

**CASA CIVIL  
INSTITUTO NACIONAL DE TECNOLOGIA  
DA INFORMAÇÃO**

**INSTRUÇÃO NORMATIVA Nº 6, DE 11 DE DEZEMBRO DE 2007**

**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 e dá outras providências.**

**O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO**, no uso das atribuições que lhe foram conferidas pelo inciso I, do art. 1º, do anexo I, do Decreto nº 4.689, de 7 de maio de 2003 e pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004;

**R E S O L V E :**

**Art. 1º** Aprovar a versão 1.0 do documento PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SOFTWARES DE BIBLIOTECAS CRIPTOGRÁFICAS E SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS (DOC-ICP-10.06), na forma definida pelo anexo.

**Art. 2º** Todo e qualquer questionamento acerca do disposto nesta Instrução Normativa deverá ser encaminhado ao endereço homologa@planalto.gov.br.

**Art. 3º** Esta Instrução Normativa entra em vigor na data de sua publicação.

**RENATO DA SILVEIRA MARTINI**

## ANEXO

### **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 (DOC-ICP-10.06) - Versão 1.0**

#### **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 parágrafo 1.1.

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

#### **2. Requisitos Técnicos**

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

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

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

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

**2.** 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 no parágrafo 8.6 dos PROCEDIMENTOS ADMINISTRATIVOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICPBRASIL [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], devidamente preenchido e assinado, em quatro vias;
- b) documentação técnica, segundo o disposto no documento citado no parágrafo 3.2; e
- c) componentes em softwares executáveis, segundo o disposto no documento citado no parágrafo 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 parágrafo 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 LEA, 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 ICPBRASIL [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 parágrafo 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 A SEREM UTILIZADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICPBRASIL [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 a aprovou.

**Fonte:**

[http://www.iti.gov.br/twiki/pub/Certificacao/LegislacaoConsolidada/instrucoes\\_normativas.pdf](http://www.iti.gov.br/twiki/pub/Certificacao/LegislacaoConsolidada/instrucoes_normativas.pdf)