

INSTRUÇÃO NORMATIVA ITI Nº 11, DE 20 DE MAIO DE 2021

Aprova a versão revisada e consolidada do documento Padrões e Procedimentos Técnicos para Processos de Homologação de Módulos de Segurança Criptográfica (MSC) na ICP-Brasil – DOC-ICP-10.05.

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,

RESOLVEU:

Art. 1º Esta Instrução Normativa aprova a versão revisada e consolidada do documento Padrões e Procedimentos Técnicos para Processos de Homologação de Módulos de Segurança Criptográfica (MSC) na ICP-Brasil.

Art. 2º Fica aprovada a versão 2.0 do documento DOC-ICP-10.05 – Padrões e Procedimentos Técnicos para Processos de Homologação de Módulos de Segurança Criptográfica (MSC) na ICP-Brasil, anexa a esta Instrução Normativa.

Art. 3º Fica revogada a Instrução Normativa nº 05, de 11 de dezembro de 2007.

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

CARLOS ROBERTO FORTNER



Infraestrutura de Chaves Públicas Brasileira

ANEXO

PADRÕES E PROCEDIMENTOS TÉCNICOS PARA PROCESSOS DE HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC) NA ICP-BRASIL

DOC-ICP-10.05

Versão 2.0

20 de maio de 2021



Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

CONTROLE DE ALTERAÇÕES	3
LISTA DE SIGLAS E ACRÔNIMOS.....	4
1 DISPOSIÇÕES GERAIS.....	5
2 REQUISITOS TÉCNICOS.....	5
3 MATERIAL E DOCUMENTAÇÃO TÉCNICOS A SEREM DEPOSITADOS	6
4 ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE.....	6
5 NÍVEL DE SEGURANÇA DE HOMOLOGAÇÃO.....	7
6 NÍVEL DE SEGURANÇA FÍSICA	7
7 DOCUMENTOS REFERENCIADOS	8



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
IN ITI nº 11, de 20.05.2021 Versão 2.0		Revisão e consolidação conforme o Decreto nº 10.139, de 28 de novembro de 2019.
Instrução Normativa nº 05, de 11 de dezembro de 2007 Versão 1.0		Aprova a versão 1.0 do DOC-ICP 10.05.



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
API	<i>Application Programming Interface</i>
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
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
MSC	Módulo de Segurança Criptográfica
NSF	Nível de Segurança Física
NSH	Nível de Segurança de Homologação
PKCS#11	<i>Cryptographic Token Interface Standard</i>



Infraestrutura de Chaves Públicas Brasileira

1 DISPOSIÇÕES GERAIS

1.1 Este documento se aplica aos processos de homologação de Módulos de Segurança Criptográfica (MSC) no âmbito da ICP-Brasil, compreendendo-se por MSC um servidor ou placa auxiliar de segurança fisicamente seguro, resistente à violação que fornece funcionalidades criptográficas com capacidade de geração e armazenamento de chaves criptográficas simétricas e assimétricas voltados para utilização em uma Infraestrutura de Chaves Públicas - ICP.

1.2 Este documento 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 segurança, gerenciamento, restrição de substâncias nocivas e documentação conforme definido no documento citado no item 3.2; e
- b) aderência a interfaces de interoperabilidade específicas, das quais ao menos uma deve ser suportada:
 - i. aderência aos requisitos de interoperabilidade ao nível de PKCS#11, informando o ambiente operacional no qual foi analisada a interoperabilidade;
 - ii. aderência aos requisitos de interoperabilidade ao nível de CryptoAPI, informando o ambiente operacional no qual foi analisada a interoperabilidade;
 - iii. aderência aos requisitos de interoperabilidade ao nível de JCE, informando o ambiente operacional no qual foi analisada a interoperabilidade;
 - iv. aderência aos requisitos de interoperabilidade ao nível de OpenSSL, informando o ambiente operacional no qual foi analisada a interoperabilidade; ou
 - v. aderência aos requisitos de interoperabilidade ao nível de uma API proprietária, caso utilizada, informando o ambiente operacional no qual foi analisada a interoperabilidade;

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 o documento citado no item 3.2.



Infraestrutura de Chaves Públicas Brasileira

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 [3];
- b) amostras de MSCs a serem submetidas ao processo de homologação, bem como leitoras de cartões inteligentes, cartões e *tokens* criptográficos para apoio no processo de controle de acesso ao módulo criptográfico, segundo o disposto no documento citado no item 3.2;
- c) documentação técnica, segundo o disposto no documento citado no item 3.2; e
- d) 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 o documento MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL [4].

3.3 O documento referido no item anterior poderá ser atualizado, a qualquer tempo, pelo ITI, de forma a melhor explicitar e explicar os requisitos técnicos e recomendações a serem observados nas avaliações de conformidade do dispositivo 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 no documento MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL [5].

4.2 O documento referido no item anterior poderá ser atualizado 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 o dispositivo de que trata este documento.



Infraestrutura de Chaves Públicas Brasileira

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 [6].

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

6 NÍVEL DE SEGURANÇA FÍSICA

6.1 No FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL [3] a parte interessada deverá definir qual o Nível de Segurança Física (NSF) pretendido para o objeto a ser homologado.

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

6.3 A escolha do NSF influenciará no nível de análise de conformidade a ser realizada sobre os mecanismos de segurança física dos MSCs.



Infraestrutura de Chaves Públicas Brasileira

7 DOCUMENTOS REFERENCIADOS

7.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, 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 resoluções que os aprovaram.

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

7.2 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
[6]	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

7.3 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 7 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL	MCT 7 – Vol. I
[5]	MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME II:	MCT 7 – Vol. II



Infraestrutura de Chaves Públicas Brasileira

PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL