RESOLUÇÃO Nº 94, DE 27 DE SETEMBRO DE 2012.

APROVA A VERSÃO 4.2 DO DOCUMENTO DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL(DOC-ICP-01).

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL, no exercício do cargo de Coordenador do referido Comitê, no uso das atribuições legais previstas nos incisos I, III, V e VI do art. 4° da Medida Provisória n° 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 no § 6º art. 2º, do Secretário Executivo para coordená-lo na hipótese de ausência do Coordenador titular e suplente;

CONSIDERANDO a necessidade de detalhamento dos perfis de certificados digitais de AC de nível subsequente ao da AC Raiz;

CONSIDERANDO a alteração de endereço da Sede do ITI e da substituição do Prestador de Serviços de Suporte para a AC Raiz; e

CONSIDERANDO o fortalecimento e robustez dos algoritmos implementados no âmbito da ICP-Brasil, com a recente atualização dos padrões e algoritmos criptográficos;

RESOLVE:

Art. 1º Altera-se o item 1.3.3 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

A AC Raiz mantém acordo com a Universidade Federal de Santa Catarina (UFSC) como prestador de serviços de suporte para disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

Art. 2º Alteram-se os campos “Endereço” e “E-mail” do item 1.4 do DOC-ICP-01, versão 4.1, que passam a vigorar com as seguintes redações:

Endereço: SCN, Quadra 2, Bloco E, CEP 70712-905 – Brasília-DF
E-mail: contato@iti.gov.br

Art. 3º Altera-se o item 7.2 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

O formato de todos os certificados emitidos pela AC Raiz está em conformidade com o padrão ITU X.509 ou ISO/IEC 9594. O certificado da AC de nível subsequente ao da AC Raiz é assinado pela AC Raiz, e possui validade limitada à validade do certificado

da AC Raiz, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

Art. 4º Altera-se o item 7.2.2 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

7.2.2.1. O certificado da AC de nível imediatamente subsequente ao da AC Raiz pode implementar quaisquer das extensões previstas na versão 3 do padrão ITU X.509.
7.2.2.2. As seguintes extensões são obrigatórias:

a) "***Authority Key Identifier*", não crítica**: o campo keyIdentifier deve conter o *hash*, obtido com algoritmo da família SHA, da chave pública da AC que emite o certificado;
b) "***Subject Key Identifier*", não crítica**: deve conter o *hash*, obtido com algoritmo da família SHA, da chave pública da AC titular do certificado;
c) "***Key Usage*", crítica**: somente os bits keyCertSign e cRLSign devem estar ativados;
d) "***Certificate Policies*", não crítica**:

d.1) o campo policyIdentifier deve conter:

i. se a AC emite certificados para outras ACs, o OID da DPC da AC titular do certificado; ou
ii. se a AC emite certificados para usuários finais, os OID das PCs implementadas, contendo o campo **policyQualifiers** com o atributo id-qt-cps e o endereço *Web* da DPC da AC;

e) "***Basic Constraints*", crítica**: deve conter o campo cA=*True*; e
f) "***CRL Distribution Points***", **não crítica**: deve conter endereço na *Web* onde se obtém a LCR correspondente ao certificado, conforme item 7.1.2.c.

Art. 5º Altera-se o item 7.2.6 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

Conforme disposto no item 7.2.2.2 d.

Art. 6º Altera-se o item 7.2.7 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

Se a AC emite certificados para usuários finais a extensão "*Policy Constraints*" poderá ser utilizada na forma definida pela RFC 5280.

Art. 7º Altera-se o item 7.2.8 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

7.2.8.1. Em certificados de AC que emitem certificado para usuário final, o campo policyQualifiers da extensão "Certificate Policies" deverá conter o endereço web (URL) da DPC da AC, conforme disposto no item 7.2.2.2.d.ii.
7.2.8.2. Para as demais ACs, não se aplica.

Art. 8º Altera-se o item 7.2.9 do DOC-ICP-01, versão 4.1, que passa a vigorar com a seguinte redação:

Se a AC emite certificados para usuários finais, extensões críticas devem ser interpretadas conforme a RFC 5280.

Art. 9º Fica aprovada a versão 4.2 do Documento DECLARAÇÃO DE PRÁTICAS DE

CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL (DOC-ICP-01).

§ 1º Todas as demais cláusulas do DOC-ICP-01, na sua versão 4.1, em sua ordem originária, integram a presente versão 4.2 e mantêm-se válidas.

§ 2º O documento referido no caput encontra-se disponibilizado, em sua totalidade, no sítio http://www.iti.gov.br.

Art. 10. Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI