ISSN 1677-7042

DIÁRIO OFICIAL DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL • IMPRENSA NACIONAL

Ano CLXIV Nº 23 Brasília - DF, terça-feira, 3 de fevereiro de 2026 SEÇÃO 1

Sumário

.....Esta edição é composta de 221 páginas .....

Presidência da República

CASA CIVIL

COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL

INSTRUÇÃO NORMATIVA ITI Nº 35, DE 30 DE JANEIRO DE 2026

Acrescenta novos algoritmos criptográficos e os certificados digitais dos tipos Selo Eletrônico e Aplicações Específicas ao documento Padrões e Algoritmos Criptográfico da ICP-Brasil - DOC-ICP-01.01. e atualiza o Manual de Condutas Técnicas nº 7.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 13 do anexo I do Decreto n° 12.103, de 8 de julho de 2024, pelo art. 1º da Resolução n° 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, e pelo art. 2° da Resolução n° 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020, resolve:

Art. 1º Esta Instrução Normativa altera o documento Padrões e Algoritmos Criptográficos da ICP-Brasil (DOC-ICP-01.01), consolidado pela Instrução Normativa ITI nº 22, de 23 de março de 2022, para acrescentar novos algoritmos criptográficos e os certificados digitais dos tipos Selo Eletrônico e Aplicações Específicas e atualiza a menção aos algoritmos criptográficos nos volumes I e II do Manual de Condutas Técnicas nº 7.

Art. 2º O Anexo da Instrução Normativa ITI nº 22, de 23 de março de 2022, (DOC-ICP 01.01) passa a vigorar com as seguintes alterações:

"2.1 .....

Geração de Chaves Assimétricas de AC	
.....	.....
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639) ou Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032) ou E-521 (Conforme parâmetros da curva estabelecidos neste DOC-ICP-01.01, PureEdDSA e HashEdDSA, conforme RFC 8032), ou ML-DSA (conforme FIPS 204).
Tamanho de chave	RSA 4096 ou brainpoolP512r1 ou Ed448 (448 bits) ou E-521 (521 bits) ou ML-DSA-(65 ou 87)

Geração de Chaves Assimétricas de Usuário Final	
.....	.....
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639) ou Curve25519 (Conforme RFC 7748) ou Ed25519 (PureEdDSA e HashEdDSA, conforme RFC 8032) ou Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032) ou E-521 (Conforme parâmetros da curva estabelecidos neste DOC-ICP-01.01, PureEdDSA e HashEdDSA, conforme RFC 8032) ou ML-DSA
Tamanho de chave A1, A2, A3, A CF-e-SAT, S1, S2, S3, T3, OM-BR, SE-S, SE-H, AE-S, AE-H	RSA 2048 ou brainpoolP256r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits) ou ML-DSA-44
Tamanho da chave A4, S4, T4, SE-H (para curvas elípticas)	RSA 2048 ou RSA 4096 ou brainpoolP512r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits) ou ML-DSA-44

Assinatura de Certificados de AC	
.....	.....
Suíte de Assinatura	sha512WithRSAEncryption sha512WithECDSAEncryption id-Ed448, id-Ed521 id-Ed448ph, id-Ed521ph id-ml-dsa-65, id-ml-dsa-87

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 id-ml-dsa-44

Assinatura de Listas de Certificados Revogados e Respostas OCSP	
.....	.....
Algoritmo de Assinatura	sha256WithRSAEncryption sha256WithECDSAEncryption
	sha512WithRSAEncryption sha512WithECDSAEncryption
	id-Ed448, id-Ed521 id-Ed448ph, id-Ed521ph id-ml-dsa-65, id-ml-dsa-87

Guarda da Chave Privada da Entidade Titular e de seu Backup	
.....	.....
Algoritmo e Tamanho de chave	3DES - 112 bits AES - 128 ou 256 bits ML-KEM-768 ou 1024
.....	.....

Assinaturas Digitais ICP-Brasil	
....	....
Suíte de Assinatura	sha256WithRSAEncryption sha256WithECDSAEncryption
	sha512WithRSAEncryption sha512WithECDSAEncryption
	id-Ed25519, id-Ed448, id-Ed521 id-Ed25519ph, id-Ed448ph, id-Ed521ph id-ml-dsa-44

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 id-ml-dsa-44

Esquemas de Acordos de Chaves
.....
.....
ML-KEM-512
ML-KEM-768
ML-KEM-1024

Esquema de Envelopes Criptográficos
.....
.....
aes128WithMLKEM512Encryption
aes256WithMLKEM768Encryption
aes256WithMLKEM1024Encryption

Art. 3º O volume I do Manual de Condutas Técnicas nº 7 - MCT 7 passa a vigorar com as seguintes alterações:

"**REQUISITO III.1.13**: Com relação aos algoritmos criptográficos obrigatórios suportados no objeto em avaliação, devem ser considerados aqueles aplicáveis definidos na versão corrente do documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL - DOC ICP-01.01".

Art. 4º O volume II do Manual de Condutas Técnicas nº 7 - MCT 7 passa a vigorar com as seguintes alterações:

"**REQUISITO III.1.13**: Com relação aos algoritmos criptográficos obrigatórios suportados no objeto em avaliação, devem ser considerados aqueles aplicáveis definidos na versão corrente do documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL - DOC ICP-01.01".

Art. 5º Ficam aprovadas:

I - a versão 6.0 do Documento Padrões e Algoritmos Criptográficos da ICP-Brasil (DOC-ICP-01.01); e

II - a versão 2.3 dos volumes I e II do Manual de Condutas Técnicas nº 7 - MCT 7.

Parágrafo único. A identificação da versão do DOC-ICP-01.01 deverá ser atualizada no preâmbulo e incluída no controle de versões do anexo da Instrução Normativa ITI nº 22, de 23 de março de 2022.

Art. 6º Fica revogada a Instrução Normativa ITI n° 04, de 09 de novembro de 2011.

Art. 7º Esta Instrução Normativa entra em vigor na data de sua publicação.

ENYLSON FLAVIO MARTINEZ CAMOLESI

AVISO

Foram publicadas em 2/2/2026 as edições extras nºs 22-A e 22-B do *DOU*.
Para acessar o conteúdo, clique nos nºs das edições.

IMPRENSA NACIONAL
Conexão com a informação oficial