

Ata da Audiência Pública nº 1/2015

Às 14 horas e 20 minutos do dia 12 do mês março do ano de 2015, tendo por local o Auditório Térreo do bloco K, na Esplanada dos Ministérios - Brasília, foi realizada audiência pública convocada pela Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão – SLTI-MP, com a finalidade de debater as contribuições referentes aos documentos relativos a auditoria em programas e equipamentos para serviços de tecnologia da informação, conforme disposto no Decreto 8.135/2013. Estiveram presentes na audiência pública 74 cidadãos, conforme a lista de presença anexa.

O sr. Cristiano Heckert, secretário da SLTI, iniciou a audiência dando um panorama do evento e colocando a SLTI aberta à participação social.

Em seguida, o Secretário passou a palavra para o sr. Leonardo Boselli, diretor do Departamento de Serviços de Rede, da SLTI, que explicou a dinâmica da audiência e fez uma apresentação sobre o Decreto nº 8135/13, a Portaria Interministerial nº 141/14 e a estruturação dos documentos Modelo de Gestão de Auditoria e Critérios de Auditoria de Segurança, elaborados pelo Grupo de Trabalho de Auditoria (GT Auditoria) e que estiveram em consulta pública no final de 2014.

A palavra foi passada para a sra. Ana Paula Mello, analista em TI da SLTI, que apresentou a arquitetura ePING e a relação dos trabalhos do GT Auditoria com a arquitetura.

Na sequência foi composta a mesa com representantes do GT Auditoria e o sr. Carlos Machado apresentou os documentos Modelo de Gestão de Auditoria e Critérios de Auditoria de Segurança.

Após a apresentação foi aberto espaço para contribuições pelos presentes e solicitado que as mesmas fossem formalizadas pelo e-mail eping@planejamento.gov.br.

A mesa informou que as respostas às contribuições seriam dadas a cada 3 contribuições.

O sr. Alessandro, da Microsoft, questionou qual a data limite para envio das contribuições, e a possibilidade de um maior alinhamento com o Common Criteria.

A mesa informou que o prazo para envio das contribuições será de 1 mês.

O sr. Roberto Gallo, da ABIMDE, sugeriu estabelecer um modelo de governança que atenda tanto a esfera civil quanto a militar. Este modelo deveria estar vinculado ao SINMETRO.

O sr. Giuseppe, da CISCO, colocou que o trabalho desenvolvido até o momento é fundamental, mas deveria estar embaixo de um framework de segurança e que o país poderia considerar o uso do Common Criteria.

Uma dúvida colocada pelo sr. Giuseppe é de como será gerenciado o código fonte que for aberto e qual a frequência de conferência dos códigos.

A mesa informou que o catálogo de componentes do Common Criteria foi usado como referência para os documentos e que o uso e alinhamento com o Common Criteria será consequência dos trabalhos da ePING, mas que o governo não abrirá mão de manter o controle sobre as auditorias.

Quanto a guarda dos códigos fontes, a mesa informou que ainda não foi avaliado pelo Grupo de Trabalho como será feito, mas que o Instituto Nacional de Tecnologia da

Informação - ITI participa do GT e trará para as discussões todo o conhecimento do órgão sobre guarda de código fonte.

Também foi informado pela mesa que é possível trabalhar com o SINMETRO, mas que o objetivo neste momento é definir a governança.

A mesa explicou que as tecnologias envolvidas nos trabalhos de auditoria atendem as esferas civil e militar, e que será desenhado um modelo nacional de certificação.

O sr. Ricardo, da Embrapa, questionou como ficam as empresas da administração pública indireta, pois estão fora do escopo da Portaria Interministerial nº 141/14.

O sr. Alessandro, da Microsoft, comentou que o Common Criteria é descentralizado, podendo atender ao governo brasileiro, mantendo a evolução do padrão.

A mesa informou que aos normativos estarão em constante evolução, tendendo a abranger todas as empresas públicas e que o Decreto 8135/13 obriga a Administração Pública Federal, mas não exclui os demais órgãos.

O sr. Pedro, do ITI, informou que o ITI criou um modelo de certificação alinhado as normas internacionais, adicionando algumas necessidades da ICP-Brasil, o que também poderia ser feito no caso do Common Criteria, e lembrou que o Brasil tem assento na ISO, podendo levar seus interesses para as discussões da ISO/IEC 15408 (Common Criteria).

Foi feito um intervalo de 10 minutos e no retorno a palavra foi passada para o CTI (Centro de Tecnologia da Informação Renato Archer), que participou do evento de forma remota.

Paulo Bueno do CTI reforçou a importância do alinhamento dos trabalhos do GT com o Common Criteria e informou que a elaboração de *Protection Profiles* ainda será tratada pelo grupo, assim como a metodologia de avaliação da criticidade dos produtos.

O sr. Machado colocou que nem todo sistema ou equipamento precisará abrir código, pois depende da criticidade e que essas discussões de segurança também são feitas em outros países, não sendo exclusividade do Brasil.

O sr. Deivi Kuhn solicitou mais uma vez que as contribuições fossem formalizadas pelo e-mail da ePING e informou que foram recebidas poucas contribuições ao texto durante a consulta pública.

Não tendo mais nenhuma contribuição pelos presentes, a audiência pública foi encerrada às 17 horas.