

RESOLUÇÃO Nº 68, DE 13 DE OUTUBRO DE 2009.

ALTERA OS PRAZOS ESPECIFICADOS NO PLANO DE ADOÇÃO DE NOVOS PADRÕES CRIPTOGRÁFICOS ANEXO II DA RESOLUÇÃO Nº 65, PUBLICADA EM 09 DE JUNHO DE 2009

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – CG ICP-BRASIL, no exercício do cargo de Coordenador do referido Comitê, no uso das atribuições legais previstas nos incisos I, V e VI do art. 4º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

CONSIDERANDO o Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG ICP-Brasil e fixa a competência, prevista em seu § 6º art. 2º, do Secretário Executivo para coordená-lo na hipótese de ausência do Coordenador titular e seu suplente; e

CONSIDERANDO a necessidade de extensão do prazo para a implantação dos novos padrões de algoritmos criptográficos da ICP-Brasil;

RESOLVE:

Art. 1º. O Anexo II da RESOLUÇÃO Nº 65, que contém o plano de migração, passa a vigorar com a seguinte redação:

ANEXO II

PLANO DE ADOÇÃO DE NOVOS PADRÕES CRIPTOGRÁFICOS

1. Primeira etapa – data limite: 09.12.2009

- 1.1 Alterar os normativos da ICP-Brasil para permitir a emissão de certificados para AC e usuários finais contendo chaves ECC. Permitir que esses certificados usem também função *hash* SHA 256 ou SHA 512 para realização de assinaturas. O objetivo dessa ação é permitir que o mercado comece a se adaptar aos novos padrões.
- 1.2 Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

2. Segunda etapa – data limite: 30.06.2010

- 2.1 Criar, na AC Raiz, nova cadeia (V2), que implemente padrão RSA 4096 bits e função *hash* SHA 512.
- 2.2 Criar na AC Raiz, nova cadeia (V3) que implemente padrão ECDSA 512 bits e função *hash* SHA 512.
- 2.3 Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

3. Terceira etapa – data limite: 31.12.2010

- 3.1 Avaliar a adesão dos sistemas de mercado e de AC, à adoção de esquemas criptográficos mais seguros e se necessário, adotar ações para ampliação do uso.
- 3.2 A partir de 01.07.2010, as AC devem adotar as ações necessárias ao início do processo de emissão de certificados vinculados à AC Raiz sob a nova hierarquia (V2 ou V3), e adaptar seus sistemas para uso dos novos padrões.
- 3.3 Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

4. Quarta etapa – data limite: 01.01.2011

- 4.1 A partir desta data é recomendado criar certificados que usem pelo menos padrão RSA 2048 bits e função *hash* SHA 256.

5. Quinta etapa – data limite: 31.12.2011

- 5.1 A partir desta data, todas as AC já devem estar emitindo certificados vinculados à AC Raiz sob a nova hierarquia (V2 e V3), adaptando seus sistemas para o uso dos novos padrões.
- 5.2 Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

6. Sexta etapa – data limite: 01.01.2012

- 6.1 A partir desta data, nenhum novo certificado de AC ou de usuários finais poderá ser gerado sob as hierarquias anteriores (V0 e V1).
- 6.2 Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

7. Sétima etapa – data limite: 31.12.2014

- 7.1 A partir desta data, nenhum certificado ICP-Brasil emitido sob as cadeias anteriores (V0 e V1) deverá estar válido, exceto certificados de AC, cuja revogação deve ser avaliada.

Art. 2º Todas as demais cláusulas da RESOLUÇÃO Nº 65, em sua ordem originária mantêm-se válidas.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

MAURÍCIO AUGUSTO COELHO