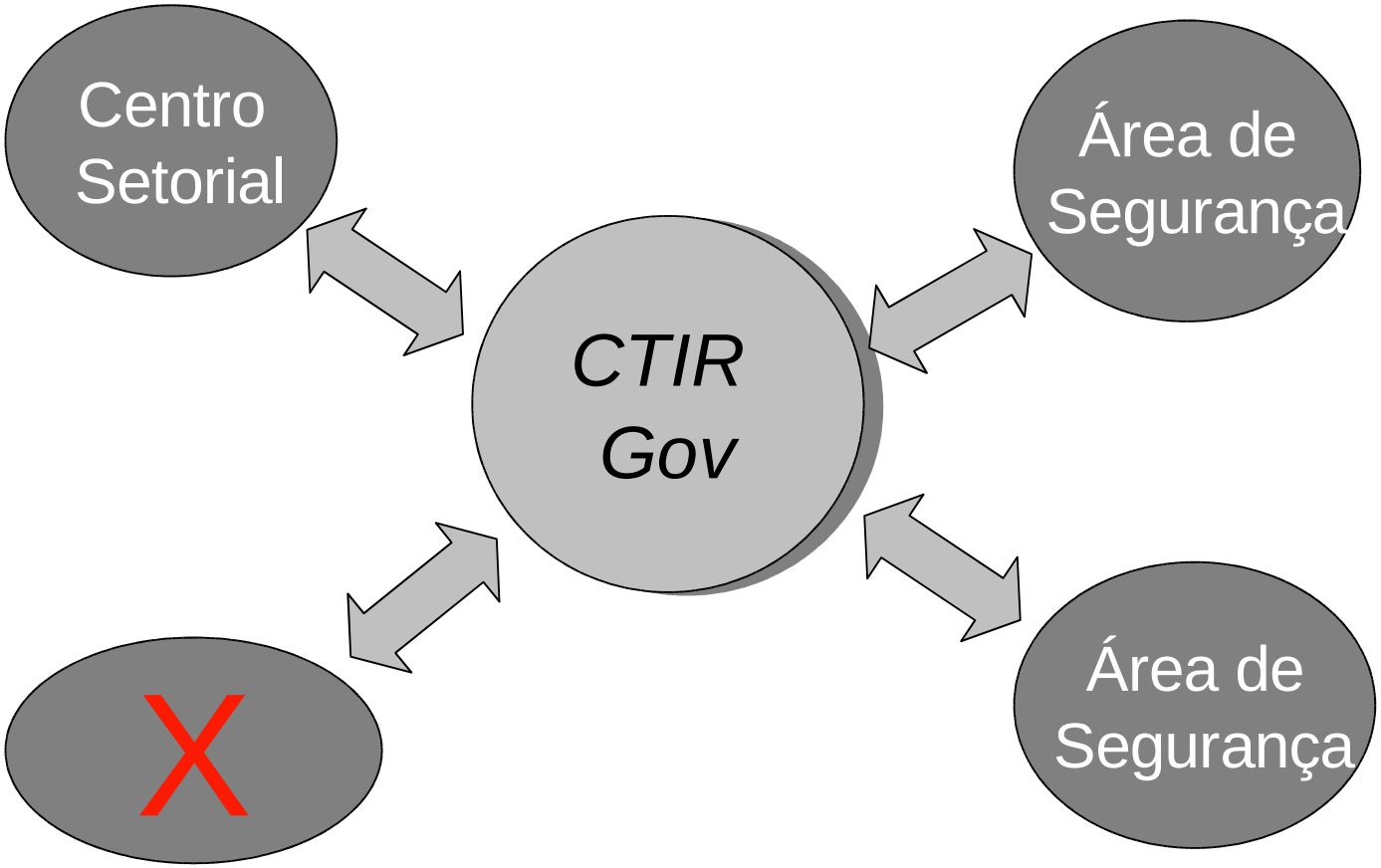
Grupos de Trabalho do Comitê Gestor de Segurança da Informação - 2003

- Normas técnicas e regulamentos para a segurança da informação
- Programa de proteção do conhecimento
- ***Centro de Tratamento de Incidentes em Redes de Computadores do Executivo Federal***
- Uso comercial de criptografia
- Normas para uso e disponibilização da Internet
- Sistemas operacionais de fonte aberta
- Política Nacional de Telecomunicações
- Pesquisa sobre segurança da informação

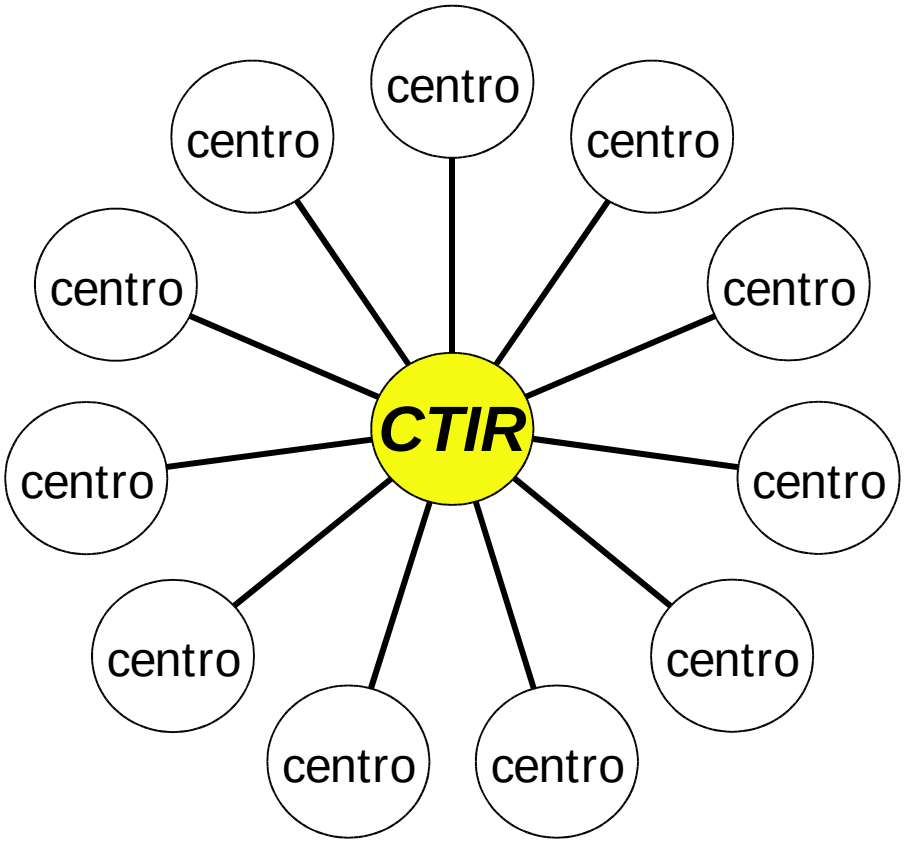
Modelos de Centros

- *Público Interno*
  - Informal
  - Distribuído
  - Centralizado
  - Misto
- *Público Externo*
  - **Articulação** (Coordenação)

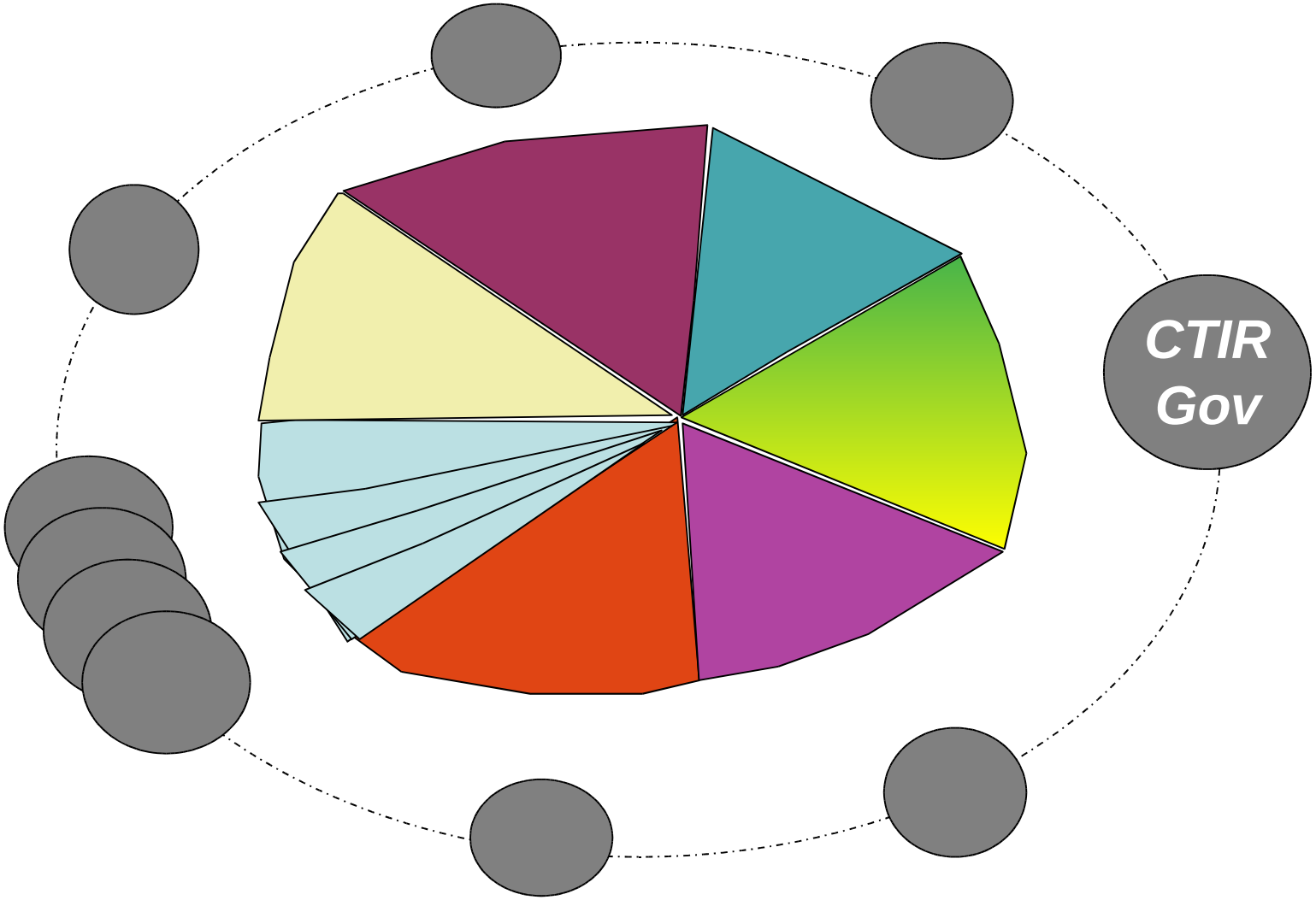
Articulação em Redes Gov



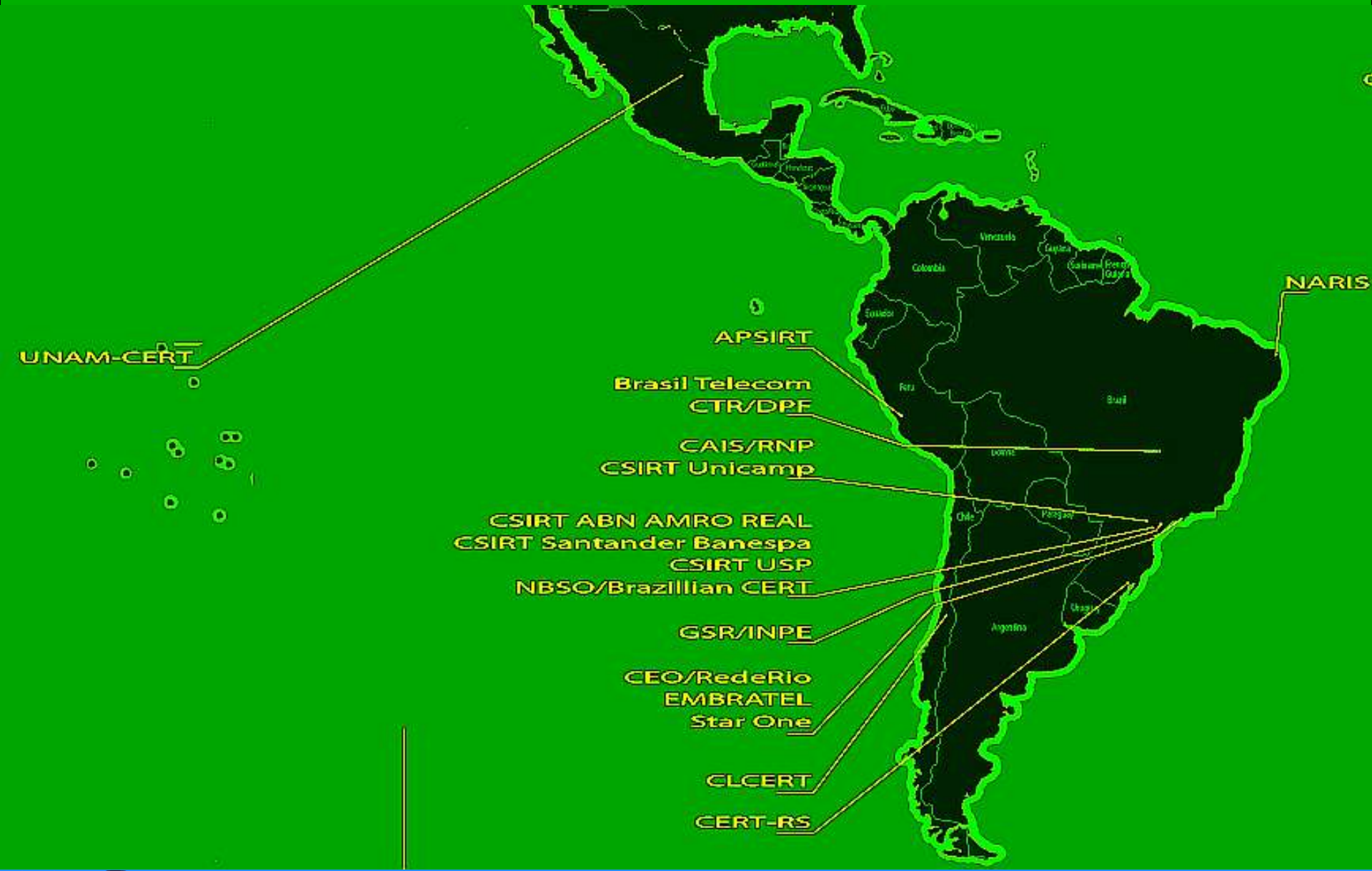
Situação Ideal



Inserção nas Redes de Centros



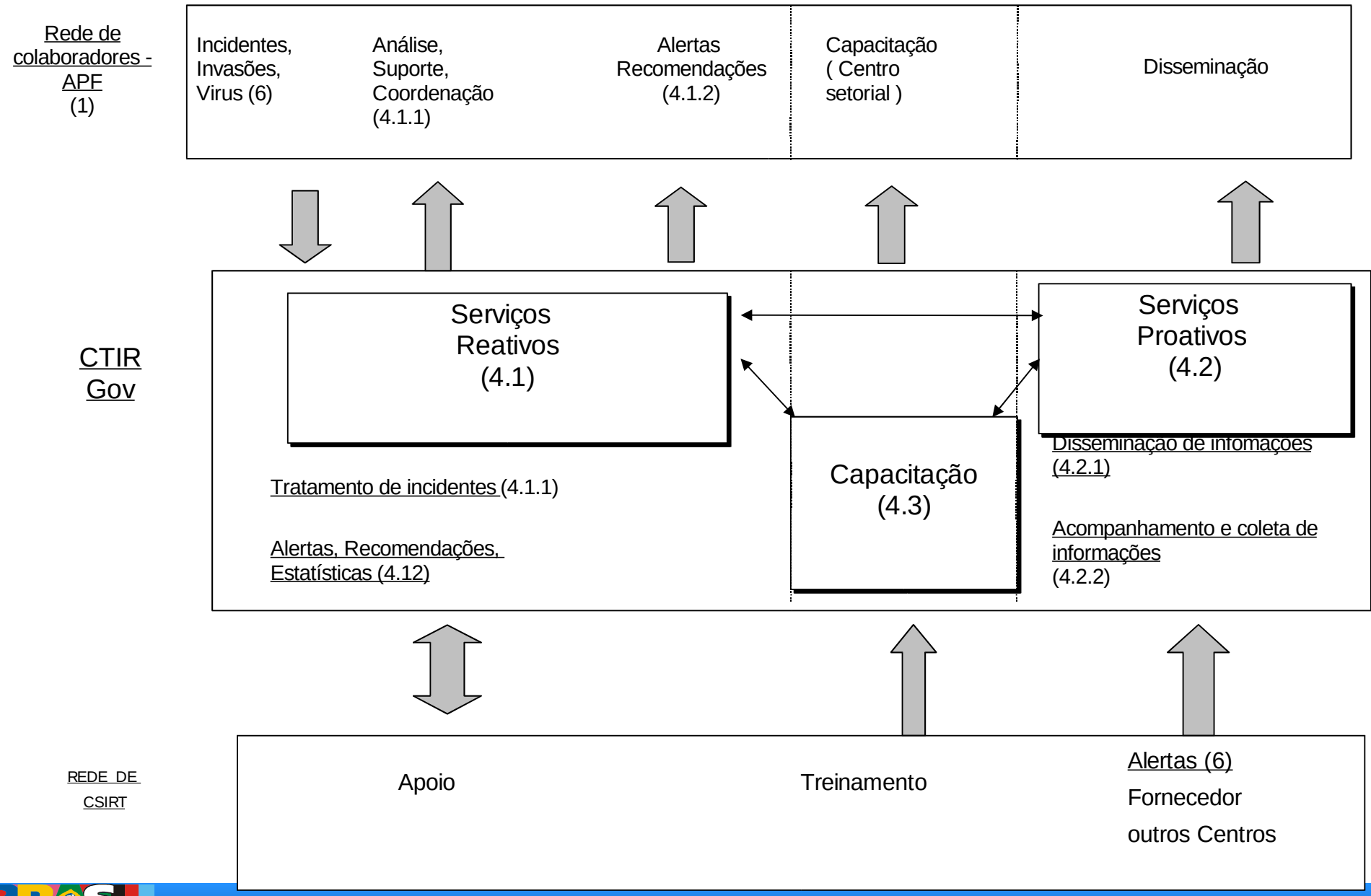
Centros da América Latina



Modelo Organizacional e Institucional do CTIR

1. Público Alvo
2. Missão
3. Autoridade
4. Serviços Prestados
   . Serviços Reativos , Pró-ativos e Capacitação
5. Fluxo de Notificações
6. Atividades Notificadas
7. Localização
8. Dotação Orçamentária
9. Horário de Funcionamento do CTIR
10. Organização do Trabalho e Recursos Humanos
11. Infra-estrutura
12. Organizações de Apoio à Implantação
13. Estratégia de Divulgação da Missão e dos Serviços
14. Relacionamento com outras áreas

Interações do CTIR Gov



Atendimento à Incidentes

- *Serviços Reativos*
  - Tratamento de incidentes
  - Distribuição de alertas e recomendações
- *Serviços Pró-ativos*
  - Guias e boas práticas
  - Acompanhamento de tendências

Políticas

- *Segurança Interna*
- *Classificação da Informação*
- *Notificação de Incidentes*
- *Tratamento de Incidentes*
- *Comunicação Externa*
- *Código de Conduta*

...

Procedimentos

- tratamento de incidentes
- obtenção, análise e guarda de evidencias
- detecção de intrusão
- documentação
- tratamento de grandes eventos
- ...

Resultados

- **Resposta adequada (serviços reativos)**
- **Redução de riscos (serviços pró-ativos)**
- **Referência de fácil acesso**
- ***Rede de Colaboradores***
- **Conhecimento sobre riscos**
- **Acompanhar iniciativas internacionais**

andre.caricatti@planalto.gov.br