INSTRUÇÃO NORMATIVA ITI Nº 12, DE 20 DE MAIO DE 2021

Aprova a versão revisada e consolidada do documento Padrões e Procedimentos Técnicos para Processos de Homologação de Softwares de Bibliotecas Criptográficas e Softwares Provedores de Serviços Criptográficos na ICP-Brasil – DOC-ICP-10.06.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9° do anexo I do Decreto n° 8.985, de 8 de fevereiro de 2017, pelo art. 1° 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,

CONSIDERANDO a determinação estabelecida pelo Decreto n° 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. 1° Esta Instrução Normativa aprova a versão revisada e consolidada do documento Padrões e Procedimentos Técnicos para Processos de Homologação de Software de Bibliotecas Criptográficas e Softwares Provedores de Serviços Criptográficos na ICP-Brasil.

Art. 2° Fica aprovada a versão 2.0 do documento DOC-ICP-10.06 – Padrões e Procedimentos Técnicos para Processos de Homologação de Software de Bibliotecas Criptográficas e Softwares Provedores de Serviços Criptográficos na ICP-Brasil, anexa a esta Instrução Normativa.

Art. 3° Fica revogada a Instrução Normativa n° 06, de 11 de dezembro de 2007.

Art. 4° Esta Instrução Normativa entra em vigor em 1° de junho de 2021.

CARLOS ROBERTO FORTNER

Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2021.05.20 16:40:47 -03'00'

CARLOS ROBERTO FORTNER

Infraestrutura de Chaves Públicas Brasileira

ANEXO

PADRÕES E PROCEDIMENTOS TÉCNICOS PARA PROCESSOS DE HOMOLOGAÇÃO DE SOFTWARES DE BIBLIOTECAS CRIPTOGRÁFICAS E SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS NA ICP-BRASIL

DOC-ICP-10.06

Versão 2.0

20 de maio de 2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
IN ITI nº 12, de 20.05.2021 Versão 2.0		Revisão e consolidação conforme o Decreto n° 10.139, de 28 de novembro de 2019.
IN nº06, de 11.12.2007 Versão 1.0		Aprova a versão 1.0 dos Padrões e Procedimentos Técnicos a Serem Observados nos Processos de Homologação de Softwares de Bibliotecas Criptográficas e Softwares Provedores de Serviços Criptográficos no Âmbito da ICP-Brasil, na forma definida pelo anexo.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
LEA	Laboratório de Ensaios e Auditoria
MCT	Manual de Condutas Técnicas
NSH	Nível de Segurança de Homologação

1 DISPOSIÇÕES GERAIS

1.1 Este documento se aplica aos processos de homologação de softwares de bibliotecas criptográficas e softwares provedores de serviços criptográficos no âmbito da ICP-Brasil.

1.2 Define o conjunto de requisitos técnicos, material e documentação técnicos para depósito e ensaios de conformidade, bem como os volumes do Manual de Condutas Técnicas do ITI aplicáveis aos processos de homologação dos objetos citados no item 1.1.

1.3 Suplementa, no que se refere aos objetos de homologação citados no item 1.1, o documento REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NA ICP-BRASIL [1].

2 REQUISITOS TÉCNICOS

2.1 Os requisitos técnicos a serem observados nos processos de homologação dos objetos citados no item 1.1 são:

a) aderência aos requisitos de documentação, segurança e funcionais, conforme definido nos documentos citados no item 3.2; e

b) aderência aos requisitos específicos, detalhados nos documentos citados no item 3.2, tais como:

i. algoritmos criptográficos mínimos e proteção de chaves em memória, para softwares de bibliotecas criptográficas; e

ii. gerenciamento, exportação e importação, certificação e proteção de chaves em memória, para softwares provedores de serviços criptográficos.

2.2 Os requisitos técnicos estabelecidos por este documento têm caráter macroestrutural, ou seja, representam, na verdade, um conjunto de requisitos técnicos específicos e pormenorizados. Para conhecer o completo detalhamento destes, consultar os documentos citados no item 3.2.

3 MATERIAL E DOCUMENTAÇÃO TÉCNICOS A SEREM DEPOSITADOS

3.1 Para efeitos do disposto nos PROCEDIMENTOS ADMINISTRATIVOS PARA HOMOLOGAÇÃO NA ICP-BRASIL [2] quanto aos processos de homologação dos sistemas de que trata este documento, o responsável técnico da parte interessada deverá apresentar ao LEA para depósito, o material e documentação técnicos, conforme descritos a seguir:

a) FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL [6];

b) documentação técnica, segundo o disposto no documento citado no item 3.2; e

c) componentes em softwares executáveis, segundo o disposto no documento citado no item 3.2.

3.2 O material e documentação técnicos estabelecidos por este documento têm caráter macroestrutural, ou seja, representam, na verdade, um conjunto de materiais de hardware, software e

documentos técnicos específicos e pormenorizados. Para conhecer o completo detalhamento destes, consultar os documentos:

a) MANUAL DE CONDUTAS TÉCNICAS 8 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE SOFTWARES DE BIBLIOTECAS CRIPTOGRÁFICAS NO ÂMBITO DA ICP-BRASIL [4].

b) MANUAL DE CONDUTAS TÉCNICAS 9 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL [5].

3.3 Os documentos referidos no item anterior poderão ser atualizados, a qualquer tempo, pelo ITI, de forma a melhor explicitar e explicar os requisitos técnicos e recomendações a serem observados nas avaliações de conformidade dos dispositivos de que trata este documento, bem como o material e documentação técnicos a serem depositados.

3.4 Para alterar, incluir ou excluir qualquer requisito técnico, material ou documentação de caráter macroestrutural, o ITI deverá editar nova instrução normativa.

4 ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE

4.1 A avaliação de conformidade dos dispositivos de que trata este documento será realizada pelos LEAs, tendo por referência os ensaios descritos nos documentos:

a) MANUAL DE CONDUTAS TÉCNICAS 8 – VOLUME II: PROCEDIMENTOS DE ENSAIO PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE SOFTWARES DE BIBLIOTECAS CRIPTOGRÁFICAS NO ÂMBITO DA ICP-BRASIL [6].

b) MANUAL DE CONDUTAS TÉCNICAS 9 – VOLUME II: PROCEDIMENTOS DE ENSAIO PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL [7].

4.2 Os documentos referidos no item anterior poderão ser atualizados pelo ITI, a qualquer tempo, de forma a melhor explicitar e explicar os ensaios técnicos a serem empregados nas avaliações de conformidade aos requisitos técnicos e recomendações estabelecidos para os dispositivos de que trata este documento.

5 NÍVEL DE SEGURANÇA DE HOMOLOGAÇÃO

5.1 No FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL [3] a parte interessada deverá definir qual o Nível de Segurança de Homologação (NSH) pretendido para o objeto a ser homologado, conforme documento ESTRUTURA NORMATIVA TÉCNICA E NÍVEIS DE SEGURANÇA DE HOMOLOGAÇÃO NA ICP-BRASIL [8].

5.2 A escolha do NSH influenciará no tipo e quantidade de materiais a serem depositados para avaliação da conformidade.

6 DOCUMENTOS REFERENCIADOS

6.1 O documento abaixo é aprovado por Resolução do Comitê Gestor da ICP-Brasil, podendo ser alterado, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desse documento e a resolução que o aprovou.

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	**REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NA ICP-BRASIL** Aprovado pela Resolução nº 36, de 21 de outubro de 2004.	**DOC-ICP-10**

6.2 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
[2]	**PROCEDIMENTOS ADMINISTRATIVOS PARA HOMOLOGAÇÃO NA ICP-BRASIL** Aprovado pela Instrução Normativa nº 02, de 13 de abril de 2005.	**DOC-ICP-10.01**
[8]	**ESTRUTURA NORMATIVA TÉCNICA E NÍVEIS DE SEGURANÇA DE HOMOLOGAÇÃO NA ICP-BRASIL** Aprovado pela Instrução Normativa nº 02, de 14 de fevereiro de 2006.	**DOC-ICP-10.02**

6.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

REF.	NOME DO DOCUMENTO	CÓDIGO
[3]	**FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL**	**ADE-ICP-10.03.A**
[4]	**MANUAL DE CONDUTAS TÉCNICAS 8 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE BIBLIOTECAS CRIPTOGRÁFICAS NO ÂMBITO DA ICP-BRASIL**	**MCT 8 – Vol. I**
[5]	**MANUAL DE CONDUTAS TÉCNICAS 9 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL.**	**MCT 9 – Vol. I**
[6]	**MANUAL DE CONDUTAS TÉCNICAS 8 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE BIBLIOTECAS CRIPTOGRÁFICAS NO ÂMBITO DA ICP-BRASIL**	**MCT 8 – Vol.II**

[7]	**MANUAL DE CONDUTAS TÉCNICAS 9 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL**	**MCT 9 – Vol.II**