# INSTRUÇÃO NORMATIVA ITI Nº 18, DE 23 DE NOVEMBRO DE 2020

Aprova a versão revisada e consolidada do documento Procedimentos para Gerenciamento da Chave Simétrica para Geração do IDN DOC-ICP-05.04.

**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, pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, e pelo art. 2º da Resolução nº 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020,

**CONSIDERANDO** a determinação estabelecida pelo Decreto nº 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

**RESOLVE**:

**Art. 1º** Esta Instrução Normativa aprova a versão revisada e consolidada do documento Procedimentos para Gerenciamento da Chave Simétrica para Geração do IDN DOC-ICP-05.04.

**Art. 2º** Fica aprovada a versão 3.0 do documento DOC-ICP-05.04 – Procedimentos para Gerenciamento da Chave Simétrica para Geração do IDN.

**Art. 3º** Ficam revogadas:

I - a Instrução Normativa nº 08, de 10 de dezembro de 2015; e

II - a Instrução Normativa nº 13, de 21 de novembro de 2016.

**Art. 4º** Esta Instrução Normativa entra em vigor em 1° de dezembro de 2020.

CARLOS ROBERTO FORTNER

Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2020.11.23 21:17:40 -03'00'

**CARLOS ROBERTO FORTNER**

ANEXO

**Infraestrutura de Chaves Públicas Brasileira**

# PROCEDIMENTOS PARA GERENCIAMENTO DA CHAVE SIMÉTRICA PARA GERAÇÃO DO IDN

**DOC-ICP-05.04**

**Versão 3.0**

**23 de novembro de 2020**

# Sumário

# CONTROLE DE ALTERAÇÕES

| Resolução ou IN que aprovou alteração | Item Alterado | Descrição da Alteração |
|---|---|---|
| **IN ITI nº 18, de 23/11/2020 Versão 3.0** | | Revisão e consolidação, conforme Decreto nº 10.139, de 28 de novembro de 2019. |
| **Resolução nº 123, de 06.07.2017 Versão 2.1** | 1.2.3 | Inclui a opção de certificação INMETRO para a importação da cópia da chave criptográfica simétrica gerada. |
| **IN nº 13, de 21.11.2016 Versão 2.0** | 1, 3, 4 e 5. | Aprova a versão 2.0 - atualiza os procedimentos de geração, armazenamento, distribuição, proteção, validade e substituição de chaves utilizadas no IDN. |
| **IN nº 08, de 10.12.2015 Versão 1.0** | | Aprova a versão 1.0 do Documento Procedimentos para Gerenciamento da Chave Simétrica para geração do IDN. |

# LISTA DE SIGLAS e ACRÔNIMOS

| SIGLA | DESCRIÇÃO |
|---|---|
| AC | Autoridade Certificadora |
| AC RAIZ | Autoridade Certificadora Raiz da ICP-BRASIL |
| DOC-ICP | Documentos Principais da ICP-BRASIL |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IDN | Identificador de Registro Biométrico |
| INMETRO | Instituto Nacional de Metrologia, Qualidade e Tecnologia |
| ITI | Instituto Nacional de Tecnologia da Informação |
| MSC | Módulo de Segurança Criptográfico |
| PSBio | Prestador de Serviço Biométrico |

# 1. GERAÇÃO, ARMAZENAMENTO E DISTRIBUIÇÃO DA CHAVE

## 1.1 Geração e armazenamento da chave

1.1.1 As chaves criptográficas simétricas serão geradas e armazenadas pela AC Raiz, em *hardware* seguro com atributos específicos que permitam o gerenciamento do seu ciclo de vida.

1.1.2 O algorítmo e o tamanho das chaves criptográficas simétricas geradas pela AC Raiz e utilizadas para geração do IDN pelas ACs estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

## 1.2 Distribuição da chave

### 1.2.1 Recebimento de certificado digital da entidade

1.2.1.1 As entidades interessadas, devidamente credenciadas no âmbito da ICP-Brasil, deverão gerar certificado digital, sendo a chave privada correspondente gerada e armazenada em MSC próprio da entidade.

1.2.1.2 Este certificado deverá ser enviado ao ITI por correio eletrônico, assinado digitalmente pelo representante legal da entidade.

### 1.2.2 Exportação da Chave Criptográfica Simétrica

1.2.2.1 Após o recebimento do certificado digital encaminhado pela entidade, o ITI agendará cerimônia interna de extração da correspondente chave pública, que servirá para cifragem e exportação da chave criptográfica simétrica.

### 1.2.3 Importação da Chave Criptográfica Simétrica pela Entidade

1.2.3.1 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].

1.2.3.2 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.

1.2.3.3 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.

### 1.2.4 Prazo para distribuição da chave criptográfica simétrica

O ITI deverá providenciar a distribuição da chave criptográfica simétrica em no máximo 30(trinta) dias úteis, contados a partir do recebimento do certificado digital da entidade.

## 2. PROTEÇÃO DA CHAVE

2.1 As chaves criptográficas simétricas da AC Raiz, ao serem exportadas, serão cifradas com a chave pública da entidade, que deverá manter a chave privada equivalente em MSC, para abrir o envelope digital seguindo as regras do esquema de cifragem.

2.2 Compete à AC Raiz acompanhar a evolução tecnológica para, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, com a atualização do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

## 3. PRAZO DE VALIDADE

3.1 Toda chave simétrica gerada pela AC Raiz terá validade de 2 (dois) anos, podendo ser prorrogada por meio de ato normativo do ITI.

3.2 Para geração e distribuição de nova chave criptográfica simétrica deverão ser observadas as regras e procedimentos estabelecidos no item 1 deste documento.

## 4. SUBSTITUIÇÃO DA CHAVE SIMÉTRICA

4.1 A AC Raiz pode, a qualquer momento, gerar uma nova chave criptográfica simétrica para geração dos IDNs da ICP-Brasil, observando as regras e procedimentos do item 1 do presente documento.

4.2 Assim que as entidades receberem da AC Raiz uma nova chave criptográfica simétrica, os indexadores IDN usados por entidades e PSBios deverão ser recalculados. Caso necessário, poderão ser mantidos os IDNs antigos até a completa reindexação de todas as bases de dados.

4.3 O procedimento de substituição da chave criptográfica simétrica, incluindo a reindexação das bases de dados com IDNs recalculados, deve ser executado num prazo máximo de 15 (quinze) dias úteis, contados a partir da importação da chave simétrica pelas entidades, de maneira sincronizada entre entidades e PSBios, de forma a não causar indisponibilidades no sistema. No caso de comprometimento da chave criptográfica simétrica, esses procedimentos devem ocorrer em no máximo 2 (dois) dias úteis.

4.4 Após a reindexação das bases de dados, os PSBios deverão excluir permanentemente qualquer informação indexada pelo IDN gerado a partir da chave criptográfica simétrica anterior, devendo as entidades manter em seus registros a associação entre IDN antigo e o novo.

## 5. CÓPIA DE SEGURANÇA DE CHAVE

5.1 Cabe à AC Raiz realizar cópias de segurança de todas as chaves criptográficas simétricas geradas, de forma a garantir a sua preservação, bem como a contingência do sistema de geração e distribuição das chaves.

## 6. DOCUMENTOS REFERENCIADOS

6.1 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

| Ref. | Nome do Documento | Código |
|---|---|---|
| [1] | PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.<br><br>Aprovado pela Instrução Normativa nº 04, de 18 de maio de 2006 | DOC-ICP-01.01 |