



Coordenação-Geral de Acreditação

**ORIENTAÇÃO PARA A ELABORAÇÃO DOS
ESCOPOS DE ACREDITAÇÃO VOLTADOS AOS
LABORATÓRIOS DE ENSAIOS QUE ATUAM NA
ÁREA DE ATIVIDADE: EQUIPAMENTOS DE
TECNOLOGIA DA INFORMAÇÃO, SUBÁREA DE
ATIVIDADE: INFRAESTRUTURA DE CHAVE PÚBLICA**

Documento de caráter orientativo

DOQ-CGCRE-066

Revisão 01 – NOV/2023



SUMÁRIO

- 1 Objetivo
- 2 Campo de aplicação
- 3 Responsabilidade
- 4 Histórico da revisão
- 5 Documentos complementares
- 6 Siglas
- 7 Proposta de harmonização voltada à área de atividade: Equipamentos de Tecnologia da Informação, subárea de atividade: Infraestrutura de chave Pública

1 OBJETIVO

Este documento estabelece orientações para a descrição de subáreas, produtos e ensaios para área de atividade: Equipamentos de Tecnologia da Informação, subárea de atividade: Infraestrutura de chave Pública, visando à harmonização dos escopos de acreditação dos laboratórios. Este documento foi desenvolvido de acordo com a análise dos volumes I e II dos Manuais de Conduta Técnica 1, 2, 3 e 7 de 2007, que dispõem sobre os requisitos ensaios a serem realizados respectivamente em cartões criptográficos (smartcard), leitoras de cartões, tokens e módulos criptográficos.

A Cgcre emitiu documentos orientativos visando harmonizar a descrição dos produtos e ensaios em algumas áreas de atividade. Caso o laboratório solicite outros ensaios em diferentes produtos que possam ser enquadrados na área de atividade em questão, solicita-se que o laboratório sinalize em sua proposta de escopo para a análise técnica no âmbito da Dicla da seguinte maneira: inclusão de descrição de ensaio – sugestão de revisão do “número do documento orientativo”.

2 CAMPO DE APLICAÇÃO

Este documento aplica-se à Dicla, aos laboratórios de ensaios acreditados e aos laboratórios postulantes à acreditação na área de atividade: Equipamentos de Tecnologia da Informação, subárea de atividade: Infraestrutura de chave Pública, e aos avaliadores e especialistas que atuam nos processos de acreditação de laboratórios desta área. Ele foi desenvolvido de acordo com diretrizes internacionais e contém aplicações sobre os requisitos da acreditação.

As orientações desse documento deverão ser consideradas tanto pelos avaliadores quanto especialistas durante a acreditação de um laboratório de ensaio.

3 RESPONSABILIDADE

A responsabilidade pela revisão deste documento é da Dicla.



4 HISTÓRICO DA REVISÃO

Revisão	Data	Itens revisados
01	Nov/2023	<ul style="list-style-type: none">▪ Atualização do cabeçalho para atender ao modelo atual.▪ Atualização da marca da Cgcre no cabeçalho.▪ Inclusão dos capítulos 4 e 5 para atender ao modelo atual de elaboração de normas.▪ Atualizado requisito da ABNT NBR ISO/IEC 17025 no capítulo 8 e retirada a referência ao ano das normas dos ensaios (cabe ao laboratório informar o ano da norma na reavaliação ou na atualização do escopo)

5 DOCUMENTOS COMPLEMENTARES

ABNT NBR ISO/IEC 17025	Requisitos Gerais para Competência de Laboratórios de Ensaio e Calibração
Manual de Condutas Técnicas 1 – Vol. I	Requisitos, Materiais e Documentos Técnicos para Homologação de Cartões Criptográficos (Smart Cards) no Âmbito da ICP-Brasil – versão 3 - 2007
Manual de Condutas Técnicas 1 – Vol. II	Procedimentos de Ensaio para Avaliação de Conformidade aos Requisitos Técnicos de Cartões Criptográficos (Smart Cards) no Âmbito da ICP-Brasil – versão 3 - 2007
Manual de Condutas Técnicas 2 – Vol. I	Requisitos, Materiais e Documentos Técnicos para Homologação de Leitoras de Cartões Inteligentes no Âmbito da ICP-Brasil
Manual de Condutas Técnicas 2 – Vol. II	Procedimentos de Ensaio para Avaliação de Conformidade aos Requisitos Técnicos de Leitoras de Cartões Inteligentes no Âmbito da ICP-Brasil – versão 3 - 2007
Manual de Condutas Técnicas 3 – Vol. I	Requisitos, Materiais e Documentos Técnicos para Homologação de Tokens Criptográficos no Âmbito da ICP-Brasil – versão 3 - 2007
Manual de Condutas Técnicas 3 – Vol. II	Procedimentos de Ensaio para Avaliação de Conformidade aos Requisitos Técnicos de Tokens Criptográficos no Âmbito da ICP-Brasil – versão 3 - 2007
Manual de Condutas Técnicas 7 – Vol. I	Requisitos, Materiais e Documentos Técnicos para Homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil – versão 1 - 2007
Manual de Condutas Técnicas 7 – Vol. II	Procedimentos de Ensaio para Avaliação de Conformidade aos Requisitos Técnicos de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil – versão 1 – 2007
NIT-Dicla-016	Elaboração de escopo de laboratórios de ensaios e de provedores de ensaios de proficiência

6 SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
Cgcre	Coordenação-Geral de Acreditação
Dicla	Divisão de Acreditação de Laboratórios
IEC	<i>International Electrotechnical Commission (Comissão Eletrotécnica Internacional)</i>
Inmetro	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	<i>International Organization for Standardization (Organização Internacional para Normalização)</i>
MCT	Manual de Conduta Técnica
NBR	Norma Brasileira



7 PROPOSTA DE HARMONIZAÇÃO VOLTADA À ÁREA DE ATIVIDADE: EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO, SUBÁREA DE ATIVIDADE: INFRAESTRUTURA DE CHAVE PÚBLICA

8.1 As normas e procedimentos citados na tabela abaixo visam indicar possíveis metodologias utilizadas pelos laboratórios de ensaio. Entretanto, cabe ao laboratório de ensaio selecionar o método visando atender o requisito 7.1.2 da norma ABNT NBR ISO/IEC 17025.

8.2 Conforme descrito na NIT-Dicla-016, para as classes de ensaio deve ser estabelecida a propriedade a ser medida ou determinada e a técnica aplicada ao ensaio.

8.3 A tabela 1 apresenta a proposta de harmonização.

Tabela 1 – Proposta de Harmonização

Área de atividade/Produto	Classe de Ensaio/Descrição do Ensaio	Norma e/ou Procedimento
<u>EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO</u>		
<u>SUBÁREA DE ATIVIDADE: INFRAESTRUTURA DE CHAVE PÚBLICA</u>	<u>ENSAIOS DE SOFTWARE</u>	
Cartões Criptográficos (Smart card)	<ul style="list-style-type: none">- Ensaio de algoritmos criptográficos;- Ensaio de funcionalidade;- Ensaio de hardware seguro;- Ensaio de software seguro;- Ensaio para verificação de controle de acesso;- Ensaio de interoperabilidade	MCT-1 vol.II, ISO 7816-2, ISO 7816-3, ISO 7816-4, ISO 7816-5, ISO 7816-6, ISO 7816-7, ISO 7816-8, ISO 7816-9
Leitoras de Cartão	<ul style="list-style-type: none">- Ensaio de algoritmos criptográficos;- Ensaio de funcionalidade;- Ensaio de hardware seguro;- Ensaio de software seguro;- Ensaio para verificação de controle de acesso;- Ensaio de interoperabilidade	MCT-2 vol.II, ISO 7816-2, ISO 7816-3, ISO 7816-4, ISO 7816-5, ISO 7816-6, ISO 7816-7, ISO 7816-8, ISO 7816-9
Token	<ul style="list-style-type: none">- Ensaio de algoritmos criptográficos;- Ensaio de funcionalidade;- Ensaio de hardware seguro;- Ensaio de software seguro;- Ensaio para verificação de controle de acesso;- Ensaio de interoperabilidade	MCT-3 vol.II, ISO 7816-2, ISO 7816-3, ISO 7816-4, ISO 7816-5, ISO 7816-6, ISO 7816-7, ISO 7816-8, ISO 7816-9
Módulos criptográficos	<ul style="list-style-type: none">- Ensaio de algoritmos criptográficos;- Ensaio de funcionalidade;- Ensaio de hardware seguro;- Ensaio de software seguro;- Ensaio para verificação de controle de acesso;- Ensaio de interoperabilidade	MCT-7 vol.II