Segurança da informação e comunicação (SIC)

ações e desafios da SLTI

Cristiano Rocha Heckert

Brasília, 24 de setembro de 2015

Câmara dos Deputados

Secretaria de Logística e Tecnologia da Informação

Ministério do Planejamento

GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

Secretaria de Logística e Tecnologia da Informação

Logística pública

Governo eletrônico

Sistemas de informação

Infraestrutura e serviços de rede

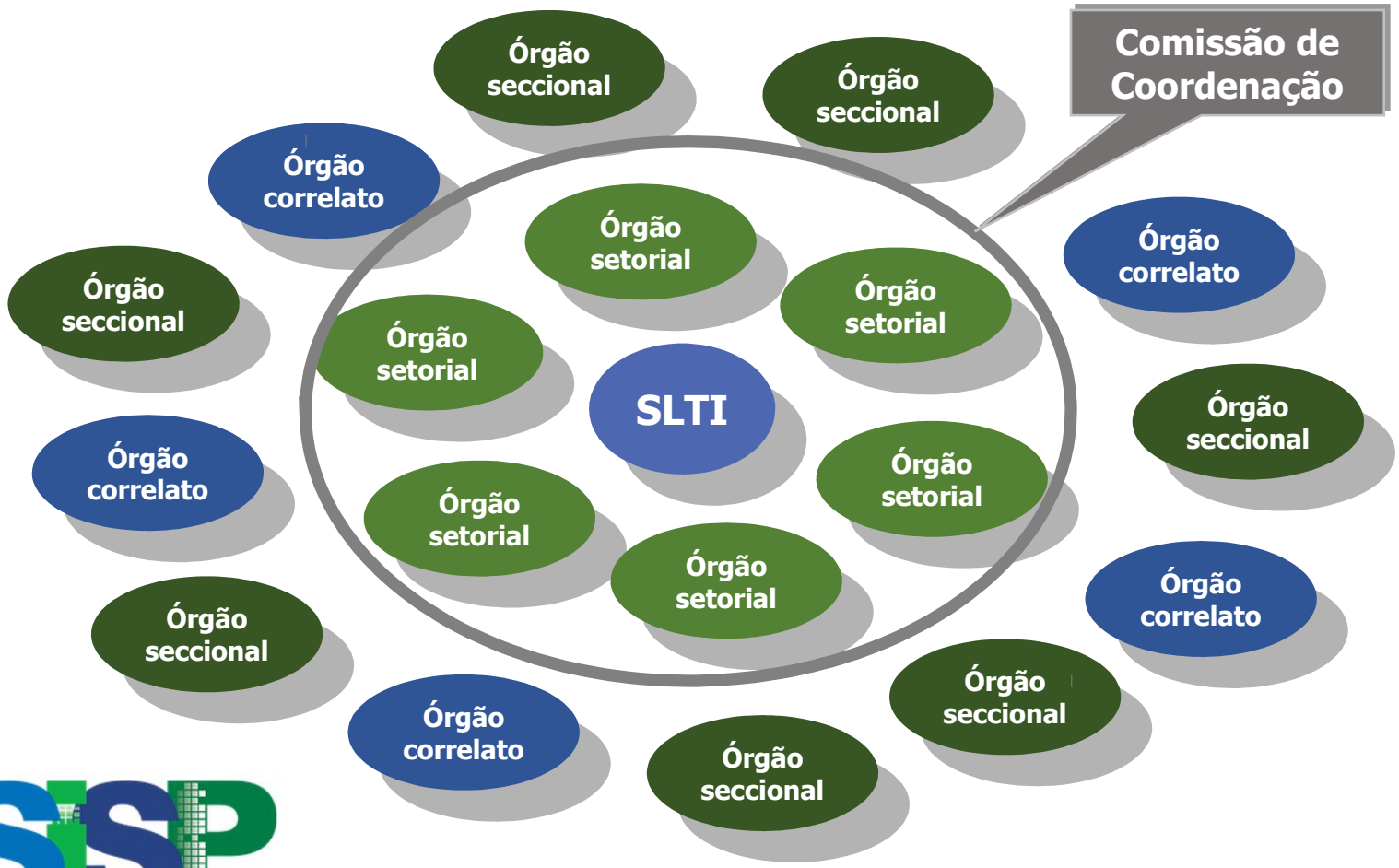
Transferências voluntárias

Sistema Integrado de Administração de Serviços Gerais – SIASG

SISP
Sistema de Administração de Recursos de Tecnologia da Informação

#Rede Siconv

Governança em rede no SISP



Sistema de Administração de Recursos de Tecnologia da Informação

Secretaria de Logística e Tecnologia da Informação

Ministério do Planejamento

GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

Eixos temáticos do SISP

Segurança cibernética

Política de Segurança da Informação (Decreto 3.505/2000)

Abrangência: órgãos e entidades da APF

Comitê Gestor da Segurança da Informação (CGSI)

Assessoramento a Secretaria-Executiva do Conselho de Defesa Nacional (CDN) na consecução das diretrizes da Política e na avaliação e análise de assuntos relativos ao Decreto

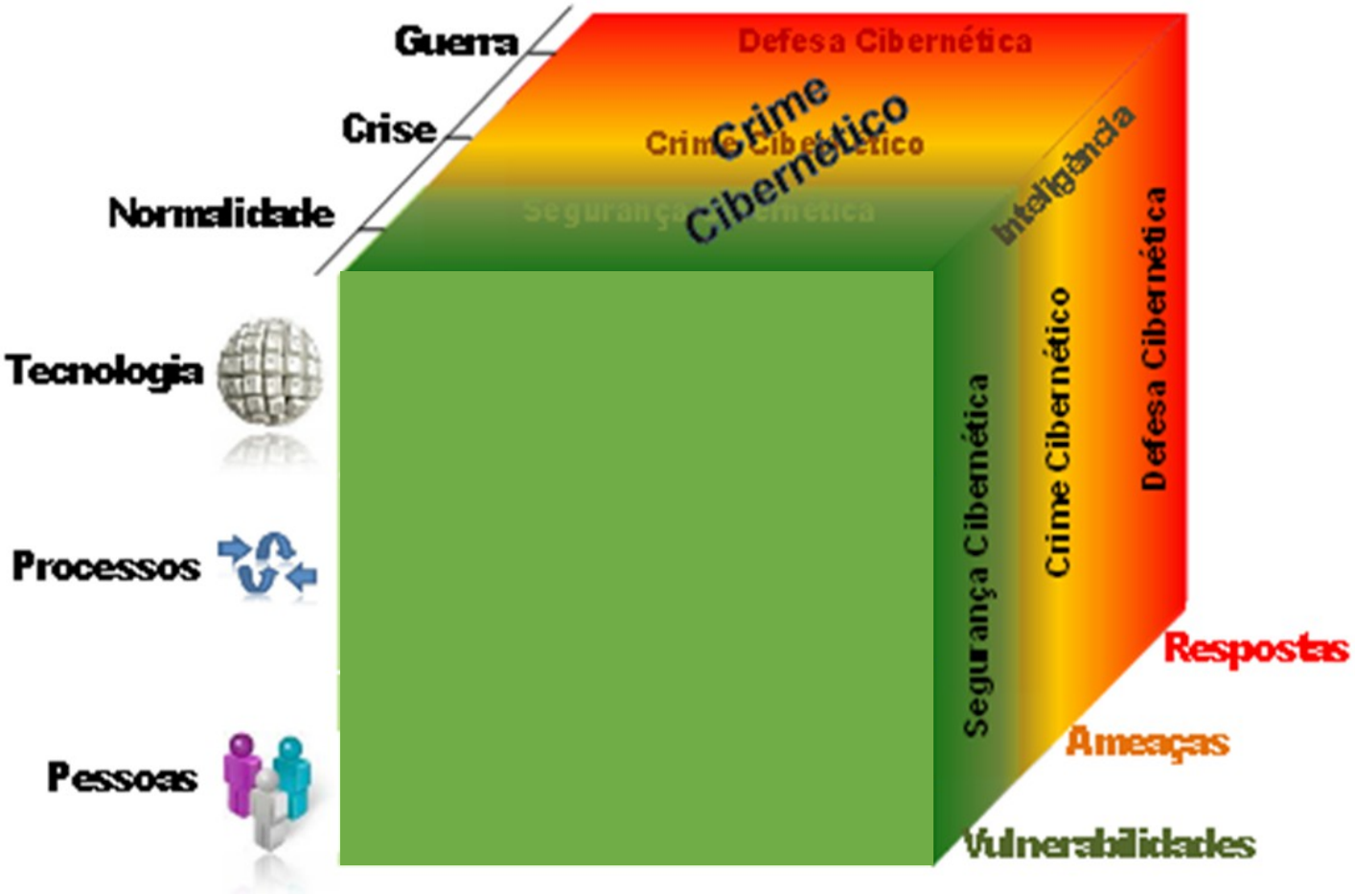
Órgão central: Gabinete de Segurança Institucional da Presidência da República (GSI/PR)

Integrantes: CC/PR; CGU; AGU; SECOM/PR; SG/PR; MJ; MD; MRE; MF; MPS; MS; MDIC; MP; MC; MCTI; MME.

Tratamento de incidentes de segurança

Estrutura descentralizada:

Eixos da Cibernética



Fonte: Departamento de Infraestrutura e Serviços de Rede – DSR/SLTI/MP, 2014

Segurança cibernética no SISP

Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética
GSI/PR

Estratégia de Governança Digital
SLTI/MP

1. **Interoperabilidade**
2. **Gerenciamento de identidades**
3. **Mapeamento de ativos de informação**
4. **Padrões de auditoria** (regulamentações do Decreto 8.135/12)
5. **Gestão de riscos**
6. **DataGov**
7. **Educação em SIC**
8. **Infovia**
9. **IPV6**
10. **Sistemas estruturantes**

Padrões de interoperabilidade
de Governo Eletrônico

Objetivos do ePING

Definir premissas, políticas e especificações técnicas que regulamentam a utilização da TICs no governo federal

Estabelece as condições de interação com os demais Poderes, esferas de governo e sociedade

Padrões de segurança alinhados à GSI

Comunicação de dados

Correio Eletrônico

Criptografia

Desenvolvimento de Sistemas

Serviços de Rede

Redes Sem Fio

Resposta a Incidentes

Auditoria em programas e equipamentos

Gerenciamento de identidades

Estudo sobre soluções de autenticação

Identificação e construção de um modelo para a APF

Aspectos analisados

Referencial teórico
Arquitetura das soluções
Níveis de segurança de autenticação
Sistemas já em operação
Autenticação biométrica

Algumas soluções pesquisadas

- ✓NAI – Núcleo de Autenticação Interbancária (DATAPREV)
- ✓Login Cidadão (Governo do Rio Grande do Sul)
- ✓GERID (DATAPREV / SERPRO)

Mapeamento e inventário
dos ativos de informação

Objetivos no SISP (NC 10/IN01/DSIC/GSIPR)

1. Prover um entendimento comum, consistente e inequívoco de seus ativos de informação
2. Identificar claramente os responsável(eis) – gestor(es) e custodiante(s)
3. Definir um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação
4. Descrever o local de cada ativo de informação
5. Identificar o valor que o ativo de informação representa para o negócio do órgão ou entidade do SISP

Padrões de auditoria
de programas e equipamentos de TIC

Decreto 8.135/2013

Dispõe sobre comunicação de dados na APF e dispensa de licitação em contratações de risco para segurança nacional

Regulamentação: Defesa, Planejamento e Comunicações

Padrões de auditoria (art. 1, §3º)

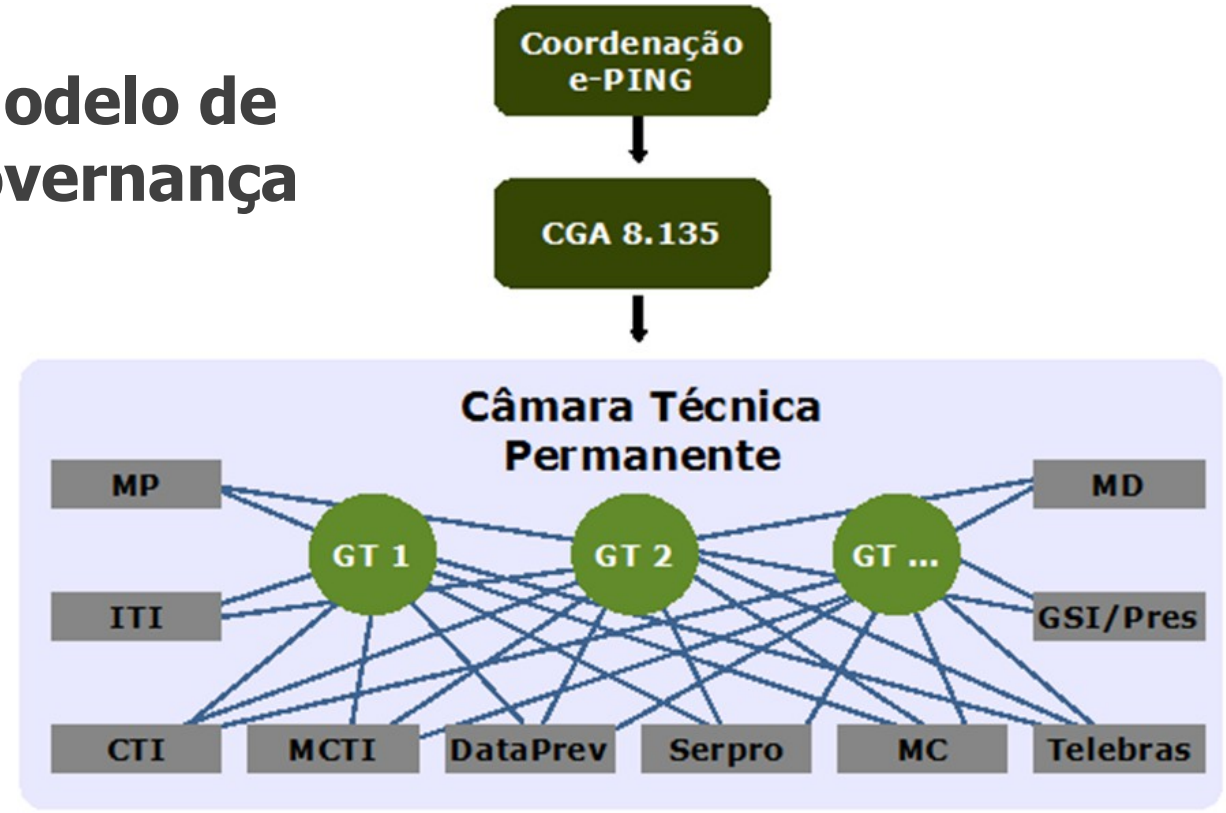
Características dos programas e equipamentos para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações

Certificação e homologação

Parceria com INMETRO e CSIC/MP

Padrões de auditoria
de programas e equipamentos de TIC

Modelo de governança



Fonte: Departamento de Infraestrutura e Serviços de Rede – DSR/SLTI/MP, 2014

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).

Ferramentas

Software público, redução de custos e interoperabilidade

Consulta Pública

Participação dos órgãos do SISP na definição da metodologia

DataGov

DataGov (1ª etapa)

Ambiente compartilhado de suporte que permite a utilização da melhor infraestrutura, tecnologia e processos de segurança possíveis, independente do tamanho, relevância ou capacidade do órgão

Benefícios diretos para a segurança da informação

- ✓ governança da segurança da informação e das infraestruturas críticas
- ✓ melhoria dos processos de segurança da informação
- ✓ taxonomia de segurança e defesa cibernética
- ✓ controle de acesso físico e lógico (gerenciamento de identidades)

Educação em SIC

Curso de Pós-Graduação em Gestão de Segurança da Informação

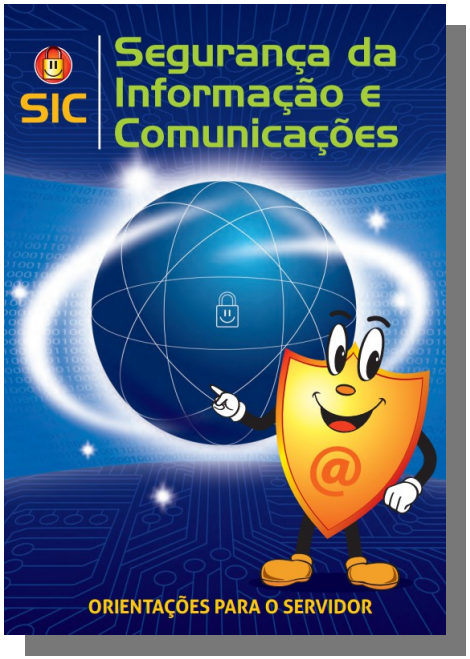
Desenvolvimento de curso em parceria com a UnB para capacitação de servidores

Cartilhas sobre SIC

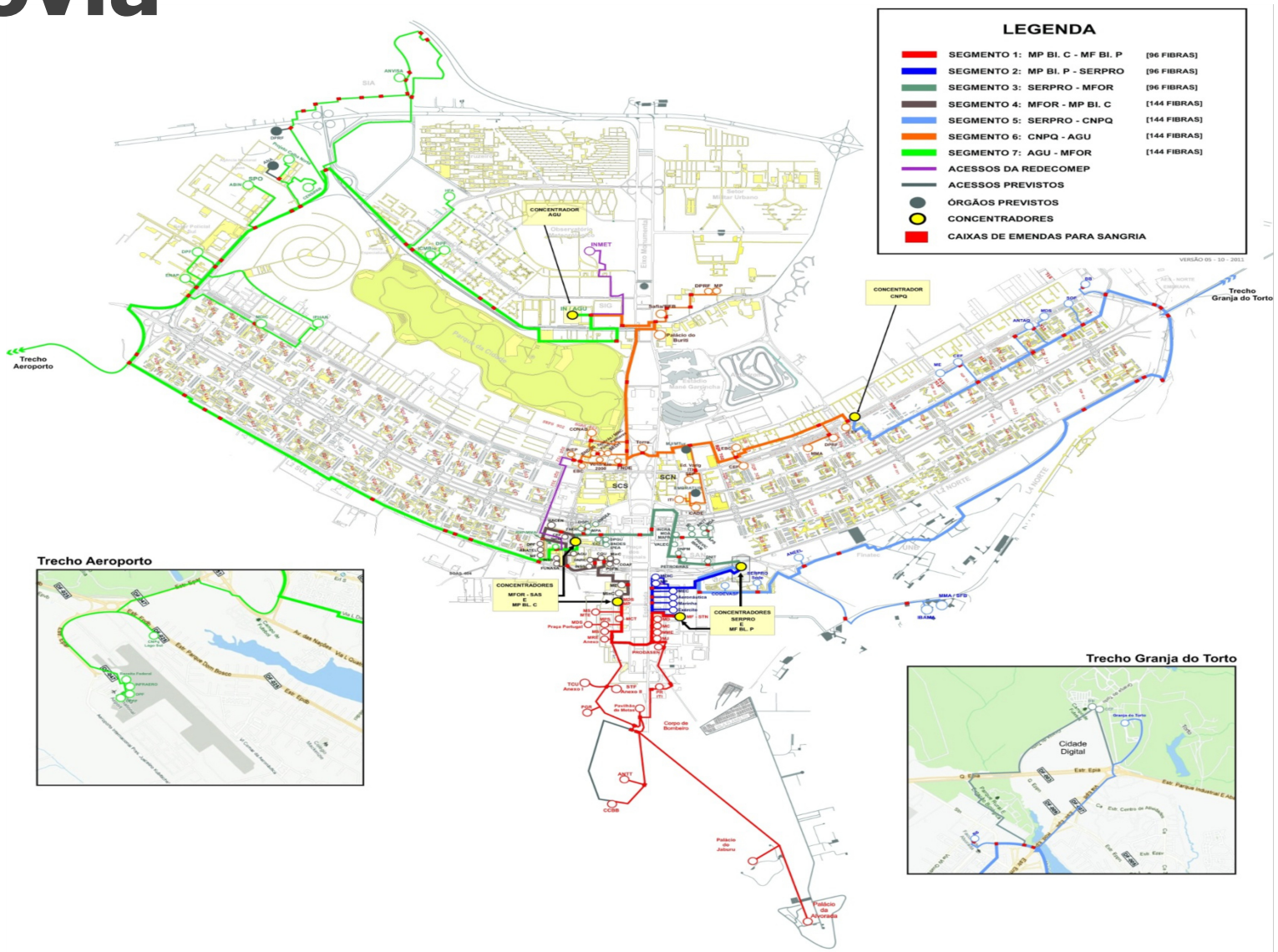
Orientação para o comportamento dos servidores em relação ao tema

Palestras para órgãos do SISP

Ministradas sob demanda por servidores da SLTI



Infovia



Secretaria de
Logística e Tecnologia da Informação

Ministério do
Planejamento

GOVERNO FEDERAL
BRASIL
PÁTRIA EDUCADORA

Infovia

Resultados no período 2011-2015

Modelo de Negócio V3 ↓ **35%** valores dos serviços

Extensão rede ↑ **167,86%** (56 → 150 Km)

Órgãos ↑ **19,23%** (78 → 91 órgãos)

Pontos de conexão ↑ **50%** (134 →201 pontos)

Banda de Internet ↑ **312%** (1,5 → 6,18 Gbps)

VoIP ↑ **24%** (25 → 31 órgãos)

Videoconferência ↑ **16,67%** (18 → 21 órgãos)

IPV6

Transição tecnológica do padrão de transmissão de dados na Internet

2010 - Plano de Ação para a Sociedade da Informação na América Latina e Caribe (meta 4)

2012 - recomendações do Comitê Gestor da Internet no Brasil

2013 - E-ping Padrões de Interoperabilidade de Governo Eletrônico

Objetivos

Superação do esgotamento de IPs

Maior eficiência na operação de redes e serviços

Endereçamento e roteamento: escalabilidade

Segurança: maior facilidade de uso do IPSec

Autoconfiguração: simplicidade na conexão de dispositivos (*plug and play*)

IPV6

Parceiros estratégicos

SERPRO, TELEBRAS e DATAPREV: transição de fora (**rede mundial** – acesso à internet, sites e portais) para dentro (**rede local** – infraestrutura, equipamentos, serviços e aplicações internos dos órgãos)

Núcleo de Informação e Coordenação do Ponto BR (NIC.br): conhecimento, capacitação e suporte

Escopo da transição: metas até 2018

Infraestrutura física

Infraestrutura lógica e dos conteúdos

Contratos de provimento de acesso à internet

Capacitação de equipes técnicas

Segurança nos sistemas estruturantes da SLTI

CAPTCHA

Após a primeira falha de login, evita acesso robotizado

Certificado digital

Possibilidade de login com certificado digital, evita o não repúdio

Controle integrado de autenticação e sessão web

Single Sign On (SSO) Picketlink gerencia uma sessão web que, caso seja expirada, força o usuário a efetuar login novamente

Controle de acessos robotizados via ativos de rede

Bloqueio de IPs e firewall

Regras de negócio (pregão eletrônico)

Minimizam o impacto da concorrência desleal entre fornecedores

Principais desafios

- ✓ Crescente dependência da gestão do Estado por recursos de TIC
- ✓ Maior demanda de informações pelos cidadãos (LAI)
- ✓ Compartilhamento de informações entre órgãos
- ✓ Padronização e interdependência entre ativos de informação
- ✓ Alta disponibilidade e armazenamento robusto de dados
- ✓ Sigilo de dados e informações e tratamento de vulnerabilidades
- ✓ Tecnologias proprietárias
- ✓ Restrições técnicas e orçamentárias
- ✓ Marcos legais
- ✓ Crescimento do crime virtual

Obrigado!

cristiano.heckert@planejamento.gov.br

(61) 2020-1400