FORUMRNP 2015
mobilidade

Auditoria de Programas e Equipamentos de Tecnologia da Informação e Comunicação (TIC)

RNP

Regulamentação do Decreto nº 8.135/2013

Onde Estamos e Onde Queremos Chegar

Anderson S. Araújo, M.Sc

Analista em TI

Ministério do Planejamento, Orçamento e Gestão

Secretaria de Logística e Tecnologia da Informação

Departamento de Infraestrutura e Serviços de Rede

Coordenação-Geral de Segurança da Informação

Contexto

- O vazamento de informações sigilosas e detalhes de programas de vigilância que países estrangeiros usam para espionar sua própria população e vários países da Europa e da América Latina, entre eles o Brasil.
- Tal vazamento, chamou ainda mais a atenção do Governo Brasileiro para questões relacionadas à Segurança da Informação e Comunicações no Brasil.

Decreto nº 8.135/2013

- 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.

- Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de TI fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

Decreto nº 8.135/2013

- § 3º Os programas e equipamentos destinados às atividades de que trata o caput **deverão ter características que permitam auditoria** para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações.
- Portaria define serviços de TI: correio eletrônico, compartilhamento e sincronização de arquivos, mensageria instantânea, conferência, e comunicação de voz sobre protocolo de internet (VoIP).
- Não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.
- A contratação não será obrigatória:
  - casos em que não houver oferta;
  - comunicações de dados militares operacionais e seus sistemas de TI;
  - redes próprias e serviços de TI próprios adequados a Portaria;
  - serviços de redes fora do território nacional; e
  - serviços prestados pela RNP, desde que compatíveis com o contrato de gestão da instituição.

Resultados Até o Momento

- Criação de Grupo de Trabalho (GT) Interministerial para regulamentar o Decreto.
- Publicação da **Portaria Interministerial nº 141/2014**, regulamentando parte do Decreto.
- Encerramento dos trabalhos do GT com a publicação dos documentos:
  - Conjunto de Características, Critérios, Condições Mínimas e Medidas para Auditoria de Segurança da Informação em Programas e Equipamentos;
  - Cronograma para Implantação dos Critérios; e
  - Modelo de Governança e Gestão de Auditoria de Segurança da Informação em Programas e Equipamentos.

Resultados Até o Momento

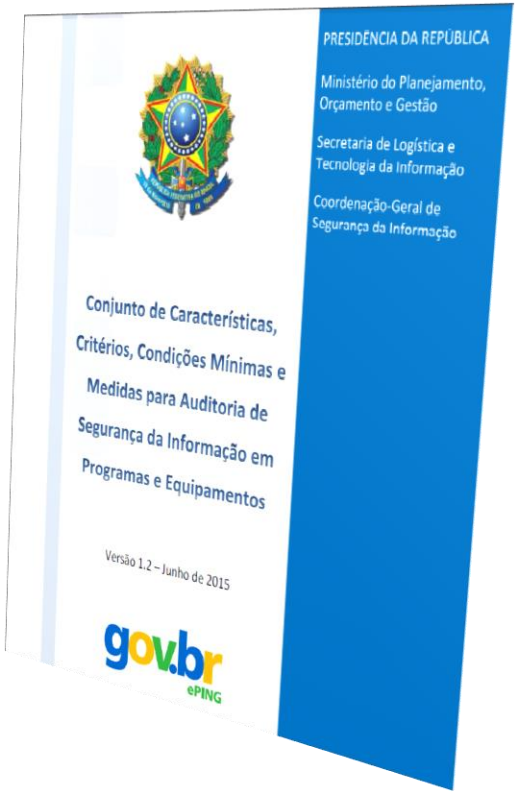
- Publicação da Portaria SLTI/MP nº 2/2015, que institui o Grupo de Trabalho Permanente (**GT-Auditoria**), vinculado ao Segmento de Segurança dos Padrões de Interoperabilidade do Governo Eletrônico – **ePING**, para:
  - produzir o refinamento dos documentos publicados pelo GT de regulamentação do Decreto nº 8135/2013;
  - consolidar um modelo de rede de colaboração envolvendo institutos de pesquisa, acadêmicos, órgãos e entidades da APF para dar suporte na operação e na continuidade dos processos de auditoria; e
  - prospectar, propor e coordenar inciativas para garantir que os programas e equipamentos destinados às atividades relacionadas possuam características que permitam auditoria (DICA).

Resultados Até o Momento

- **Portaria Interministerial nº 141/2014**
  - Regulamentação de parte do Decreto nº 8.135/2013.
  - Elaborada por grupos técnicos representativos: MP, MC e MD, SERPRO, DATAPREV e TELEBRÁS.
  - Ouvidos representantes: RNP, BACEN, GSI/PR e MRE, além do CTI/MCTI.
  - Aprovada pelas Secretarias Executivas do MP, MC e MD.
- Apresentada à direção do SERPRO, DATAPREV, TELEBRÁS, RNP e à Casa Civil para fins de alinhamento estratégico com objetivos do Decreto nº 8.135/2013.

Resultados Até o Momento

- **Documentos Publicados pelo GT de Regulamentação do Decreto nº 8.135/2013**
  - Conjunto de Características, Critérios, Condições Mínimas e Medidas para Auditoria de Segurança da Informação em Programas e Equipamentos.
  - Cronograma para Implantação dos Critérios de Auditoria de Segurança da Informação em Programas e Equipamentos.

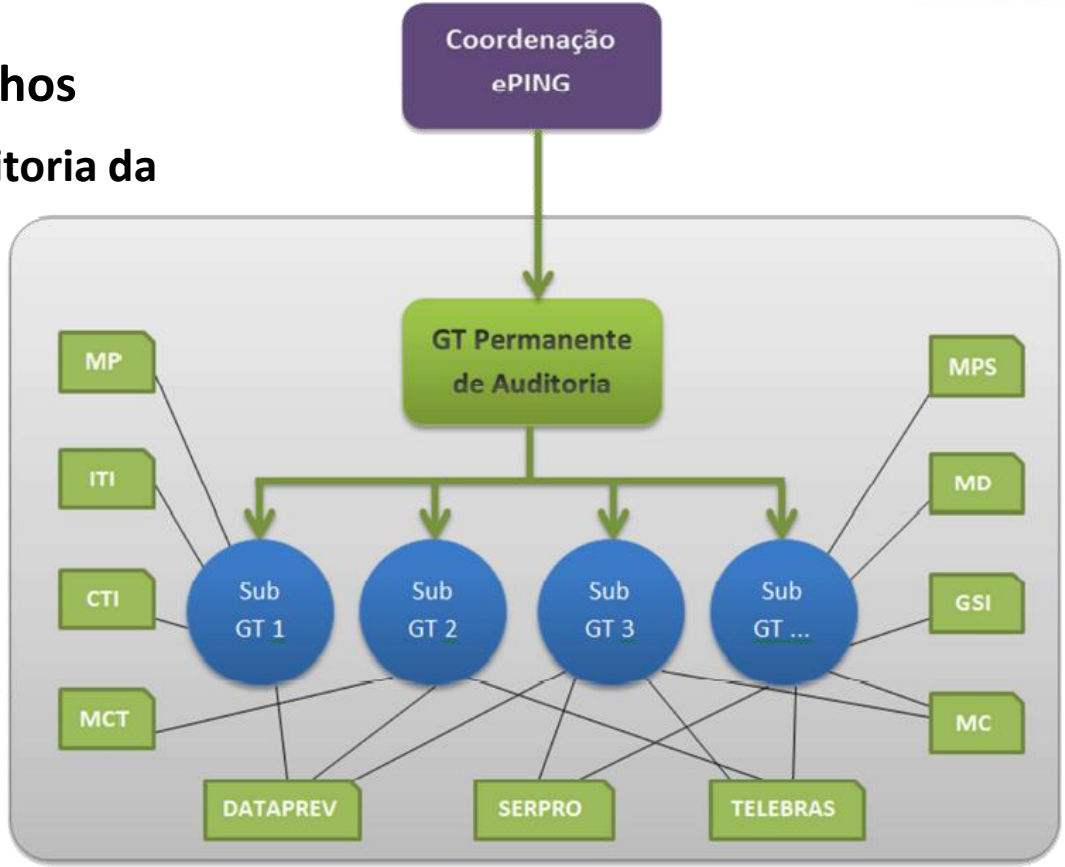


Resultados Até o Momento

- **Documentos Publicados pelo GT de Regulamentação do Decreto nº 8.135/2013**
  - Modelo de Governança e Gestão de Auditoria de Segurança da Informação em Programas e Equipamentos
- OBS: As regras de auditoria se aplicam tanto para as contratações padronizadas quanto para contratações de empresas privadas.

Estado Atual dos Trabalhos

- **GT Permanente de Auditoria da ePING**



Estado Atual dos Trabalhos

- **Subgrupo de Trabalho Temporário: Correio Eletrônico**
  - Estrutura do Anexo (*template*) aprovada.
  - Em fase de preenchimento da especificação dos critérios de auditoria.
  - Previsão de conclusão: dezembro de 2015.
- **Subgrupo de Trabalho Temporário: Certificação e Homologação**
- Em fase de formação.
- Enviado ofício ao INMETRO para viabilizar acordo de cooperação com o MP.
- Solicitação de indicação por parte do MP aos órgãos correlatos.
  - MD (Comandos Militares), CDCiber, MCTI (CTI), SERPRO, DATAPREV, ANATEL, INMETRO, Telebras, ITI, RNP, GSI/PR

Impacto Para a Administração Pública

- Contratação dos Serviços de Rede e TI
  - Serviços padronizados a partir dos planos de disponibilidade → junto às empresas estatais (dispensa);
  - Serviços com parâmetros não padronizados → empresas estatais serão consultadas sobre a disponibilidade (dispensa);
  - Serviços não padronizados e negativa das empresas estatais → empresas privadas (licitação).
- Para serviços padronizados, compete ao órgão gerenciador (MP):
  - regulamentar as contratações previstas (publicação de IN);
  - verificação do atendimento da regulamentação específica do serviço; e
  - revisar periodicamente os preços estabelecidos.

Impacto Para a Administração Pública

- Termo de Referência ou Projeto Básico deverá prever:
  - características que permitam auditoria de programas e equipamentos, pelo órgão ou entidade contratante ou por instituição credenciada pelo Governo Federal; e
  - detalhamento dos critérios e condições mínimas de segurança.

- Diretrizes e especificações técnicas, para auditoria de programas e equipamentos, serão definidas em capítulo específico dos Padrões de Interoperabilidade de Governo Eletrônico (ePING).
  - http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/auditoria-em-programas-e-equipamentos

Visão de Futuro

- Aumento da importância do espaço cibernético e da governança digital nas funções do Estado Brasileiro.
- Criação de um sistema de “auditoria” de segurança da informação em programas e equipamentos.
- De forma análoga, o Centro de Defesa Cibernética (CDCiber) está desenvolvendo o Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética (SHCDCiber).
- Finalizar o preenchimento de todos os Anexos que compõem o Conjunto de Características, Critérios, Condições Mínimas e Medidas para Auditoria de Segurança da Informação em Programas e Equipamentos.
- Estes formarão a Base Normativa para a implantação do PBCerTI.

Visão de Futuro

- Uso do arcabouço provido pelo Sistema Nacional de Metrologia, Normatização e Qualidade Industrial (SINMETRO) e do padrão internacional de avaliação de conformidade de segurança em tecnologia da informação, "*Common Criteria for Information Technology Security Evaluation*".
- O Estado Brasileiro deve integrar os sistemas!

gov.br e-PING

e-PING
Padrões de Interoperabilidade de Governo Eletrônico

RNP Ministério da Cultura Ministério da Saúde Ministério da Educação Ministério da Ciência, Tecnologia e Inovação GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

FORUM RNP 2015 mobilidade

Anderson S. Araújo

br.linkedin.com/in/asaraujo
eping@planejamento.gov.br
dsr@planejamento.gov.br