ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA PARA O SISP

Brasília, Novembro de 2014

SISP

Decreto 7.579 de 11 de outubro de 2011
(Revoga o Decreto nº 1.048, de 21 de janeiro de 1994)

- 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 informação 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

Art. 3º Integram o SISP:

- Órgão Central (SLTI/MP)
- Comissão de Coordenação (representantes dos órgãos setoriais e órgão central)
- Órgãos Setoriais (unidades de TI dos Ministérios e órgãos da Presidência da República),
- Órgãos Seccionais (unidades de TI das autarquias e fundações),
- Órgãos Correlatos (unidades de TI desconcentradas nos Órgãos Setoriais e Seccionais.)

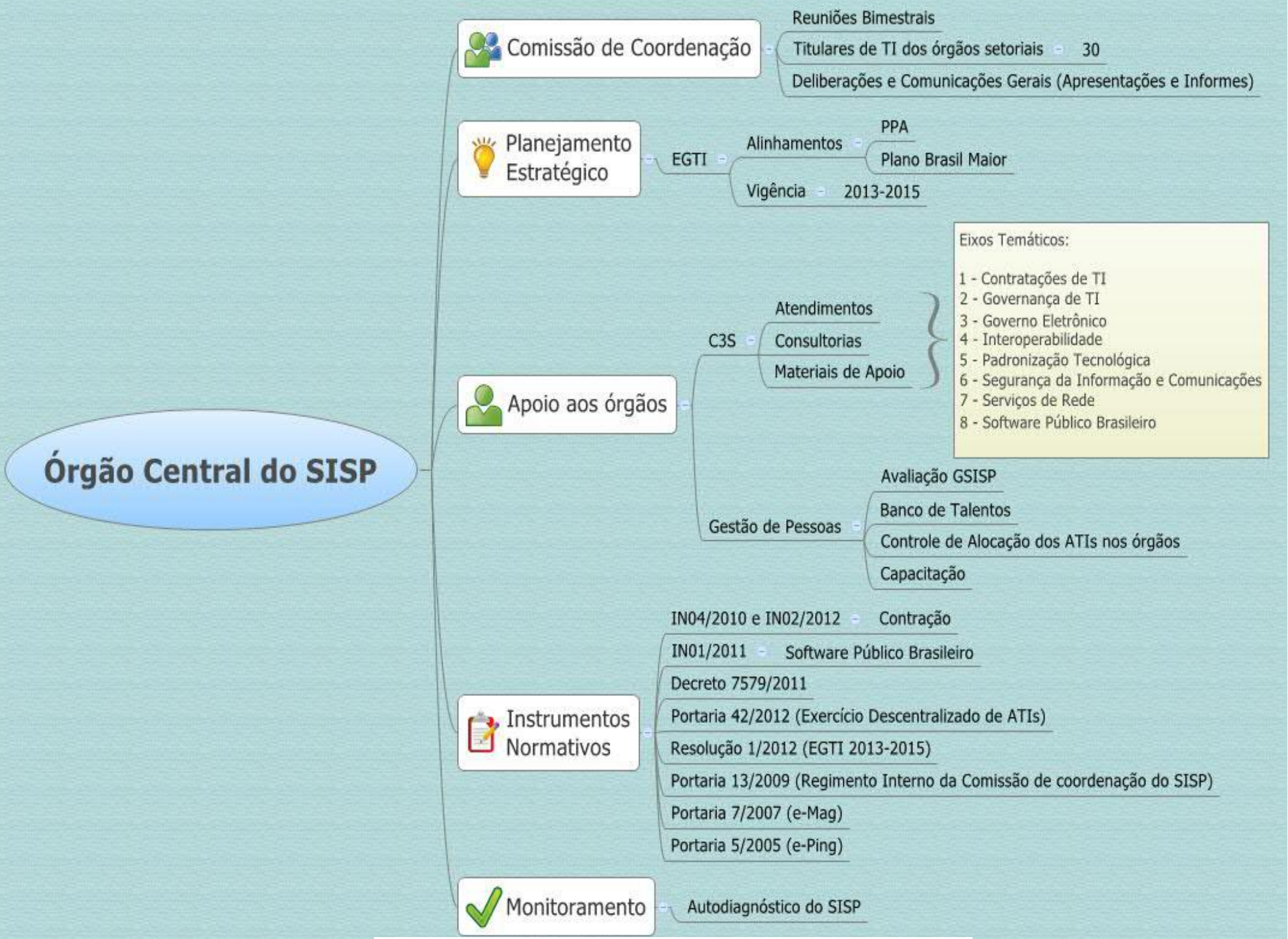
Art. 1º Parágrafo único. É **facultada** às **empresas públicas** e às **sociedades de economia mista** a participação no SISP, cujas condições devem constar de termo próprio a ser firmado entre os dirigentes das entidades e o titular do Órgão Central do SISP.

SISP

Quantitativos

- Órgão Central (SLTI/MP)
- Órgãos Setoriais – 30 (14%)
- Órgãos Seccionais – 163 (74%)
  - 97 (59%) são Institutos ou Universidades
- Órgãos Correlatos – 26 (12%)

Total: **220**

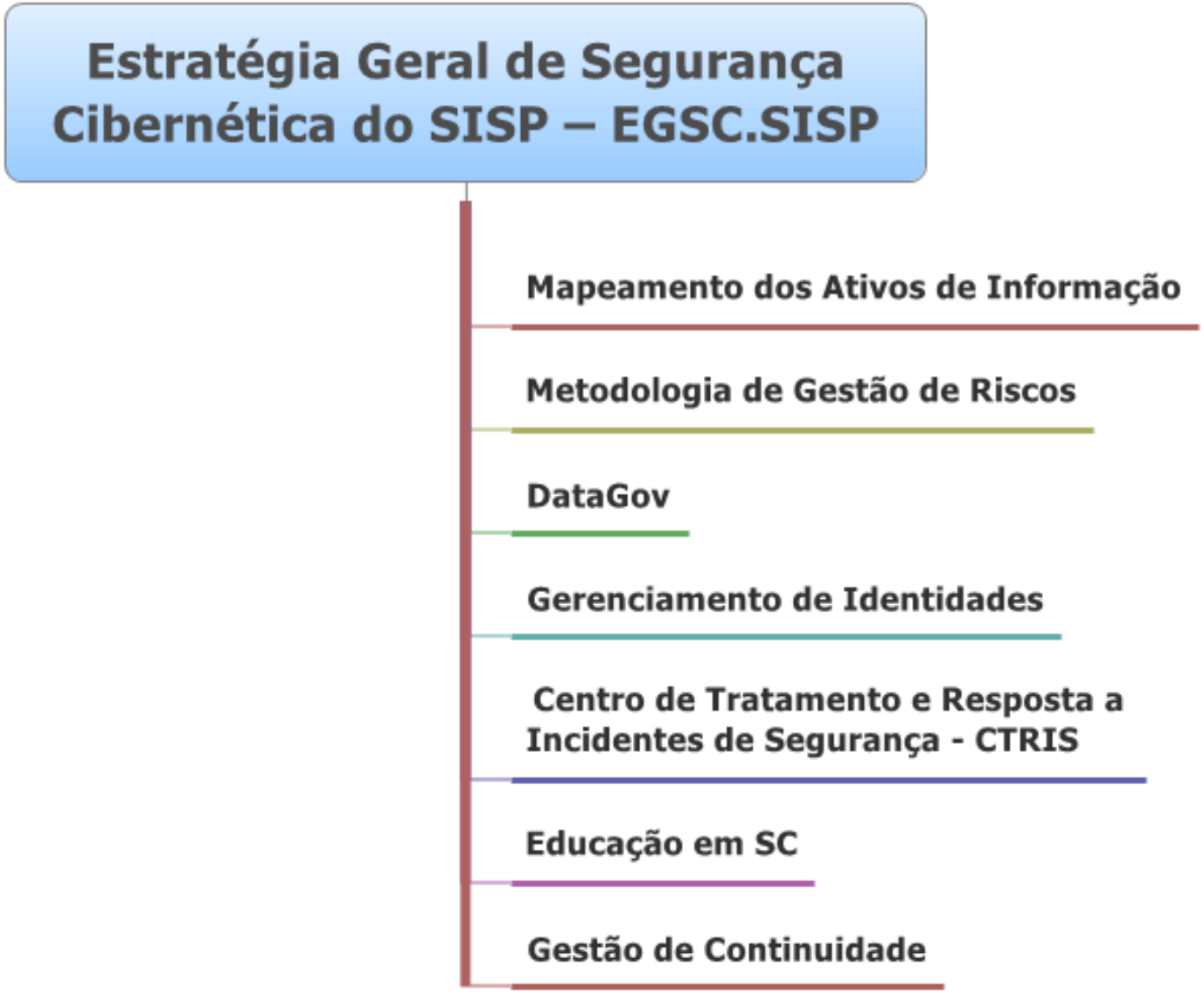


Estratégia Geral de Segurança Cibernética do SISP – EGSC.SISP

A Estratégia Geral de Segurança Cibernética (EGSC.SISP) será 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.

Estratégia Geral de Segurança Cibernética do SISP – Vetores

- Padronização
- Aumento da exposição
- Aumento da demanda de informações pelos cidadãos
- Convergência Digital
- 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 vetores...



Plano Diretor de Segurança Cibernética

O Plano Diretor de Segurança Cibernética (PDSC) é o elemento específico para planejar a Gestão e Governança da Segurança Cibernética, dando suporte aos órgãos do Sistema na elaboração dos Planejamentos de Segurança.

O PDSC é fundamental para se obter coerência e integração com as atividades subsequentes do ciclo PDCA.

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

Metodologia de Gestão de Riscos

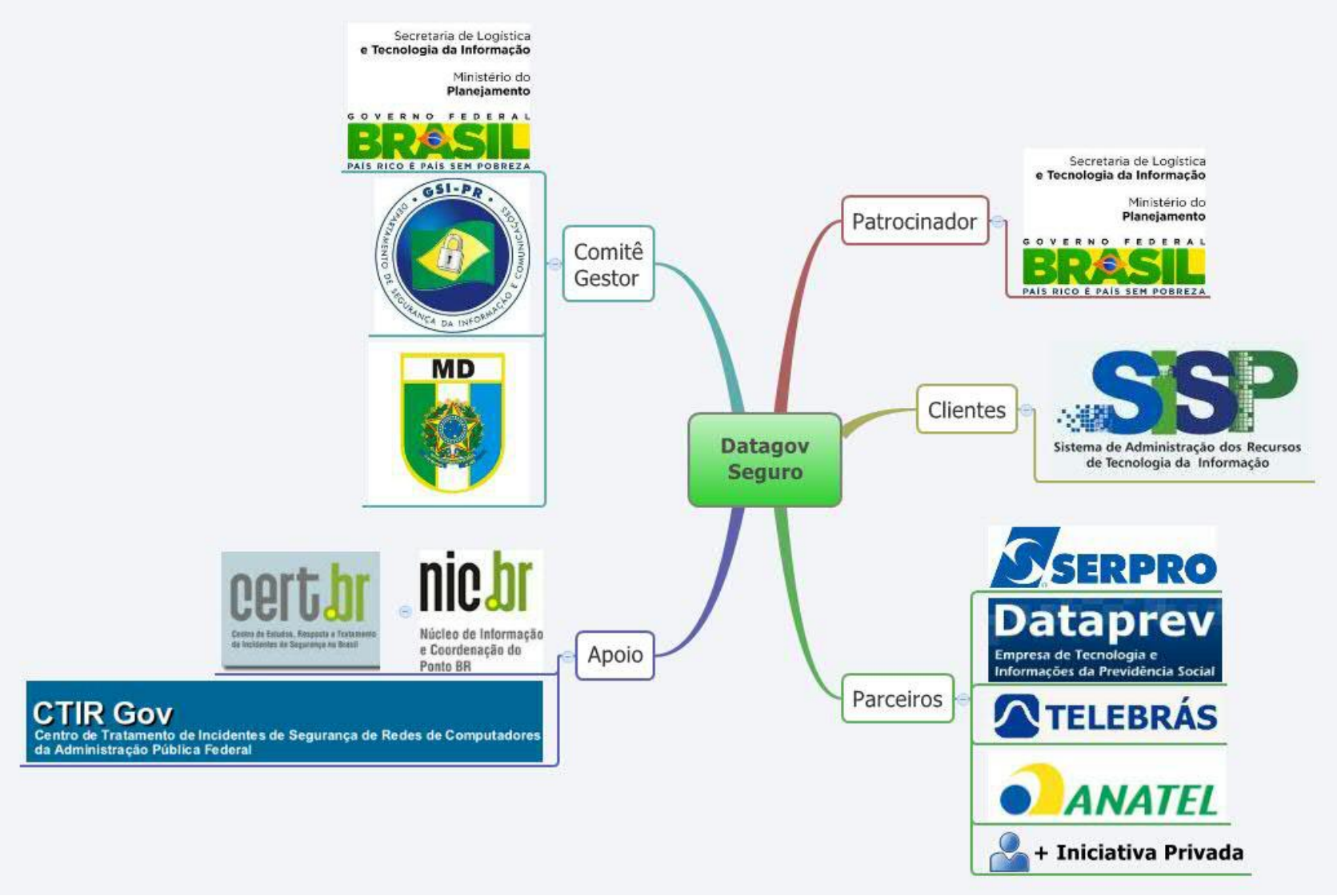
Conjunto de procedimentos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (NC 04/IN01/DSIC/GSIPR).

DataGov

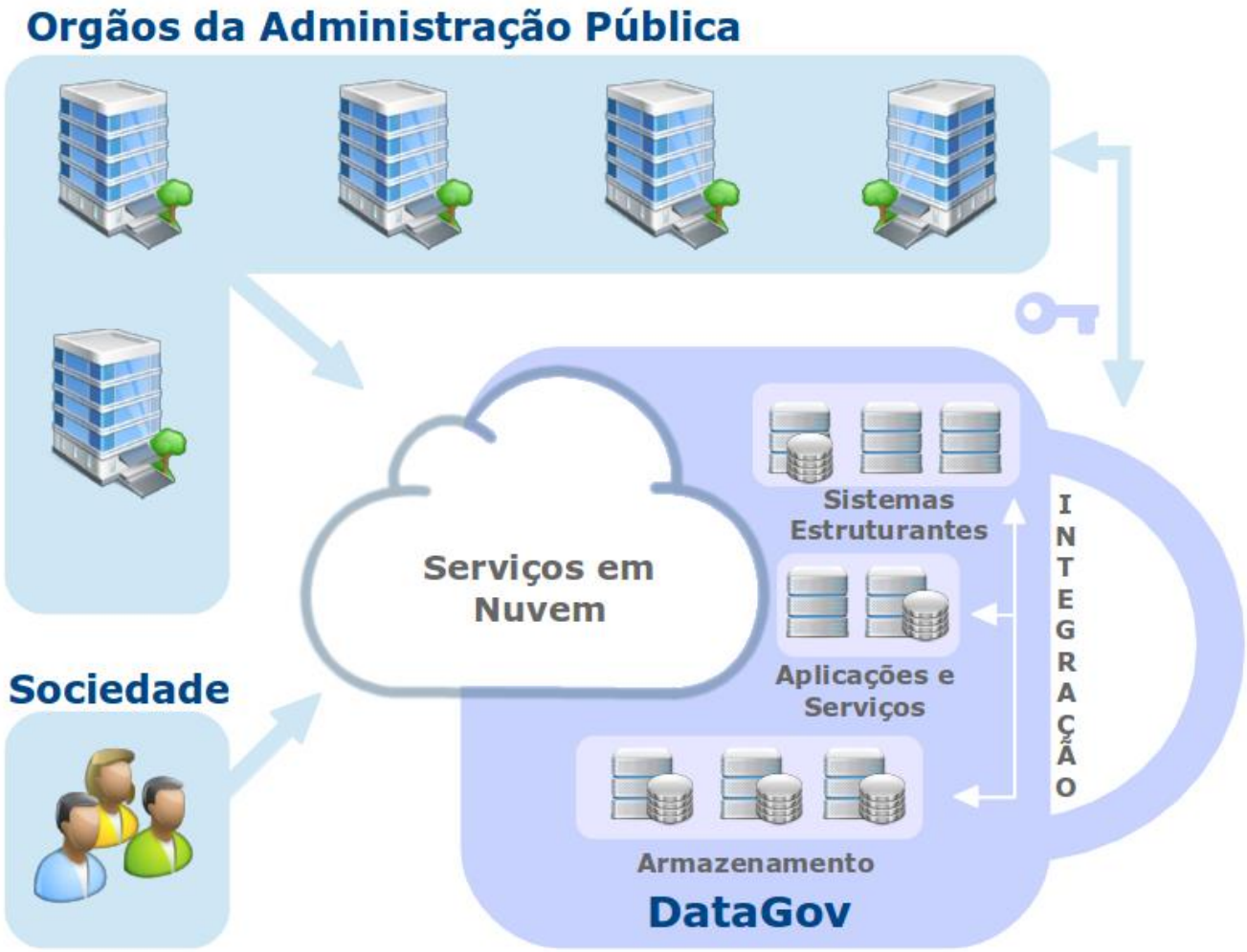
Conjunto integrado de componentes de alta tecnologia que possibilitará o fornecimento de serviços de infraestrutura de valor agregado, geralmente processamento e armazenamento de dados, em larga escala e que otimize a utilização dos recursos de TI.

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



DataGov – Desenho da Infraestrutura



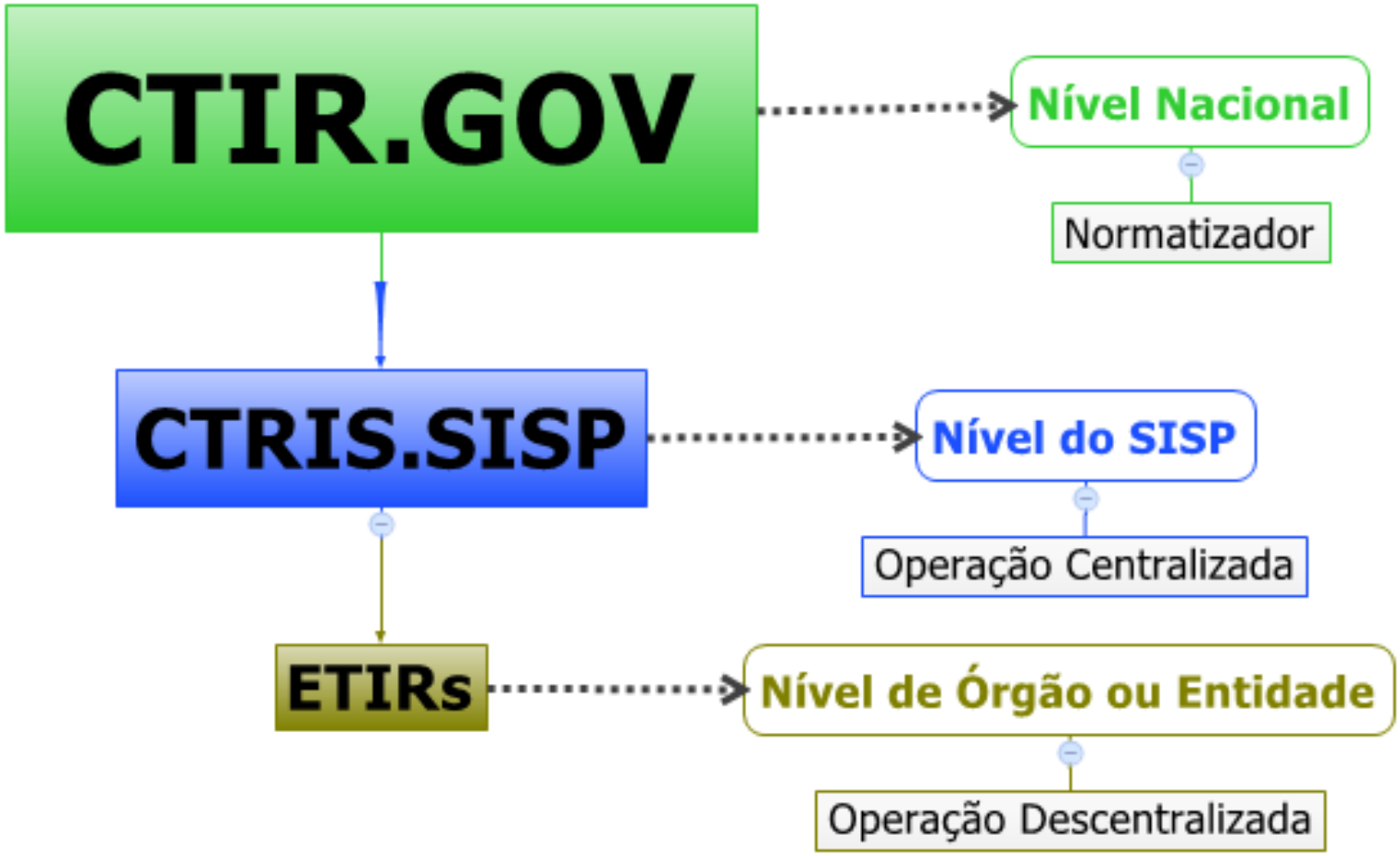
Gerenciamento de Identidades - GI

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)

CTRIS.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)

CTRIS.SISP – Estrutura



CTRIS.SISP – Possíveis Cenários

1	2	3
GSI (CTIR.GOV) + CTRIS	CTRIS + Comitê Gestor Cibernético – GSI ⇩ Câmara Política + Câmaras Técnicas	CTRIS + Câmaras Técnicas

CTRIS.SISP – Interações

Educação em Segurança Cibernética

A Norma Complementar nº 03, de 30 de junho de 2009 ï do Departamento de Segurança Institucional da Presidência da República ï que estabelece diretrizes para Elaboração de Política de Segurança da Informação e Comunicações, recomenda aos órgãos e entidades da APF, promover a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.
(NC 18/IN01/DSIC/GSIPR)

Educação em SC – Atividades de Ensino

Sensibilização: orientar sobre o que é Segurança da Informação e Comunicações (SIC) fazendo com que os participantes possam perceber em sua **rotina pessoal e profissional** ações que precisam ser corrigidas.

Conscientização: orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua **rotina pessoal e profissional**, além de servirem como **multiplicadores** sobre o tema.

Capacitação: orientar sobre o que é SIC, fazendo com que os participantes saibam **aplicar os conhecimentos** em sua rotina pessoal e profissional, além de servirem como **multiplicadores** sobre o tema, estando **aptos para atuar em suas organizações como Gestores de SIC**.

Especialização: orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC, além de tornarem-se **referência na pesquisa de novas soluções e modelos de SIC**.

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)