	ANÁLISE DE SOFTWARE PARA AVALIAÇÃO DE MODELO DE INSTRUMENTOS DE PESAGEM AUTOMÁTICOS DE VEÍCULOS RODOVIÁRIOS EM MOVIMENTO	NORMA Nº NIT-SINST-026	REV. Nº 01
		PUBLICADO EM ABR/2022	PÁGINA 1/15

SUMÁRIO

- 1 Objetivo
 - 2 Campo de aplicação
 - 3 Responsabilidade
 - 4 Documentos de referência
 - 5 Documentos complementares
 - 6 Siglas
 - 7 Termos e definições
 - 8 Orientações gerais
 - 9 Requisitos gerais de *software* e *hardware*
 - 10 Requisitos específicos de *software* e *hardware*
 - 11 Disposições gerais
 - 12 Histórico da revisão e quadro de aprovação
- ANEXO A – Ensaio funcionais de *software*

1 OBJETIVO

Esta Norma estabelece os procedimentos a serem utilizados na análise de *software* para avaliação de modelo de instrumentos de pesagem automáticos de veículos rodoviários em movimento.

2 CAMPO DE APLICAÇÃO

Esta Norma aplica-se à Dimel/Disme/Sinst e laboratórios acreditados.


3 RESPONSABILIDADE

A responsabilidade pela aprovação, revisão e cancelamento desta norma é do Sinst.

4 DOCUMENTOS DE REFERÊNCIA

Portaria Inmetro nº 19 de 12/01/2022	Aprova o Regulamento Técnico Metrológico consolidado para instrumentos de pesagem automáticos de veículos rodoviários em movimento.
Portaria Inmetro nº 232 de 08/05/2012	Vocabulário Internacional de Metrologia: Conceitos fundamentais e gerais e termos associados (VIM) - 1ª. Edição Luso-brasileira
Portaria Inmetro nº 150 de 29/03/2016	Vocabulário Internacional de Termos de Metrologia Legal
OIML D 31: 2008	<i>General requirements for software controlled measuring instruments</i>
OIML D 11: 2004	<i>General requirements for electronic measuring instruments</i>

(continua)

	NIT-SINST-026	REV. 01	PÁGINA 2/15
---	----------------------	--------------------	------------------------

WELMEC <i>Software Guide</i> 7.2 2015	<i>Measuring instruments directive 2014/32/EU – WELMEC</i>
NIST <i>special publication</i> 800-57 <i>Part 1 Revision 4</i>	<i>Recommendation for key management – Part 1: General</i>

5 DOCUMENTOS COMPLEMENTARES

Não aplicável.

6 SIGLAS

As siglas das UP/UO do Inmetro podem ser acessadas em:
<http://www.inmetro.gov.br/inmetro/pdf/regimento-interno.pdf>.

AM	Avaliação de Modelo
ACF	Análise do Código Fonte
AMD	Análise do Memorial Descritivo
EFS	Ensaio Funcional de <i>Software</i>
IPA	Instrumento de Pesagem Automático de veículos rodoviários em movimento
NIST	<i>National Institute of Standards and Technology</i> (Instituto Nacional de Padrões e Tecnologia)
OS	Sistema Operacional
OTP	<i>One-Time Programmable</i> (Programável uma vez)
RBMLQ-I	Rede Brasileira de Metrologia Legal e Qualidade - Inmetro
RTM	Regulamento Técnico Metrológico
VIM	Vocabulário Internacional de Metrologia
VIML	Vocabulário Internacional de Metrologia Legal

7 TERMOS E DEFINIÇÕES

7.1 Arquivo binário


Arquivo de computador que não está em formato texto, oriundo da compilação de um código-fonte, que contém *software* legalmente relevante.

7.2 Assinatura digital

Código atribuído a um arquivo digital de forma a provar a sua integridade, autenticidade e não repúdio.

7.3 Carga de *software*

Processo de transferência automática de *software* para o instrumento de medição usando qualquer meio apropriado local ou remoto sem a necessidade de romper selagem principal.

	NIT-SINST-026	REV. 01	PÁGINA 3/15
---	----------------------	--------------------	------------------------

7.4 Componente imutável

Componentes e dispositivos eletrônicos do instrumento com a função de processamento de dados, que sejam não programáveis ou que não permitam alteração de seu *firmware* interno ou que sejam dotados de memória de programação apenas do tipo OTP.

7.5 Instrumento com computador tipo U

Um instrumento com computador de propósito geral, geralmente baseado em um PC, que não obedece a definição de computador tipo P.

7.6 Instrumento com computador tipo P

Um instrumento com computador tipo P embarcado é caracterizado por:

- a) o *software* é construído exclusivamente para fins de medição. Adicionalmente funções para a proteção de *software* e dados, para transmissão de dados e para carga de *software* são considerados construídos para o propósito de medição;
- b) a interface do usuário é dedicada ao propósito de medição;
- c) um sistema operacional (OS) ou subsistemas podem ser incluídos se apenas o *software* legalmente relevante possui comunicação externa; se não permite carregar ou alterar programas, parâmetros ou dados ou executar programas; se não permite alterar o ambiente da aplicação legalmente relevante; e inclui controle de acesso e não permite uma mudança subsequente na configuração de controle de acesso; e
- d) o ambiente de *software* é invariável e não há meios internos ou externos para programar ou alterar o *software* em seu *status* incorporado, salvo quando os requisitos de carga de *software* são atendidos.

7.7 Legalmente relevante

Todos os módulos de *software* (programas, sub-rotinas, objetos, etc.) que executam funções legalmente relevantes ou que contêm domínios de dados legalmente relevantes formam a parte de *software* legalmente relevante de um instrumento de medição. Mais especificamente, isso inclui todos os módulos de *software* que:


- a) têm impacto no cálculo de uma unidade de medida legal;
- b) contribuem para funções como: exibir, proteger e armazenar dados legalmente relevantes;
- c) identificam os *softwares* legalmente relevantes; e/ou
- d) executam carga de *software* legalmente relevante.

7.8 Memorial descritivo

Documento que descreve detalhadamente as implementações tecnológicas para atender os requisitos de segurança de *hardware* e *software*.

7.9 Não legalmente relevante

Todo *software/hardware/dados* presentes no instrumento que não são legalmente relevantes.

	NIT-SINST-026	REV. 01	PÁGINA 4/15
---	---------------	------------	----------------

7.10 Requerente

É toda pessoa jurídica, pública ou privada, nacional ou estrangeira, sediada no Brasil, que desenvolva atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de instrumentos que solicita serviço de avaliação de modelo à Dimel.

7.11 Requisitos gerais de *software*

Requisitos gerais são os requisitos do RTM que o *software* e *hardware* considerados legalmente relevante devem satisfazer totalmente.

7.12 Requisitos específicos de *software*

Os requisitos do RTM que devem ser obedecidos quando o *software* e o *hardware* empregam funcionalidades tecnológicas específicas.

7.13 Selagem principal

Selagem do instrumento de medição (lacre) que demonstra que o instrumento estará apto a operar mediante a verificação por parte do Órgão da RBMLQ-I ou por entidade autorizada.

7.14 Verificação de integridade

Processo que verifica que os dados/*software*/parâmetros não foram alterados durante o uso, reparo, manutenção, transferência ou armazenamento sem que haja autorização do Inmetro.

8 ORIENTAÇÕES GERAIS

8.1 A análise de *software* de IPA para avaliação de modelo será baseada nas seguintes fontes de evidências:

a) documentação, conforme descrito na NIT-Sinst-003, em especial:

a.1) memoriais descritivos (de *hardware* e *software*);

a.2) código-fonte das partes legalmente relevantes; e

b) ensaios funcionais.

8.1.1 Ao se iniciar a análise de *software* de IPA, o técnico responsável deverá realizar o estudo preliminar dos memoriais descritivos, manual operacional e código-fonte, de forma a familiarizar-se com o IPA.

8.1.2 Todos os documentos devem fornecer as informações técnicas detalhadas pertinentes à versão atual de cada *software* legalmente relevante do IPA.

8.1.3 Caso seja necessário, o técnico responsável poderá requisitar entrevista com representante do requerente para obter esclarecimentos sobre o funcionamento do *software* e/ou *hardware* do IPA e auxiliar na avaliação de modelo.

	NIT-SINST-026	REV. 01	PÁGINA 5/15
---	----------------------	--------------------	------------------------

8.1.4 O requerente deve fornecer todos os periféricos que se comunicam com o IPA para realização dos ensaios funcionais descritos no Anexo A.

8.2 Métodos de análise

8.2.1 Os métodos de análise de *software* para fins de avaliação de modelo são a seguir relacionados: análise do memorial descritivo (AMD), ensaios funcionais de *software* (EFS), e análise do código-fonte (ACF).

8.2.2 Análise do memorial descritivo (AMD): consiste na leitura e análise do memorial descritivo de *software* e demais documentos fornecidos pelo requerente, e deve ser empregada em todos os casos de avaliação de modelo.

8.2.2.1 O técnico responsável deve verificar se os documentos fornecidos pelo requerente evidenciam o cumprimento dos requisitos do Anexo B da Portaria Inmetro nº 19/2022, e se as soluções tecnológicas empregadas são adequadas para garantir a integridade e segurança da medição e do instrumento em si.

8.2.2.2 Documentação adicional pode ser solicitada ao requerente, caso a análise do memorial descritivo e demais documentos não puder fornecer evidências adequadas do cumprimento dos requisitos do Anexo B da Portaria Inmetro nº 19/2022.

8.2.3 Ensaio funcional de *software* (EFS): consiste na análise do comportamento do *software* do IPA em situações de operação real.

8.2.3.1 O ensaio funcional de *software* deve ser aplicado, quando requerido pelo técnico responsável, para assegurar, ratificar ou respaldar a análise do memorial descritivo.

8.2.3.2 O ensaio funcional de *software* pode auxiliar na verificação do cumprimento dos seguintes requisitos:

- a) versão do *software* legalmente relevante;
- b) correção dos algoritmos e funções;
- c) proteção de *software* e *hardware*;
- d) detecção de falhas;
- e) autenticidade e integridade dos dados de medição;
- f) indicações compartilhadas;
- g) transferência de dados;
- h) carga de *software* legalmente relevante;
- i) carga de *software* não legalmente relevante;
- j) arquiteturas com componentes eletrônicos imutáveis;
- k) arquitetura com utilização de interfaces;
- l) arquiteturas com separação de *software* e/ou *hardware*; e
- m) arquiteturas com assinatura digital.

8.2.3.3 A relação de ensaios funcionais passíveis de serem realizados encontra-se no Anexo A da presente norma.

	NIT-SINST-026	REV. 01	PÁGINA 6/15
---	----------------------	--------------------	------------------------

8.2.3.4 Os procedimentos específicos dos ensaios funcionais de *software* devem tomar por subsídio as informações contidas nos casos de teste, manual operacional, memoriais descritivos e padrão de funcionamento do instrumento e equipamentos de teste.

8.2.3.5 Através da realização de ensaios funcionais de *software*, as características descritas nos memoriais descritivos e manual operacional podem ser verificados em procedimentos práticos.

8.2.3.6 Através do ensaio funcional de *software*, deve ser analisada a operação normal do instrumento.

8.2.3.6.1 Todas as chaves ou teclas e combinações descritas devem ser empregadas e a reação do instrumento avaliada.

8.2.3.6.2 Para interfaces gráficas de usuário, todos os menus e demais elementos gráficos devem ser ativados e avaliados.

8.2.4 Análise de código-fonte (ACF): consiste na leitura, análise e eventual processamento, por *software* especializado, do código-fonte dos componentes com *software* legalmente relevante.

8.2.4.1 O técnico responsável deve analisar o código-fonte, avaliando cada parte do código para determinar se os requisitos do Anexo B da Portaria Inmetro nº 19/2022 são atendidos e se as funções e características do *software* estão em conformidade com a documentação fornecida pelo requerente.

8.2.4.2 O técnico responsável também pode se concentrar em algoritmos e funções que tenha identificado como complexas, sujeitas a erro, insuficientemente documentadas, etc. e inspecionar a respectiva parte do código-fonte através de análise e verificação.

9 REQUISITOS GERAIS DE SOFTWARE E HARDWARE

9.1 Versão do *software* legalmente relevante

9.1.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.2 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

9.1.2 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

9.2 Correção dos algoritmos e funções

9.2.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.3 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

9.2.2 Avaliar na ACF a adequabilidade dos tipos utilizados na captura, armazenamento e processamento dos dados de medição.

9.2.3 A avaliação da exatidão dos algoritmos e funções de medição poderá ser realizada através de ensaios funcionais metrológicos, em uma etapa do processo de AM diferente da avaliação de *software*.

	NIT-SINST-026	REV. 01	PÁGINA 7/15
---	---------------	------------	----------------

9.3 Proteção de *software* e *hardware*

9.3.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.4 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

9.3.2 Deve ser avaliado se, através de alguma interface de comunicação (serial, *ethernet*, etc.), de posse do *software* de comunicação e configuração do requerente, é possível realizar intrusão ou modificações não autorizadas.

9.3.3 Considera-se que, quando da realização de procedimentos de verificação de integridade, a realização em laboratório equivale à realização em campo.

9.3.4 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

9.3.5 O requerente deve fornecer arquivos binários, assim como o procedimento e ferramentas necessárias para carregá-los no instrumento, para serem utilizados nos ensaios funcionais constantes no Anexo A desta norma. Esses arquivos binários devem permitir a realização de ensaios que evidenciem a proteção contra mudanças acidentais.

9.4 Detecção de falhas

9.4.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.5 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

9.4.2 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta Norma.

9.5 Autenticidade e integridade dos dados de medição

9.5.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.6 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

9.5.2 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta Norma.

9.6 Documentação requerida para os requisitos gerais

9.6.1 Deve ser avaliado se a documentação entregue pelo requerente encontra-se completa de acordo com o exigido no item 2.7 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10 REQUISITOS ESPECÍFICOS DE *SOFTWARE* E *HARDWARE*

10.1 Indicações compartilhadas

10.1.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.2 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10.1.2 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta Norma.

	NIT-SINST-026	REV. 01	PÁGINA 8/15
---	---------------	------------	----------------

10.2 Transferência de dados

10.2.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.3 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022

10.2.2 Avaliar o *software* do computador tipo U que verifica dados recebidos por este. Esta avaliação pode ser dispensada caso as seguintes condições sejam satisfeitas simultaneamente:

10.2.2.1 A autenticidade e integridade dos dados transmitidos seja garantida pela utilização da assinatura digital destes dados.

10.2.2.2 A assinatura digital e todos os dados que a compõe sejam publicados juntamente com o resultado final da medição.

10.2.3 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta Norma.

10.3 Carga de *software* legalmente relevante

10.3.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.4 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10.3.2 Para instrumentos que permitam a carga de *software* em campo sem rompimento de lacre, se a assinatura digital for adotada pelo requerente como solução de autorização e autenticação, é necessário que o Inmetro realize procedimento de assinatura digital para validação da versão de *software* aprovada e teste-o antes da finalização do processo de AM.

10.3.3 Com respeito à autenticação do usuário para carga de *software* legalmente relevante, são requisitos mínimos:


- a) uso compulsório de autenticação aprovada segundo a versão mais atual do documento NIST *special publication 800-57 Part 1*;
- b) implementação de comando de protocolo de comunicação que possibilite a alteração da chave (senha) de autenticação, se aplicável; e
- c) implementação de comando de protocolo de comunicação que possibilite habilitar a expiração da chave (senha) de autenticação, se aplicável.

10.3.4 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

10.3.5 O requerente deve fornecer arquivos binários assinados, assim como o procedimento e ferramentas necessárias para carregá-los no instrumento, para serem utilizados nos ensaios funcionais constantes no Anexo A desta norma. Esses arquivos binários devem permitir a realização de ensaios que evidenciem o sucesso e a falha na carga de *software*.

10.4 Carga de *software* não legalmente relevante

10.4.1 O *software* não legalmente relevante não é passível de aprovação conforme indicado no item 3.5.1 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

	NIT-SINST-026	REV. 01	PÁGINA 9/15
---	---------------	------------	----------------

10.4.2 A critério do técnico responsável pela análise do *software* do instrumento, podem ser feitas recomendações de alterações no *software* não legalmente relevante quando forem identificadas características deste que impactem na segurança da medição, na clareza da indicação de informações legalmente relevantes, ou em outros aspectos que julgar relevantes.

10.5 Arquitetura com componentes eletrônicos imutáveis

10.5.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.6 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10.5.2 A documentação detalhada do componente deve ser analisada para constatar sua imutabilidade.

10.5.3 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

10.6 Arquiteturas com utilização de interfaces

10.6.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.7 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10.6.2 Para avaliação de arquiteturas com utilização de interfaces, o código-fonte deve ser analisado de forma a evidenciar se a lista de comandos fornecida pelo requerente corresponde àqueles efetivamente implementados.

10.6.3 Com respeito à alteração de parâmetros legalmente relevantes, são requisitos mínimos:

- a) uso compulsório de autenticação aprovada segundo a versão mais atual do documento NIST *special publication 800-57 Part 1*;
- b) implementação de comando de protocolo de comunicação que possibilite a alteração da chave (senha) de autenticação; e
- c) implementação de comando de protocolo de comunicação que possibilite habilitar a expiração da chave (senha) de autenticação.

10.6.4 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

10.7 Arquiteturas com separação de *software* e/ou *hardware*


10.7.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.8 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10.7.2 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

10.8 Arquiteturas com assinatura digital

10.8.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.9 do Anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

10.8.2 As chaves criptográficas devem ser únicas para cada instrumento.

	NIT-SINST-026	REV. 01	PÁGINA 10/15
---	----------------------	--------------------	-------------------------

10.8.3 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta Norma.

10.9 Documentação requerida para os requisitos específicos

10.9.1 Deve ser avaliado, onde aplicável, se a documentação entregue pelo requerente encontra-se completa de acordo com o exigido no item 3.10 do anexo B do RTM aprovado pela Portaria Inmetro nº 19/2022.

11 DISPOSIÇÕES GERAIS

11.1 A documentação deve evidenciar o ambiente seguro de gestão das chaves criptográficas.

11.2 O requerente deve fornecer *software* e *hardware* necessários para realização dos ensaios funcionais estabelecidos no Anexo A desta norma.

12 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
01	Abr/2022	<ul style="list-style-type: none"> ▪ Atualização dos requisitos da Portaria Inmetro nº 19 de 12/01/2022; e ▪ Adequação ao MOD-Gabin-040 rev. 02.

Quadro de Aprovação		
	Nome	Atribuição
Elaborado por:	Juliana Wilm Guedes	Auxiliar Administrativo
Verificado por:	Rogerio Possidonio Nunes	Pesquisador Tecnologista em Metrologia e Qualidade
	Fabiano de Oliveira Leitão	Pesquisador Tecnologista em Metrologia e Qualidade
Aprovado por:	Roberto Lima do Amaral	Chefe do Sinst

ANEXO A - ENSAIOS FUNCIONAIS DE *SOFTWARE*

Tabela 1 – Ensaios funcionais de *software* baseados nos requisitos do anexo B do RTM da Portaria Inmetro nº 19/2022

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
1	2.2	Versão do <i>software</i> legalmente relevante	Identificador de versão, estrutura e acesso.	Verificar se o identificador de versão existe, como é acessado e se é idêntico ao descrito na documentação. Verificar a estrutura do identificador de versão. Verificar se o identificador apresentado vem precedido da inscrição “Versão do <i>software</i> legalmente relevante”
2	2.3	Correção dos algoritmos e funções	Exatidão metrológica da medição de pesagem.	A ser executado pelo Semas. De acordo com a NIT-Semas-001.
3	2.4	Proteção de <i>software e hardware</i>	<p>Possibilidade de uso impróprio ou fraudulento do instrumento</p> <p>Selagem mecânica. Outros meios de proteção do <i>software e hardware</i> do instrumento.</p> <p>Reação do instrumento a modificações acidentais ou não autorizadas de seu <i>software</i>.</p> <p>Reação do instrumento a modificações acidentais ou não autorizadas de seus parâmetros legalmente relevantes.</p> <p>Influência das partes legalmente relevantes do instrumento por outras partes do sistema de medição.</p> <p>Procedimento de verificação de integridade, sucesso da verificação, falha da verificação.</p>	<p>Explorar eventuais fragilidades com o objetivo de fazer uso fraudulento do instrumento (por exemplo, modificação de parâmetro legalmente relevante sem rompimento de lacre ou autenticação).</p> <p>Verificar se a selagem mecânica protege o instrumento contra modificações não autorizadas de seu <i>software</i> ou parâmetros legalmente relevantes.</p> <p>Verificar se os outros meios de proteção do instrumento (eletrônicos, criptográficos) são robustos e eficazes (de acordo com documentos FIPS NIST) contra modificações não autorizadas de seu <i>software</i> ou parâmetros legalmente relevantes.</p> <p>Simular situações de falha acidental/não autorizada no <i>software</i> do instrumento e observar se a reação está de acordo com o memorial descritivo.</p> <p>Simular situações de falha acidental/não autorizada nos parâmetros legalmente relevantes do instrumento e observar se a reação está de acordo com o memorial descritivo.</p> <p>Verificar se a ferramenta de verificação de integridade atesta como íntegro um <i>firmware</i> íntegro carregado no instrumento/sistema de medição.</p> <p>Verificar se a ferramenta de verificação de integridade atesta como não íntegro um <i>firmware</i> não íntegro carregado no instrumento/sistema de medição.</p>
4	2.5	Detecção de falhas	Reação às falhas descritas e verificação do desempenho do instrumento.	Colocar o instrumento no estado das falhas detectáveis e verificar se as reações contra as mesmas ocorrem do modo descrito no memorial descritivo.

(continua)

5	2.6	Autenticidade e integridade dos dados de medição	<p>Garantia da autenticidade e integridade dos dados de medição ao longo da cadeia legalmente relevante.</p> <p>Reconstrução do resultado de medição.</p> <p>Inclusão do identificador unívoco do veículo (placa) no resultado de medição.</p>	<p>Verificar se os mecanismos que garantem autenticidade e integridade dos dados de medição correspondem àqueles referenciados no memorial descritivo.</p> <p>Verificar como é possível validar a autenticidade e integridade dos dados de medição.</p> <p>Simular situação de falha da autenticidade e integridade dos dados de medição e observar se a reação do instrumento está de acordo com o memorial descritivo.</p> <p>Verificar como é feita a reconstrução do resultado de medição.</p> <p>Simular situação de falha na reconstrução do resultado de medição e observar se a reação do instrumento ou <i>software</i> específico está de acordo com o memorial descritivo.</p> <p>Verificar se a placa do veículo é incluída no resultado de medição. A inserção da placa do veículo pode se dar pela ação do operador do instrumento diretamente no computador tipo U.</p>
6	3.2	Indicações compartilhadas	<p>Garantia da clareza da informação legalmente relevante.</p> <p>Arquitetura do instrumento.</p> <p>Operação do <i>software</i> que realiza a indicação da informação legalmente relevante.</p>	<p>Verificar se a indicação das informações legalmente relevantes, especialmente o resultado da pesagem, pode ser confundida com outras informações não legalmente relevantes.</p> <p>Avaliar a arquitetura do instrumento. Possui separação de <i>software/hardware</i>? Arquiteturas que fazem uso de <i>hardware</i> específico (tipo P), computador universal (tipo U) e que usam assinatura digital para assegurar autenticidade e integridade dos dados são consideradas como tendo separação de <i>software/hardware</i>.</p> <p>Avaliar o comportamento do <i>software</i> que realiza a indicação da informação legalmente relevante, caso o instrumento possua separação de <i>software/hardware</i>. Este <i>software</i> deve indicar apenas resultados de medição que tenham tido sua autenticidade e integridade previamente verificadas. Este <i>software</i> deve atender ainda às exigências do item 3.2.4 do Anexo B do RTM.</p>
7	3.3	Transferência de dados	<p>Garantia da autenticidade, integridade e carimbo de tempo dos dados transferidos</p> <p>Atrasos de transferência</p> <p>Carimbo de tempo</p>	<p>Verificar se os mecanismos que garantem autenticidade, integridade e carimbo de tempo dos dados transmitidos correspondem àqueles referenciados no memorial descritivo.</p> <p>Verificar se os dados transmitidos têm sua autenticidade e integridade checadas após a recepção.</p> <p>Simular situação de falha da autenticidade e integridade dos dados transmitidos e observar o descarte destes dados.</p> <p>Simular situação de atraso de transferência e verificar se o resultado de medição é influenciado.</p> <p>No caso de indisponibilidade dos sistemas de transferência de dados, verificar: a) se os dados de medição são mantidos; b) se o processo de medição é interrompido para impedir a perda de dados, caso estes não sejam armazenados; c) se uma sinalização é ativada.</p> <p>Verificar a transmissão dos dados armazenados quando do restabelecimento dos sistemas de transferência após uma interrupção.</p> <p>Verificar se o carimbo de tempo é obtido conforme apresentado no memorial descritivo.</p>

(continua)

8	3.4	Carga de <i>software</i> legalmente relevante	<p>Aprovação do <i>software</i> pelo Inmetro</p> <p>Automação da carga de <i>software</i></p> <p>Comportamento do instrumento durante e ao final da carga de <i>software</i></p> <p>Autenticação de usuário para efetuar carga de <i>software</i></p> <p>Garantia da autenticidade e integridade do <i>software</i> a ser carregado</p> <p>Registro de auditoria da carga de <i>software</i></p>	<p>Verificar se os mecanismos que garantem que o <i>software</i> tenha sido aprovado pelo Inmetro correspondem àqueles referenciados no memorial descritivo.</p> <p>Verificar se a carga de <i>software</i> é automática, ou seja, uma vez iniciada independe do operador.</p> <p>Verificar se o instrumento realiza medições durante o processo de carga de <i>software</i>.</p> <p>Verificar se, após a carga de <i>software</i>, o ambiente de proteção retorna ao mesmo nível de segurança declarado no processo de avaliação de modelo.</p> <p>Atestar a existência de autenticação de usuário para realização da carga de <i>software</i>. Esta autenticação deve atender às exigências do item 9.3.3 desta norma.</p> <p>Verificar se os mecanismos que garantem a autenticidade e a integridade do <i>software</i> correspondem àqueles referenciados no memorial descritivo.</p> <p>Simular situação de falha da autenticidade e integridade do <i>software</i> a ser carregado e observar seu descarte e uso da versão da anterior. Alternativamente, o instrumento pode tornar-se inoperante.</p> <p>Verificar se a carga de <i>software</i> ocorre apenas quando há abertura de proteção física ou acesso autenticado.</p> <p>Verificar se há registro da carga de <i>software</i>. O registro de auditoria da carga de <i>software</i> deve armazenar, no mínimo, as seguintes informações: a) identificação do nível de acesso do responsável pela carga; b) data e hora da carga; c) sucesso ou insucesso da carga; d) versões anterior e posterior à carga.</p> <p>Verificar se os registros de auditoria são armazenados por, no mínimo, 5 (cinco) anos.</p> <p>Verificar a disponibilização dos registros de auditoria para leitura.</p>
9	3.6	Arquiteturas com componentes eletrônicos imutáveis	<p>Imutabilidade de componentes eletrônicos</p>	<p>A critério do técnico responsável pela avaliação de modelo, podem ser efetuados testes complementares que comprovem a imutabilidade de componente eletrônico responsável por processamento de informação legalmente relevante.</p>

(continua)

10	3.7	Arquitetura com utilização de interfaces	<p>Proteção do instrumento</p> <p>Funções ativadas pela interface</p> <p>Alteração de parâmetros legalmente relevantes</p> <p>Registro de auditoria de alteração de parâmetros legalmente relevantes</p> <p>Leitura de parâmetros legalmente relevantes em uso no instrumento</p>	<p>Verificar se os meios técnicos utilizados para proteger partes do instrumento correspondem àqueles referenciados no memorial descritivo.</p> <p>Verificar se apenas as funções documentadas podem ser ativadas pelas interfaces de comunicação e de usuário.</p> <p>Verificar se as funções de interface permitem o uso fraudulento do instrumento.</p> <p>Verificar se o procedimento de alteração de parâmetros legalmente relevantes somente pode ser executado após autorização do usuário e se este procedimento se dá conforme apresentado no memorial descritivo.</p> <p>Verificar se a alteração de parâmetros ocorre apenas quando há abertura de proteção física ou acesso autenticado.</p> <p>Verificar se há registro de alterações de parâmetros. O registro de auditoria deve armazenar, no mínimo, as seguintes informações: a) identificação do nível de acesso do responsável pela alteração; b) data e hora da alteração; c) tipo do parâmetro alterado; d) valores anterior e posterior à alteração.</p> <p>Verificar se os registros de auditoria são armazenados por, no mínimo, 5 (cinco) anos.</p> <p>Verificar a disponibilização dos registros de auditoria para leitura.</p> <p>Verificar a disponibilização dos valores atuais dos parâmetros legalmente relevantes para leitura.</p> <p>Verificar a inviolabilidade dos componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes.</p>
11	3.8	Arquiteturas com separação de <i>software</i> e/ou <i>hardware</i>	<p>Identificação das partes legalmente relevantes e não legalmente relevantes</p> <p>Comunicação entre as partes legalmente relevantes e não legalmente relevantes</p> <p>Influência das partes legalmente relevantes</p> <p>Comportamento da medição</p>	<p>Verificar se a distribuição física das partes legalmente relevantes e não legalmente relevantes está de acordo com o memorial descritivo.</p> <p>Verificar se todas as comunicações entre as partes legalmente relevantes e não legalmente relevantes são realizadas exclusivamente através da interface de separação de <i>software</i> e/ou <i>hardware</i>.</p> <p>Verificar se há correspondência unívoca e não ambígua entre cada comando emitido via interface e cada função iniciada ou alteração de dados realizada na parte legalmente relevante.</p> <p>Verificar a completude dos comandos emitidos via interface.</p> <p>Verificar a influência das partes legalmente relevantes por comandos não documentados recebidos através da interface de separação de <i>software</i> e/ou <i>hardware</i>.</p> <p>Verificar se a medição é comprometida por atrasos ou bloqueios ocorridos pela realização de outras tarefas.</p>

(continua)



12	3.9	Arquiteturas com assinatura digital	Ferramentas fornecidas pelo requerente Armazenamento de dados Gestão de chaves criptográficas	Verificar a ferramenta de publicação e conferência dos dados assinados. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação. Simular situação de falha na chave pública e verificar se a ferramenta indica tal situação. Verificar a ferramenta de reconstituição do valor final da medição a partir dos dados assinados. Simular situação de falha nos dados assinados e verificar se a ferramenta indica tal situação. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação. Verificar se os dados ou valores assinados, juntamente com a respectiva assinatura digital, são armazenados por, no mínimo, 60 dias. Verificar se as chaves criptográficas privadas são mantidas secretas e seguras internamente ao instrumento.
----	-----	-------------------------------------	---	---

Fonte: Dimel/Disme/Sinst