Instituto Nacional de Tecnologia da Informação

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN QUADRA 02 BLOCO E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3945 - https://www.iti.gov.br

INSTRUÇÃO NORMATIVA Nº 08, DE 31 DE OUTUBRO DE 2019

Altera o DOC-ICP-01.01 para retirar dos Algoritmos e Suítes de Assinatura a função hash SHA-1 e os algoritmos criptográficos RSA 1024 bits para certificados de usuário final e RSA 2048 bits para certificados de AC.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9º do anexo I do Decreto nº 8.985, de 8 de fevereiro de 2017, e pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004,

CONSIDERANDO a Resolução nº 68, de 13 de outubro de 2009, que alterou os prazos especificados no Plano de adoção de novos padrões criptográficos, determinando que a partir de 2012 a função hash SHA-1 e os algoritmos criptográficos RSA 1024 bits para certificados de usuário final e RSA 2048 bits para certificados de AC não deveriam mais ser usados,

RESOLVE:

Art. 1º O DOC-ICP-01.01, versão 4.1, passa a vigorar com as seguintes alterações:

"2. .....

.....

Geração de Chaves Assimétricas de AC

.....	.....
.....	.....
Tamanho de chave	RSA 4096 ou brainpoolP512r1 ou Ed448 (448 bits) ou E-521 (521 bits).

Geração de Chaves Assimétricas de Usuário Final

.....	.....
.....	.....
Tamanho de chave A1, A2, A3, A CF-e-SAT, S1, S2, S3, T3, OM-BR	RSA 2048 ou brainpoolP256r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits)
.....	.....

Assinatura de Certificados de AC

.....	.....
Suíte de Assinatura	ha512WithRSAEncryption sha512WithECDSAEncryption id-Ed448, id-Ed521 id-Ed448ph, id-Ed521ph

Assinatura de Certificados de Usuário Final

.....	.....
Suíte de Assinatura	sha256WithRSAEncryption sha256WithECDSAEncryptin sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph

Assinatura de Listas de Certificados Revogados e Respostas OCSP

.....	.....
Algoritmo de Assinatura	sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed448, id-Ed521 id-Ed448ph, id-Ed521ph

.....

.....

Assinaturas Digitais ICP-Brasil CAdES, XAdES e PAdES

.....	.....
.....	.....
Suíte de Assinatura	sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph

Assinatura de Pedidos e Respostas de Carimbos do Tempo

.....	.....
.....	.....
Suíte de Assinatura	sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph

.....

.....

Esquemas de Acordos de Chaves

RSA 2048

RSA 4096

Esquema de Envelopes Criptográficos

3desWithRSA2048Encryption

aes128WithRSA2048Encryption
aes256WithRSA4096Encryption
aes128WithECIES256Encryption
aes256WithECIES512Encryption

.....

....." (NR)

Art. 2º Excluir a NOTA (1) da tabela Geração de Chaves Assimétricas de AC, do item 2 do DOC-ICP-01.01, versão 4.1.

Art. 3º Aprovar a versão 4.2 do documento DOC-ICP-01.01 - PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

§ 1º As demais cláusulas do referido documento, na sua versão imediatamente anterior, integram a presente versão 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 Instrução Normativa entra em vigor na data de sua publicação.

MARCELO AMARO BUZ

Diretor-Presidente

Documento assinado eletronicamente por **Marcelo Amaro Buz**, **Presidente**, em 31/10/2019, às 18:23, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 22449

A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0398261** e o código CRC **FE2615AC**.