

RESOLUÇÃO Nº 91, DE 05 DE JULHO DE 2012

APROVA A VERSÃO 5.0 DO DOCUMENTO REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04).

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, III, 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 Infraestrutura 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;

CONSIDERANDO a deliberação da reunião do Comitê Gestor da ICP-Brasil, ocorrida em 05.07.2012;

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

CONSIDERANDO a necessidade de clarificar questões relativas à formatação de campos e nos tamanhos de chaves;

RESOLVE:

Art. 1º Alteram-se a Tabelas do item 6.3.2.3 e do Anexo I, do DOC-ICP-04, versão 4.0, que passam a vigorar com os seguintes conteúdos:

Tabela 6-Períodos de Validade dos Certificados:

<i>Tipo de Certificado</i>	<i>Período Máximo de Validade do Certificado (em anos)</i>
A1 e S1	1
A2 e S2	2
A3, S3, T3	5
A4, S4, T4	6

ANEXO I-Tabela Comparativa de Requisitos Mínimos por Tipo de Certificado:

Tipo de Certificado	Chave Criptográfica			Validade máxima do certificado (anos)	Frequência de emissão de LCR (horas)	Tempo limite para revogação (horas)
	Tamanho (bits)	Processo de Geração	Mídia Armazenadora			
A1 e S1	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Software	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma do item 6.1.1	1	6	12
A2 e S2	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Software	Cartão Inteligente ou <i>Token</i> , ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica	2	6	12
A3 e S3	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Hardware	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou <i>hardware</i> criptográfico homologado junto à ICP-Brasil	5	6	12
T3	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Hardware	<i>Hardware</i> criptográfico homologado junto à ICP-Brasil	5	6	12
A4 e S4	RSA 2048 (V0 e V1), 4096 (V2) ECDSA 512	Hardware	<i>Hardware</i> criptográfico homologado junto à ICP-Brasil	6	6	12
T4	RSA 2048 (V0 e V1), 4096 (V2) ECDSA 512	Hardware	<i>Hardware</i> criptográfico homologado junto à ICP-Brasil	6	6	12

Art. 2º Alteram-se as alíneas “iii” do subitem “b” e “ii” do subitem “c”, constantes no item 7.1.2.3 do DOC-ICP-04, versão 4.0, que passam a vigorar com a seguinte redação:

OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;

Art. 3º Fica aprovada a versão 5.0 do Documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04).

§ 1º Todas as demais cláusulas do DOC-ICP-04, na sua versão 4.0, em sua ordem originária, integram a presente versão 5.0 e mantêm-se válidas.

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

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI