

RESOLUÇÃO Nº 128, DE 13 DE SETEMBRO DE 2017.

APROVA A OBRIGATORIEDADE DE IMPLEMENTAÇÃO DA EXTENSÃO *SUBJECT ALTERNATIVE NAME* PARA CERTIFICADOS DO TIPO SSL/TLS.

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. 4º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, em plenária virtual encerrada em 13 de setembro de 2017,

RESOLVEU:

Art. 1º A alínea “c” do item 7.1.2.3, do DOC-ICP-04, versão 6.2, passa a vigorar com a seguinte redação:

c) Para certificado de equipamento ou aplicação:

c.1) 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

- i. **OID = 2.16.76.1.3.8 e conteúdo** = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;
- ii. **OID = 2.16.76.1.3.3 e conteúdo** = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;
- iii. **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;
- iv. **OID = 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.2) Para certificados do tipo SSL/TLS, Campo *dNSName*, obrigatório, contendo um ou mais domínios, seguindo as regras definidas na RFC 5280 e na RFC 2818.

Art. 2º A alínea “c”, do item 2.1.1 do DOC-ICP-05.02, versão 1.3, passa a vigorar com a seguinte redação:

- c) emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC. A extensão *Subject Alternative Name* é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

Art. 3º Ficam aprovadas as novas versões dos Documentos: DOC-ICP-04 - REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (versão 6.3) e DOC-ICP-05.02 - PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL (versão 1.4).

§ 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. 4º As entidades da ICP-Brasil têm o prazo de até 120 (cento e vinte) dias, contados da data da publicação, para se adequarem às mudanças previstas nesta Resolução.

Art. 5º Esta Resolução entra em vigor na data de sua publicação.

LUIZ CARLOS DE AZEVEDO