



PRESIDÊNCIA DA REPÚBLICA  
CASA CIVIL  
INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA  
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

## **REUNIÃO DA COMISSÃO TÉCNICA EXECUTIVA - COTEC**

**DATA: 24 DE NOVEMBRO DE 2015**

**HORÁRIO: 14h30 às 18h**

**LOCAL: SALA DE REUNIÕES DO TÉRREO – ITI**

### **APRESENTAÇÃO DOS GRUPOS DE TRABALHO DA COTEC**

#### **GRUPO 1 - RUY CÉSAR RAMOS FILHO (Responsável)**

##### **PAUTA:**

1. Proposta de regulamentação de certificado tipo “*mobile*”;
2. Redução do escopo de aplicação para certificados do tipo A1;
3. Fim dos certificados do tipo A2;
4. Proposta de reformulação dos certificados de sigilo “S”;
5. Proposta de regulamentação de certificado tipo “*IoT*” (Internet das Coisas);

#### **GRUPO 2 – ANDRÉ MACHADO CARICATTI (Responsável)**

##### **PAUTA:**

7. Estudos com vistas à adoção de novos algoritmos criptográficos de curvas elípticas, de resumos criptográficos (hashes) e de especificações e padrões para “*middlewares*” multiplataforma para hardwares criptográficos (SmartCards e Tokens);

#### **GRUPO 3 – JOSÉ RODRIGUES GONÇALVES JUNIOR (Responsável)**

##### **PAUTA:**

8. Proposta de ajuste na redação que trata do prazo para revogação de certificado de AC de 1º nível pela AC Raiz (DOC-ICP-01 item 4.4.3.3). Prazo máximo para situações críticas somente;
9. Proposta de regulamentação de prazo diferenciado para LCRs de certificados da AC Raiz revogados. Ideia de que o prazo da LCR após a revogação seja até a data de vencimento/expiração do certificado revogado (DOC-ICP-01 item 4.4.9). Avaliar pertinência de regulação com o mesmo objetivo para o caso das raízes vigentes, porém, sem certificados de usuário finais vigentes (V1 em breve V2);
10. Proposta para retirar campo AIA da LCR;
11. Proposta de obrigatoriedade do uso de OCSP para ACs que emitem certificados para usuários finais;
12. Proposta de fim do 3º repositório de LCRs na AC-Raiz;

#### **GRUPO 4 – RUY CÉSAR RAMOS FILHO (Responsável)**

##### **PAUTA:**

13. Proposta de tornar obrigatória a inserção diretamente pelas ACs de seus certificados de AC no programa da Fundação Mozilla;

14. Propor obrigatoriedade para as ACs emissoras de certificados SSL, habilitação do CAB Fórum para emissão de certificados ICP-Brasil, SSL-EV;

#### **GRUPO 5 – WILSON ROBERTO HIRATA (Responsável)**

##### **PAUTA:**

6. Proposta de regulamentação de prestador de serviço de assinatura digital remota;

16. Propor regulação de Portais de Assinatura;

#### **GRUPO 6 – Dr. ANDRÉ PINTO GARCIA (Responsável)**

##### **PAUTA:**

15. Plano de contingenciamento encerramento de Acs;

17. Regulamentar o credenciamento de AR no exterior.