SEGURANÇA CIBERNÉTICA NO ESTADO BRASILEIRO

VISÃO DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO

QUEM SOMOS

Ministério do Planejamento, Orçamento e Gestão/MP

- **Missão:** Promover o planejamento participativo e a melhoria da gestão pública para o desenvolvimento sustentável e socialmente includente do País.

- **Representante:** Ministra Miriam Belchior

SLTI – Secretaria de Logística e Tecnologia da Informação/MP

- **SLTI Competência:** Planejar, coordenar, supervisionar e orientar normativamente as atividades de administração dos recursos de informação e informática, de serviços gerais e de gestão de convênios e contratos de repasse, bem como propor políticas e diretrizes a elas relativas, no âmbito da administração federal direta, autárquica e fundacional.
- **Representante:** Secretária Loreni Foresti
- **Órgão Governante Superior - OGS:** Tem 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)

SISP

•Decreto 7.579 de 11 de outubro de 2011

• Art 1º: “Ficam organizados sob a forma de sistema, com a denominação de **Sistema de Administração dos Recursos de Tecnologia da Informação - SISP**, o planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos **recursos de tecnologia da informaçã**o dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, em articulação com os demais sistemas utilizados direta ou indiretamente na gestão da informação pública federal.”

SISP – Eixos Temáticos

CONCEITOS

Principais Conceitos de Segurança da Informação e Comunicações

- Segurança da Informação
- DICA – Disponibilidade, Integridade, Confidencialidade e Autenticidade
- Ativos de Informação
- Política de Segurança da Informação e Comunicações
- Gestão de Riscos de Segurança
- Gestão de Incidentes
- Gestão de Continuidade dos Negócios
- Controles de Acesso

ARCABOUÇO NORMATIVO

Gabinete de Segurança Institucional da Presidência da República – GSIPR (OGS em SIC)

Leis

- **12.527/2011** – Lei Acesso à Informação (LAI)

- **9.983** – Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências.

Decretos

- **3.505/2000** – Política de Segurança da Informação na APF
- **7.724/2012** – Regulamenta a LAI (acesso à informação)
- **7.845/2012** – Credenciamento de segurança para tratamento de informações classificadas

Instruções Normativas

- **01/2008** – Gestão da Segurança da Informação e Comunicações na APF (Revisão)
  - 21 Normas Complementares (Temas: Política de Segurança, Riscos, Continuidade, Incidentes, Nuvem, dentre outros)

- **02/2013** – Credenciamento de segurança para o tratamento de informação classificada

- **03/2013** – Criptografia baseada em algoritmo Estado para informações classificadas

Projetos – SLTI

Estratégia Nacional de Segurança Cibernética Nacional

- Grupo de Trabalho coordenado pela Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR);
- Instituído pela Portaria nº 124/2013;
- **Objetivo:** Definir diretrizes para a Estratégia de Segurança Cibernética para o Estado Brasileiro.
    - Estágio: Desenvolvimentos dos Eixos Temáticos:
    - Governança;
    - Educação em Segurança da Informação;
    - Infraestruturas;
    - Pesquisa e Desenvolvimento.

Estratégia Geral de Segurança Cibernética do SISP

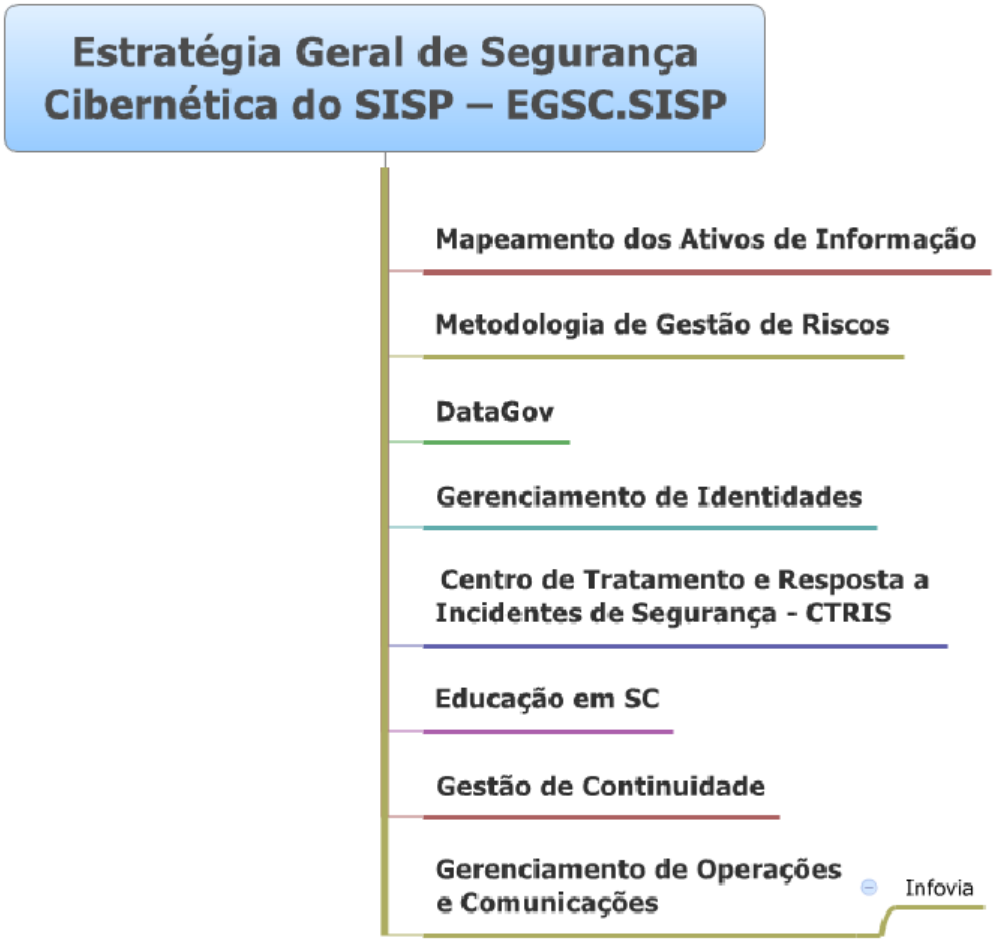
- A Estratégia Geral de Segurança Cibernética (EGSC.SISP) um instrumento de gestão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), que definirá macro diretrizes que possibilitarão o aumento dos níveis da Segurança Cibernética (SC) nos órgãos e entidades do SISP.

- Grupo de Trabalho.

Estratégia Geral de Segurança Cibernética do SISP – Desafios

- Padronização
- Aumento da exposição e da transferência de informações
- Aumento da demanda de informações pelos cidadãos
- Aumento exponencial de compartilhamento de informações
- Fragilidade de identificação do usuário ao acesso à internet
- Compartilhamento de informações e ferramentas de ataque e invasão
- Crescimento exponencial do crime virtual
- Crescente dependência da gestão do Estado por recursos de TIC
- Interdependência entre os ativos de informação
- Tecnologias proprietárias
- Outros desafios...

Estratégia Geral de Segurança Cibernética do SISP – Eixos



Mapeamento dos Ativos de Informação

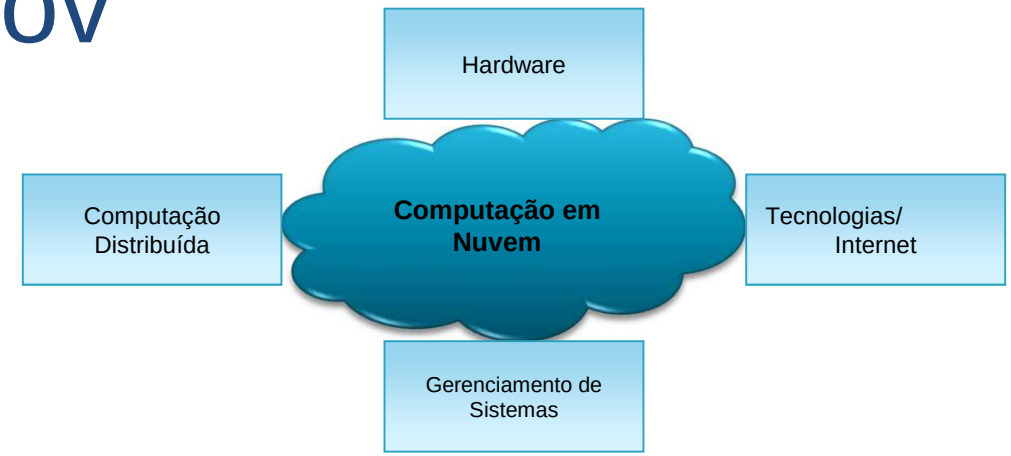
- O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o órgão ou entidade do SISP (NC 10/IN01/DSIC/GSIPR):
  - de um entendimento comum, consistente e inequívoco de seus ativos de informação;
  - da identificação clara de seu(s) responsável(eis) - gestor(es) e custodiante(s);
  - de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação;
  - de uma descrição do local de cada ativo de informação; e
  - da identificação do valor que o ativo de informação representa para o negócio do órgão ou entidade do SISP

Gestão de Riscos de SIC

- **Metodologia**
  - Conjunto de critérios e procedimentos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (NC 04/IN01/DSIC/GSIPR).

- **Ferramenta**
  - Software Público
  - Redução de custos
  - Interoperabilidade

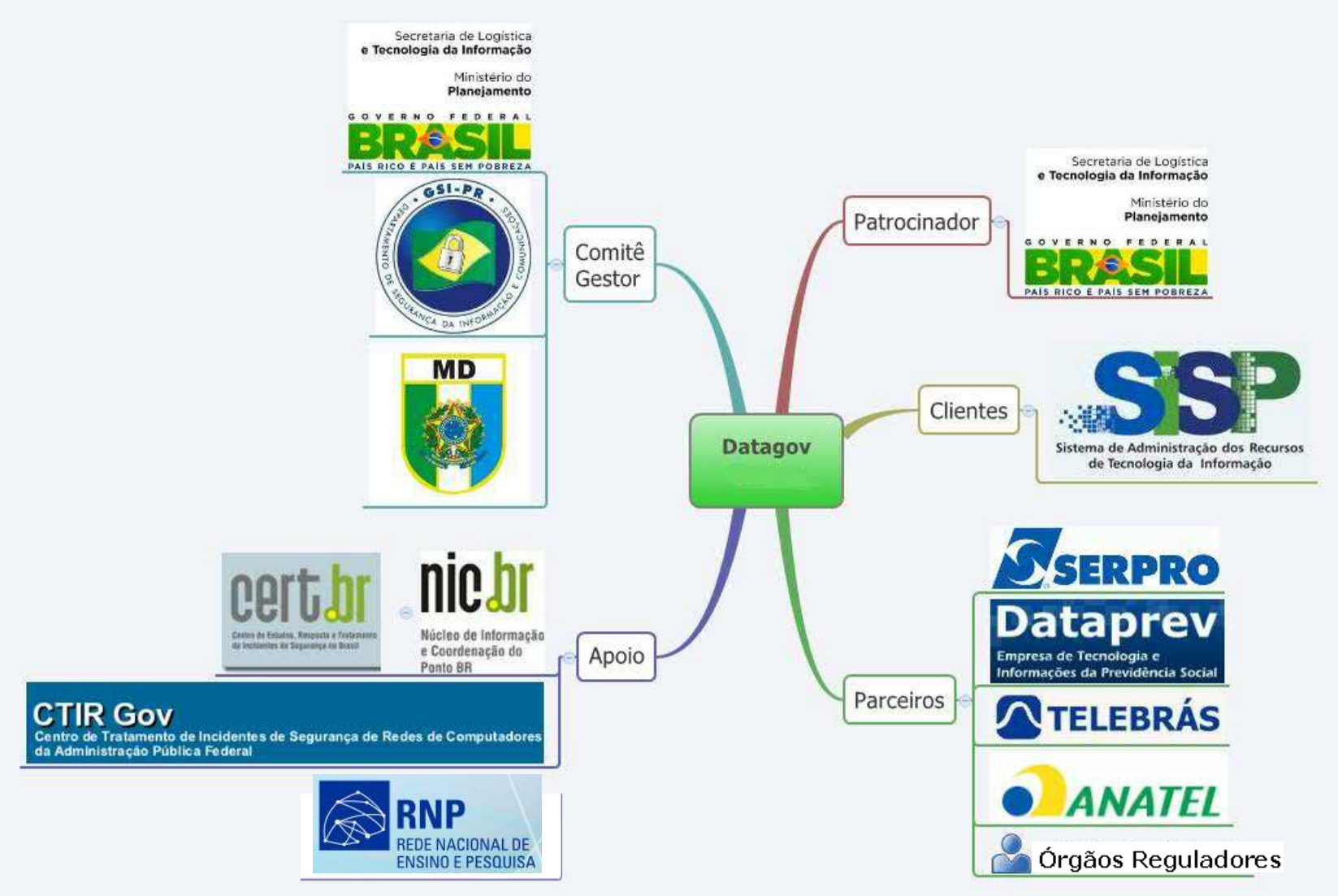
DataGov



Conjunto integrado de componentes de alta tecnologia que possibilitará o fornecimento de serviços de infraestrutura de valor agregado, geralmente processamento e armazenamento de dados, em larga escala e que otimize a utilização dos recursos de TI. (Norma Complementar nº 14/IN01/DSIC/GSIPR e outras)

O DataGov deverá suportar a recuperação dessa infraestrutura em caso de desastres, fazendo com que os órgãos e entidades do SISP continuem a funcionar sem interrupção, de forma a entregar níveis de serviço adequados.

DataGov: Estrutura de Governança



Gerenciamento de Identidade (Identidade Única)

- Conjunto de processos de negócio e de infraestrutura com suporte para criação, manutenção e uso de identidades digitais que darão suporte ao Controle de Acesso Físico e Lógico. (NC 07/IN01/DSIC/GSIPR)

- Projeto em desenvolvimento em parceria com SERPRO/DATAPREV/MPOG

- Piloto: Sistema de Gestão de Pessoal - SIGEP/SIAPE

CTRIS.SISP – Centro de Tratamento e Resposta a Incidentes de Segurança do SISP

•O CTRIS.SISP tem como finalidade o atendimento, análise, resposta aos incidentes em redes de computadores pertencentes aos órgãos e entidades integrantes do SISP.

•Outro objetivo do CTRIS.SISP é coordenar ações relativas a incidentes de forma articulada, auxiliando o SISP no desenvolvimento da cooperação entre os grupos de respostas de incidentes existentes no Brasil e no exterior; no fomento das iniciativas de gerenciamento de incidentes; na distribuição de informações, alertas e recomendações para os administradores de segurança em redes de computadores. (NCs 05 e 08/IN01/DSIC/GSIPR)

•Órgão central de gerenciamento de incidentes

CTRIS.SISP - Estrutura

Centro de Tratamento de Incidentes de Rede

Centro de Tratamento de Incidentes de Segurança

Equipe de Tratamento de Incidentes de Redes

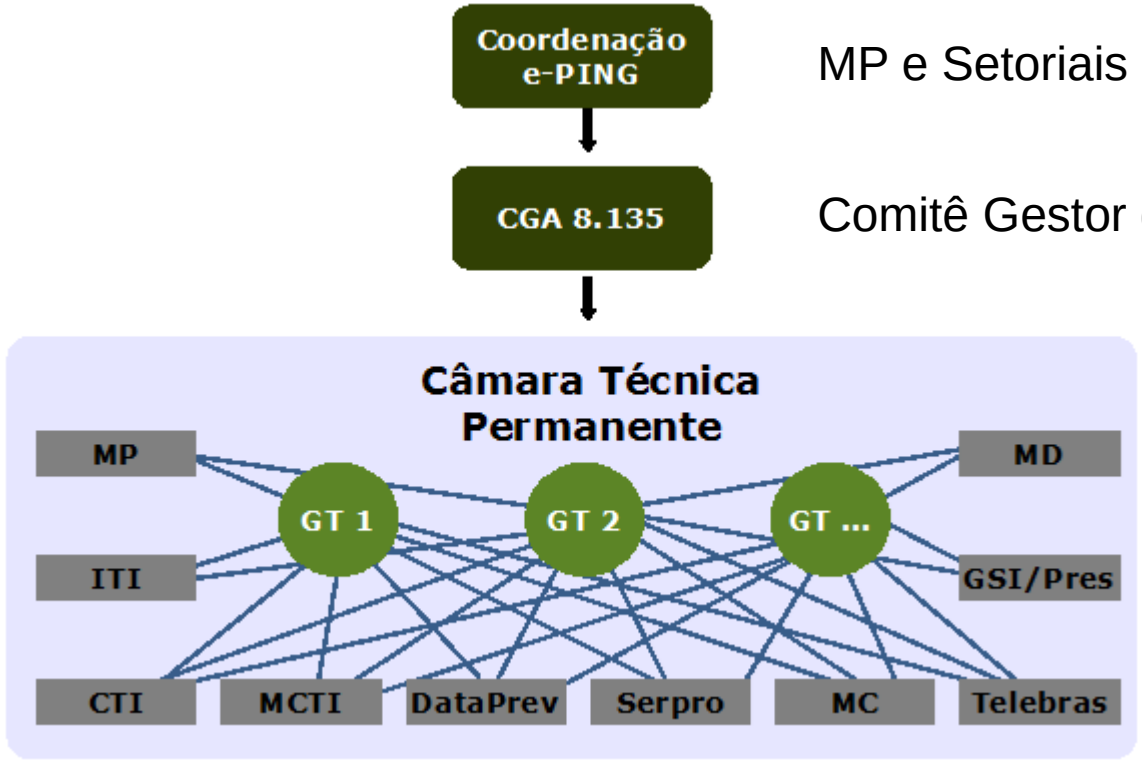
CTRIS.SISP – Visão de Futuro

Padrões Auditoria – Decreto 8.135

- Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.
- Critérios de auditoria: Os programas e equipamentos deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações.
- Ministério do Planejamento, Comunicações e Defesa.

Padrões Auditoria – Decreto 8.135

- Modelo de governança



MP e Setoriais

Comitê Gestor de Auditoria

Gestão de Continuidade dos Serviços Públicos

- Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado. (NC 06/IN01/DSIC/GSIPR)

Ministério do Planejamento, Orçamento e Gestão

Secretaria de Logística e Tecnologia da Informação

Loreni F. Foresti

loreni.foresti@planejamento.gov.br

Obrigado!