RESOLUÇÃO Nº 123, DE 06 DE JULHO DE 2017.

ATUALIZA OS PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL, OS REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL E OS PROCEDIMENTOS PARA GERENCIAMENTO DA CHAVE SIMÉTRICA PARA GERAÇÃO DO IDN.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6º, §1º, inc. III, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4°, da Medida Provisória n° 2.200-2, de 24 de agosto de 2001, em reunião extraordinária realizada em 06 de julho de 2017,

CONSIDERANDO a implementação de programa de avaliação de conformidade (PAC) no âmbito do INMETRO para equipamentos de certificação digital ICP-Brasil;

CONSIDERANDO que a homologação destes equipamentos na ICP-Brasil trata-se de mero procedimento administrativo,

RESOLVEU:

Art. 1º Alterar o item 3 do DOC-ICP-01.01, versão 3.1, que passa a vigorar com a seguinte redação:

A tabela a seguir relaciona os padrões mínimos a serem empregados nos hardware criptográficos com sua utilização na ICP-Brasil e com os documentos normativos que tratam dessa utilização.

Utilização	Padrões Obrigatórios	Normativo
Módulo criptográfico de geração de chaves assimétricas de usuário final	Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-04 item 6.2.1 DOC-ICP-05 item 6.2.1.2
Módulo criptográfico para armazenamento da chave privada de titular do certificado	Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-04 item 6.8
Parâmetros de geração de chaves assimétricas de usuário final	Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-04 item 6.1.6
Módulo criptográfico de geração de chaves assimétricas de AC	Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-05 item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-05 item 6.8
Parâmetros de geração de chaves assimétricas de AC	Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-05 item 6.1.6

Utilização	Padrões Obrigatórios	Normativo
Módulo criptográfico de geração de chaves Assimétricas da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.2.1
Módulo criptográfico para armazenamento da chave privada da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.1.6
Processo para verificação de parâmetros de geração de chaves assimétricas da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.1.7 DOC-ICP-04 item 6.1.7 DOC-ICP-05 item 6.1.7

Art. 2º Alterar a Tabela 4 do item 6.1.1 do DOC-ICP-04, versão 6.1, que passa a vigorar com a seguinte redação:

Tabela 4 – Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A1 e S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima
A2 e S2	Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica
A3 e S3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A4 e S4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
T3 e T4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A CF-e-SAT	Hardware criptográfico.

Nota: para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação ou certificação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê-Gestor da ICP-Brasil.

Art. 3º Alterar a Tabela Comparativa de Requisitos Mínimos por Tipo de Certificado, do Anexo I do DOC-ICP-04, versão 6.1, que passa a vigorar com a seguinte redação:

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 Token, 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	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.	5	6	12
T3	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Hardware	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.	5	6	12
A4 e S4	RSA 2048 (V0 e V1), 4096 (V2)	Hardware	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.	6	6	12
	ECDSA 512	Hardware	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.	11	6	12
T4	RSA 2048 (V0 e V1), 4096 (V2)	Hardware	Hardware criptográfico,homologado junto à ICP-Brasil ou com certificação INMETRO.	6	6	12

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			
	ECDSA 512	Hardware	Hardware criptográfico,homologado junto à ICP-Brasil ou com certificação INMETRO.	11	6	12
A CF-e-SAT	RSA 2048	Hardware	Hardware criptográfico	5	6	12

Nota: Para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação ou certificação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê-Gestor da ICP-Brasil.

Art. 4º Alterar o item 1.2.3 do DOC-ICP-05.04, versão 2.0, que passa a vigorar com a seguinte redação:

1.2.3 Importação da Chave Criptográfica Simétrica pela Entidade

A cópia da chave criptográfica simétrica gerada será importada em MSC homologado ou com certificação INMETRO, pertencente à entidade, seguindo formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

A importação da chave criptográfica simétrica será feita na presença de um representante legalmente constituído da entidade, acompanhado por representante da AC Raiz, em cerimônia específica, com data e hora previamente estabelecidas.

Para fins de auditoria, essa cerimônia deverá produzir evidências que a chave criptográfica importada não poderá ser exportada. Caberá ainda ao representante legal da entidade assinar termo específico de importação de chave criptográfica produzida na AC Raiz da ICP-Brasil.

Art. 5º Ficam aprovadas as novas versões dos Documentos: DOC-ICP-01.01 - PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (versão 3.2), DOC-ICP-04 - REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (versão 6.2) e DOC-ICP-05.04 - PROCEDIMENTOS PARA GERENCIAMENTO DA CHAVE SIMÉTRICA PARA GERAÇÃO DO IDN (versão 2.1).

§ 1º As demais cláusulas dos referidos documentos, nas suas versões imediatamente anteriores, em sua ordem originária, integram as presentes versões e mantêm-se válidas.

§ 2º Os documentos referidos no caput encontram-se disponibilizados, em sua totalidade, no sítio http://www.iti.gov.br.

Art. 6º Esta Resolução entra em vigor na data de sua publicação.

LUIZ CARLOS DE AZEVEDO