SUMÁRIO

1 OBJETIVO

Esta norma estabelece os procedimentos a serem utilizados na análise de software para apreciação de modelo de bombas medidoras de combustíveis líquidos.

2 CAMPO DE APLICAÇÃO

Esta norma aplica-se aos laboratórios nela designados e/ou acreditados e à Dimel/Disme/Sinst.

3 RESPONSABILIDADE

A responsabilidade pela aprovação, revisão e cancelamento desta Norma é da Dimel/Disme/Sinst.

4 DOCUMENTOS DE REFERÊNCIA

Portaria Inmetro n.° 559/2016	Aprovar o Regulamento Técnico Metrológico (RTM) estabelecendo os requisitos técnicos, metrológicos e de segurança de software e hardware aplicáveis às bombas medidoras de combustíveis líquidos utilizadas nas medições de volume
Portaria Inmetro n.° 150/2016	Adotar, no Brasil, o Vocabulário Internacional de Termos de Metrologia Legal (VIML), em anexo, baseado no documento OIML V1, edição 2013, com a devida tradução ao nosso idioma, e o Anexo de notas da versão brasileira do VIML
OIML D 31:2008	*General requirements for software controlled measuring instruments, Edition 2008 (E)*
WELMEC Software Guide 7.2 2015	*Measuring Instruments Directive 2014/32/EU – WELMEC, 2015*
NIST Special Publication 800-57 Part 1 Revision 4	*Recommendation for Key Management – Part 1: General*

5 DOCUMENTOS COMPLEMENTARES

NIT-Sinst-003	Organização da documentação para o processo de avaliação de software
NIT-Sinst-020	Requisitos do protocolo de comunicação serial para verificação de integridade de software em instrumentos de medição

6 DEFINIÇÕES

6.1 Siglas

As siglas das UP/UO do Inmetro podem ser acessadas em: http://intranet.inmetro.gov.br/tema/qualidade/docs/pdf/siglas-inmetro.pdf.

EFS	Ensaio Funcional de Software
AMD	Análise do Memorial Descritivo
ACF	Análise do Código Fonte
NIST	*National Institute of Standards and Technology*
OS	Sistema Operacional

6.2 Termos

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

6.2.2 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.

6.2.3 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
d) executam carga de software legalmente relevante.

6.2.4 Memorial Descritivo – documento que descreve detalhadamente as implementações tecnológicas para atender os requisitos de segurança de hardware e software.

6.2.5 Não Legalmente Relevante – Todo software/hardware/dados presentes no instrumento que não são legalmente relevantes.

6.2.6 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.

6.2.7 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.

6.2.8 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.

7 ORIENTAÇÕES GERAIS

7.1 A análise de software de bombas medidoras de combustíveis líquidos para apreciação 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); e
  a.2) código-fonte das partes legalmente relevantes;
b) Ensaios funcionais.

7.1.1 Ao se iniciar a análise de software de bombas medidoras de combustíveis líquidos, o técnico responsável deverá realizar o estudo preliminar dos memoriais descritivos, manual operacional e código-fonte, de forma a familiarizar-se com o instrumento.

7.1.2 Caso seja necessário, o técnico responsável poderá requisitar entrevista com representante do fabricante para obter esclarecimentos sobre o funcionamento do software e/ou hardware da bomba medidora de combustíveis líquidos, dirimir dúvidas e auxiliar na realização de ensaios funcionais.

7.1.3 O fabricante deve fornecer todos os periféricos que se comunicam com a bomba medidora de combustíveis líquidos para realização dos ensaios funcionais descritos no Anexo A.

7.1.4 A análise das fontes de evidências do cumprimento dos requisitos exigidos pelo RTM aprovado pela Portaria Inmetro n.º 559/2016 deverá ser registrada em relatório apropriado.

7.2 Métodos de Análise

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

7.2.2 Análise do memorial descritivo (AMD): consiste na leitura e análise dos memoriais descritivos e demais documentos fornecidos pelo fabricante, e deve ser empregada em todos os casos de apreciação técnica de modelo.

7.2.2.1 O técnico responsável deve verificar se os documentos fornecidos pelo fabricante evidenciam o cumprimento dos requisitos da Portaria Inmetro n.º 559/2016, e se as soluções tecnológicas empregadas são adequadas para garantir a integridade, autenticidade e segurança da medição e do instrumento em si.

7.2.2.2 Documentação adicional pode ser requerida ao fabricante caso a análise do memorial descritivo e demais documentos não puder fornecer evidências adequadas do cumprimento dos requisitos da Portaria Inmetro n.º 559/2016.

7.2.2.3 As soluções tecnológicas adotadas para o cumprimento dos requisitos da Portaria Inmetro n.º 559/2016 e o resultado da avaliação devem ser registrados em relatório apropriado.

7.2.3 Ensaio funcional de software (EFS): consiste na análise do comportamento do software da bomba medidora de combustíveis líquidos em situações de operação real.

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

7.2.3.2 O ensaio funcional de software pode auxiliar na verificação do cumprimento da totalidade dos requisitos do Anexo B do RTM aprovado pela Portaria Inmetro n.° 559/2016.

7.2.3.3 A relação de ensaios funcionais possíveis de serem realizados encontra-se no Anexo A.

7.2.3.4 Os procedimentos específicos dos ensaios funcionais de software devem tomar por subsídio as informações contidas no manual operacional, memoriais descritivos e padrão de funcionamento do instrumento e equipamentos auxiliares.

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

7.2.3.6 Através do ensaio funcional de software, deve ser analisada a operação normal do instrumento. Todas as chaves ou teclas de interface de usuário descritas devem ser empregadas e a reação do instrumento/sistema avaliada. Para interfaces gráficas de usuário, todos os menus e demais elementos gráficos devem ser ativados e avaliados.

7.2.3.7 O resultado dos ensaios funcionais deve ser registado em relatório apropriado.

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

7.2.4.1 O técnico responsável deve analisar o código fonte, avaliando cada parte do código para determinar se os requisitos da Portaria Inmetro n.º 559/2016 são atendidos e se as funções e características do software estão em conformidade com a documentação fornecida pelo fabricante.

7.2.4.2 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.

7.2.4.3 O resultado da avaliação de código-fonte deve ser registado em relatório apropriado.

8 REQUISITOS GERAIS

8.1 Versão do Software Legalmente Relevante

a) deve ser avaliado se o software legalmente relevante dos dispositivos transdutor e indicador possuem versões que os identifiquem univocamente; e
b) deve ser avaliado se as versões do software legalmente relevante são apresentadas por comandos das interfaces de usuário e de verificação metrológica.

8.2 Proteção de Software e Hardware

a) deve ser avaliado se alguma característica de projeto e construção do instrumento, evidenciada por seu software e hardware, possibilitam o uso impróprio ou fraudulento do instrumento;
b) deve ser avaliado se as proteções do instrumento garantem que intervenções no mesmo sejam evitadas e, caso aconteçam, evidenciadas;
c) deve ser avaliado se partes legalmente relevantes do instrumento, quer sejam de software ou de hardware, podem ser inadmissivelmente influenciadas por outras partes do instrumento;
d) deve ser avaliado se o software e os parâmetros legalmente relevantes são protegidos contra alterações inadmissíveis ou não autorizadas, carga de software não autorizada e modificações causadas pela troca indevida de unidades de memória;
e) deve ser avaliado se há meios técnicos adicionais de proteção, em complementação à selagem mecânica, para proteger partes do instrumento que possuam sistema operacional embarcado, interfaces de comunicação ou opção de carga de software;
f) deve ser avaliado se somente funções claramente documentadas podem ser ativadas pelas interfaces de usuário, de verificação metrológica e de comunicação, e se sua concepção impedem o uso fraudulento ou impróprio do instrumento;
g) deve ser avaliado se os parâmetros que definem características metrológicas do instrumento são armazenados de forma segura, protegidos contra intrusão e modificações indevidas, podendo ser alterados somente mediante procedimento documentado pelo fabricante;
h) deve ser avaliado se o Registro de Alteração de Parâmetros Metrológicos Relevantes segue o disposto no item 3.3.8 ao item 3.3.14 do Anexo A do RTM aprovado pela Portaria Inmetro n.º 559/2016;
i) deve ser avaliado se os componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes sejam física e logicamente invioláveis; e
j) deve ser avaliado se o dispositivo transdutor do instrumento é inviolável, não sendo permitido o acesso físico, ou lógico indevido, ao seu interior.

8.3 Detecção de Falhas

a) deve ser avaliado se o instrumento possui funções de detecção de falhas, a critério do fabricante, mediante implementações de software e/ou hardware;
b) deve ser avaliado se, no caso da ocorrência de falhas, o instrumento reage conforme descrito em seu manual operacional;
c) deve ser avaliado, se aplicável e possível, se o instrumento interrompe o funcionamento caso seja constatada diferença na indicação de volume de combustível, acima do especificado pelo fabricante, entre a medição realizada pelo dispositivo transdutor e o valor registrado pelo dispositivo controlador;
d) deve ser avaliado se o instrumento interrompe o funcionamento caso sejam detectadas tentativas de acesso não autorizadas no instrumento, tanto por meios físicos como por meios lógicos;

e) deve ser avaliado se em caso de interrupção do funcionamento do instrumento devido a algum dos motivos elencados no item 3.4.3 do Anexo A do RTM aprovado pela Portaria Inmetro 559/2016, uma mensagem de erro é exibida no dispositivo indicador até que seja realizada uma operação de manutenção pelo responsável autorizado pelo órgão metrológico;
f) deve ser avaliado se o Registro de Interrupções de Funcionamento segue o disposto no item 3.4.5 ao item 3.4.6 do Anexo A do RTM aprovado pela Portaria Inmetro n.º 559/2016; e
g) Deve ser avaliado se o Registro de Eventos de Manutenção segue o disposto do item 3.4.7 ao item 3.4.8 do Anexo A do RTM aprovado pela Portaria Inmetro n.º 559/2016.

8.4 Comunicação entre Dispositivos de Hardware da Bomba Medidora

a) deve ser avaliado se a comunicação realizada entre o dispositivo transdutor e o dispositivo controlador da bomba medidora de combustível é realizada através de protocolo de comunicação e, adicionalmente, outros modos de comunicação;
b) a especificação do protocolo utilizado deve ser fornecida para avaliação;
c) deve ser verificado se o dispositivo transdutor armazena internamente um identificador unívoco que o permita referenciá-lo sem ambiguidade, e se este identificador é protegido contra alterações de qualquer natureza;
d) deve ser verificado se o dispositivo transdutor armazena par de chaves criptográficas assimétricas para realização de assinatura digital, utilizando circuito integrado aprovado pelo Inmetro;
e) deve ser verificado como é garantido que não haja geração e utilização de pares de chaves criptográficas idênticos em dispositivos de um mesmo fabricante;
f) deve ser verificado como a chave privada do dispositivo transdutor é armazenada de modo inviolável e inextricável do meio físico e lógico e que garantias são fornecidas para este armazenamento seguro;
g) deve ser analisado se os identificadores únicos e chaves públicas dos dispositivos transdutores são armazenados nos dispositivos controlador e indicador;
h) deve ser verificado se, antes de cada abastecimento, o dispositivo controlador verifica o identificador unívoco e a chave pública do dispositivo transdutor;
i) deve ser verificado se, em caso de falha na verificação da condição do item 8.4 h), o funcionamento do dispositivo transdutor correspondente é impedido;
j) deve ser verificado se o evento a que se refere o item 8.4 i) é armazenado no Registro de Interrupções de Funcionamento do instrumento;
k) deve ser verificado se o registro armazenado a que se refere o item 8.4 j) possui: identificação do tipo de evento que gerou a interrupção do funcionamento do instrumento, identificador unívoco do dispositivo associado à falha e data e hora da falha;
l) deve ser verificado se a operação de manutenção para sanar a falha descrita no item 8.4 i) é armazenada no Registro de Eventos de Manutenção;
m) deve ser verificado se o registro armazenado a que se refere o item 8.4 l) possui: identificação do nível de acesso do responsável pela manutenção do instrumento, resultado da operação de manutenção, identificação do dispositivo ou parte da bomba medidora que foi alvo da manutenção e data e hora da operação;
n) deve ser verificado se, ao final de cada abastecimento e na interrupção de fluxo de combustível, o dispositivo transdutor envia ao dispositivo controlador as informações de totalização da medição em um pacote de dados assinado digitalmente com a chave privada do dispositivo transdutor;
o) deve ser verificado se o pacote de dados a que se refere o item 8.4 n) possui, pelo menos, as seguintes informações: identificação unívoca do dispositivo transdutor, identificação unívoca do dispositivo controlador, identificador unívoco do abastecimento, quantidade de pulsos e/ou informação de medição de volume do abastecimento registrado pelo dispositivo transdutor, constante de calibração do dispositivo

transdutor, volume abastecido total calculado pelo dispositivo transdutor, valor monetário total da transação, preço por litro do combustível, data e hora do abastecimento;
p) deve ser verificado se o pacote de dados a que se refere o item 8.4 o) é assinado digitalmente pela chave privada do dispositivo transdutor e se a assinatura digital pode ser conferida pela chave pública correspondente;
q) deve ser verificado se, na instalação de um novo dispositivo transdutor no instrumento, o dispositivo controlador o habilita e verifica sua identidade;
r) deve ser verificado se, ao final do abastecimento, o dispositivo indicador apresenta as informações de volume abastecido, valor monetário da transação e preço por litro do combustível;
s) deve ser verificado se, ao final do abastecimento, o dispositivo indicador apresenta a informação de que a assinatura digital do pacote de dados a que se refere o item 8.4 o) é conferida e o resultado desta conferência;
t) deve ser verificado se, em caso de falha na conferência da assinatura digital do pacote de dados a que se refere o item 8.4 o), o funcionamento do dispositivo transdutor é impedido e uma mensagem de erro é apresentada no dispositivo indicador;
u) deve ser verificado se o evento a que se refere o item 8.4 t) é armazenado no Registro de Interrupções de Funcionamento do Instrumento;
v) deve ser verificado se o registro armazenado a que se refere o item 8.4 u) possui: identificação do tipo de evento que gerou a interrupção do funcionamento do instrumento, identificador unívoco do dispositivo transdutor associado à falha e data e hora do evento;
w) deve ser verificado se a operação de manutenção para sanar a falha descrita no item 8.4 t) é armazenada no Registro de Eventos de Manutenção;
x) deve ser verificado se o registro armazenado a que se refere o item 8.4 w) possui: identificação do nível de acesso do responsável pela manutenção do instrumento, resultado da operação de manutenção, identificação do dispositivo ou parte da bomba medidora que foi alvo da manutenção e data e hora da operação;
y) deve ser verificado se a comunicação do instrumento com equipamentos auxiliares, não constantes da Portaria de Aprovação de Modelo, só pode ser realizada mediante interface de comunicação própria e dedicada a este fim, cujo ponto de acesso deve estar disponível fora da área selada do instrumento;
z) deve ser verificado se há conexões de equipamentos auxiliares, não constantes na Portaria de Aprovação de Modelo, diretamente nas placas eletrônicas do dispositivos transdutor, controlador ou indicador;
aa) deve ser verificado se as interfaces de comunicação do instrumento com equipamentos auxiliares externos são protegidas contra tentativas de acesso não autorizados ou indevidos ao instrumento; e
ab) deve ser verificado se comandos dos protocolos de interface de comunicação com equipamentos externos podem alterar parâmetros, dados ou software legalmente relevante de forma diferente daquela declarada pelo fabricante.

8.5 Verificação de Integridade de Software

a) Deve ser verificado se está disponível uma interface de verificação metrológica no dispositivo controlador, padrão *Bluetooth*, especificada na Norma NIT-Sinst-020, que possibilite o acesso ao registro de alterações de parâmetros metrológicos relevantes, registro de interrupções de funcionamento do instrumento, registro de eventos de manutenção e registro de cargas de software, acesso ao pacote de dados do último abastecimento de cada dispositivo transdutor, assinado digitalmente, sua correspondente chave pública e a assinatura digital desta chave fornecida pelo Inmetro;
b) Deve ser verificado se é possível realizar a execução do procedimento de verificação de integridade, conforme Norma NIT-Sinst-020, do software dos dispositivos transdutores e indicadores;

c) Deve ser verificado se o nome do dispositivo *Bluetooth* da interface de verificação metrológica está afixado em área visível sobre a superfície do instrumento, conforme descrito no item 7 (Inscrições Obrigatórias) da Portaria Inmetro 559/2016; e
d) Deve ser verificado se o emparelhamento da interface de verificação metrológica é possível a qualquer momento a partir do início da operação de abastecimento.

9 REQUISITOS ESPECÍFICOS

9.1 Os requisitos específicos só devem ser avaliados quando de sua implementação no instrumento, que não é compulsória, mas sim uma escolha de projeto e arquitetura realizada pelo fabricante.

9.2 Separação de Software

a) deve ser verificado se todos os módulos de software e hardware dos dispositivos transdutor e indicador, que realizem tarefas legalmente relevantes, são corretamente identificados como partes legalmente relevantes do instrumento;
b) deve ser verificado se partes legalmente relevantes do hardware ou software do instrumento podem ser inadmissivelmente influenciadas por comandos recebidos através de interfaces de comunicação ou de partes não legalmente relevantes do instrumento;
c) deve ser verificado se todo comando emitido por uma interface (de usuário, de verificação metrológica, de comunicação ou de separação de software e/ou hardware) possui uma correspondência unívoca e não ambígua com respectiva função iniciada no software legalmente relevante ou alteração de dados realizada na parte legalmente relevante;
d) deve ser identificada e verificada a existência de uma interface de separação de software e/ou hardware que realize a comunicação entre a parte legalmente relevante e a parte não legalmente relevante;
e) deve ser verificada a existência de declaração de completude de comandos da interface de separação de software; e
f) deve ser verificado se atrasos ou bloqueios resultantes da realização de tarefas não legalmente relevantes pode implicar no comprometimento do resultado da medição.

9.3 Armazenamento e Transmissão de Dados em Meio Inseguro

a) deve ser verificado se os dados legalmente relevantes têm sua autenticidade e integridade garantidas;
b) deve ser verificado se, no caso do uso de assinatura digital para garantia de autenticidade e integridade, esta assinatura é verificada pelo software ou hardware responsável pela sua publicação ou processamento;
c) deve ser verificado se, no caso de sucesso na verificação da assinatura digital, os dados de medição são corretamente utilizados;
d) deve ser verificado se, no caso de falha na verificação da assinatura digital, os dados de medição são descartados; e
e) deve ser verificado se as chaves criptográficas privadas empregadas são mantidas secretas e seguras internamente ao instrumento.

9.4 Carga de Software Legalmente Relevante

a) deve ser verificado se somente software legalmente relevante submetido pelo requerente e aprovado no processo de avaliação de modelo pode ser carregado no instrumento;

b) deve ser verificado se, durante a carga de software legalmente relevante, o instrumento para de realizar medições;
c) deve ser verificado se ao final do procedimento de carga e instalação de software legalmente relevante, o ambiente de proteção retorna ao mesmo nível de segurança declarado no processo de avaliação de modelo;
d) deve ser verificado se os meios técnicos para garantir a autenticidade e integridade do software a ser carregado são adequados;
e) deve ser verificado se a autenticidade ou integridade do novo software não puder ser verificada, o instrumento o descarta, utiliza a versão anterior ou torna-se inoperante;
f) deve ser verificado se a carga e a tentativa de carga de software implicam no rompimento de lacres físicos, bem como no registro desta ação em memória não volátil (registro de carga de software); e
g) deve ser verificado se o registro a que se refere o item 9.4 f) contém: identificação do nível de acesso do responsável pela carga, data e hora da carga, sucesso ou insucesso da carga e as versões do software anterior e posterior à carga.

9.5 Carga de Software Não Legalmente Relevante

a) deve ser verificado se a carga de software não legalmente relevante pode ser realizada sem necessidade de aprovação pelo Inmetro, ou seja, sem um certificado digital, válido ou inválido.

9.6 Disposições Gerais

a) deve ser verificado se ao dispositivo transdutor a manutenção, sem clara violação física ou lógica, não é permitida;
b) deve ser verificado se o software legalmente relevante avaliado e aprovado tem sua versão e *hash* do arquivo de firmware registrados e identificados na Portaria de Aprovação de Modelo; e
c) deve ser verificado como o fabricante assegura o ambiente seguro de gestão das chaves criptográficas dos dispositivos transdutores.

10 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
00	Abr/2019	▪ Emissão Inicial.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Marcos Trevisan Vasconcellos	Pesquisador-Tecnologista em Metrologia e Qualidade
Verificado por:	Carlos Eduardo Cardoso Galhardo Juliana Wilm Guedes	Pesquisador-Tecnologista em Metrologia e Qualidade Assistente Administrativo
Aprovado por:	Bruno Erthal de Abreu	Chefe do Sinst

/ANEXO A

ANEXO A – ENSAIOS FUNCIONAIS DE SOFTWARE

#	Item da norma	Requisito	Características Analisadas	Descrição do Ensaio
1	8.1	Versão do software legalmente relevante	Identificação, apresentação.	1. Executar procedimento documentado pelo fabricante para apresentação das versões do software legalmente relevante dos dispositivos transdutor e indicador. 2. Verificar se as versões do software legalmente relevante apresentadas pelo instrumento correspondem àquelas em avaliação de modelo pelo Inmetro.
2	8.2a	Proteção de software e hardware	Uso impróprio ou fraudulento.	1. Identificar características de projeto e construção do instrumento que possibilitem seu uso impróprio ou fraudulento. 2. Identificar funcionalidades do instrumento que possibilitem a manipulação indevida da quantidade de combustível abastecido ou sua apresentação no dispositivo indicador.
3	8.2b	Proteção do instrumento	Evitar ou evidenciar intervenções	1. Verificar se as proteções do instrumento evitam ou, caso aconteça, evidenciam intervenções. 2. Verificar se os pontos e modos de lacração impedem a manipulação indevida do instrumento. 3. Verificar se pequenas intervenções possibilitam manipulação indevida do instrumento.
4	8.2c	Proteção de software e hardware	Influência de partes do instrumento	1. Verificar se a parte legalmente relevante do instrumento pode ser negativamente influenciada por outra parte do instrumento. 2. Verificar se, durante o abastecimento, é possível intervir em características não legalmente relevantes do instrumento de forma a manipular indevidamente o abastecimento em si ou sua exibição no dispositivo indicador.
5	8.2d	Proteção de software e hardware	Proteção contra alterações inadmissíveis, troca indevida de unidades de memória.	1. Verificar se o software e os parâmetros legalmente relevantes são protegidos contra alterações inadmissíveis ou não autorizadas. 2. Verificar se é necessário que um usuário se autentique para realizar a alteração de parâmetros legalmente relevantes. 3. Verificar se a forma de autenticação para alteração de parâmetros é resistente a códigos plausíveis e à força bruta por busca exaustiva. 4. Verificar o uso de dispositivo de bloqueio em caso de falhas de autenticação repetidas. 5. Verificar se o software e os parâmetros legalmente relevantes são protegidos contra carga de software não autorizada. 6. Verificar se o software e os parâmetros legalmente relevantes são protegidos contra alterações causadas pela troca ou adulteração física indevida de unidades de memória.

(Continua)

6	8.2e	Proteção de software e hardware	Proteção além da selagem mecânica.	1. Verificar se, em complementação à selagem mecânica, outros meios técnicos de proteção são utilizados para proteger partes do instrumento que possuam sistema operacional embarcado, interfaces de comunicação ou opção de carga de software. 2. Verificar a existência de selos ou dispositivos digitais de proteção, autenticação ou bloqueio de acessos indevidos. 3. Verificar o uso de assinatura digital para proteção contra cargas de software indevidas. 4. Verificar o uso de senha forte (resistente a ataque de força bruta) para alteração de parâmetros legalmente relevantes (constante de calibração, razões de transformação de corrente e tensão, data e hora, calendário).
7	8.2f	Proteção de software e hardware	Proteção das funções	1. Verificar se somente funções claramente documentadas podem ser ativadas pelas interfaces de usuário, de verificação metrológica e de comunicação. 2. Verificar se a concepção das funções documentadas do instrumento impedem seu uso fraudulento ou impróprio [por exemplo, alterar o dado do totalizador de volume (encerrante) pode ensejar uma ação fraudulenta].
8	8.2g	Proteção de software e hardware	Proteção dos parâmetros	1. Verificar se os parâmetros que definem características metrológicas do instrumento são armazenados de forma segura, protegidos contra intrusão e modificações indevidas. 2. Verificar se os parâmetros que definem características metrológicas do instrumento podem ser alterados somente mediante procedimento documentado pelo fabricante. 3. No caso de uso de senha para proteção de parâmetros legalmente relevantes, verificar se ela é forte contra o ataque de força bruta.

(Continua)

9	8.2h	Proteção de software e hardware	Registro de alteração de parâmetros	1. Verificar se o Registro de Alteração de Parâmetros Metrológicos Relevantes segue o disposto no item 3.3.8 ao item 3.3.14 do Anexo A do RTM aprovado pela Portaria Inmetro 559/2016. 2. Verificar se a alteração de parâmetros implica no rompimento de lacres físicos. 3. Realizar a alteração de um parâmetro legalmente relevante. 4. Utilizar um dispositivo adequado de leitura para verificar se a alteração é armazenada no Registro de Alteração de Parâmetros Metrológicos Relevantes. 5. Verificar se todas as informações especificadas no item 3.3.9 do RTM aprovado pela Portaria Inmetro 559/2016 são armazenadas corretamente. 6. Realizar novas alterações de parâmetros legalmente relevantes e verificar se o armazenamento no Registro de Alteração de Parâmetros Metrológicos Relevantes ocorre em ordem cronológica indexada por um índice monotonicamente crescente. 7. Alterar a data do instrumento para 4 anos e 11 meses adiante no futuro, realizar mais uma alteração de parâmetros legalmente relevantes e verificar se as alterações realizadas anteriormente neste ensaio são mantidas.
10	8.2i	Proteção de software e hardware	Segurança dos componentes que armazenam registros de auditoria	1. Verificar se os componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes são física e logicamente invioláveis. 2. Verificar se é possível remover, adulterar, trocar ou substituir os componentes que armazenam registros de auditoria.
11	8.2j	Proteção de software e hardware	Segurança do dispositivo transdutor	1. Verificar se o dispositivo transdutor do instrumento é inviolável e se o acesso indevido ao seu interior, físico ou lógico, não é permitido.
12	8.3a	Detecção de falhas	Existência de detecção de falhas	1. Verificar se o instrumento possui funções de detecção de falhas. 2. A função de detecção de falhas deve ser descrita na documentação apresentada.
13	8.3b	Detecção de falhas	Reação às falhas	1. Verificar se o instrumento reage às falhas conforme o fabricante descreve no manual operacional. 2. Selecionar de uma a três falhas factíveis de serem provocadas e verificar se a reação do instrumento ocorre conforme descrito em seu manual operacional.

(Continua)

14	8.3c	Detecção de falhas	Diferença de medição	1. Verificar, se aplicável, se o instrumento interrompe o funcionamento caso seja constatada diferença na indicação de volume de combustível, acima do especificado pelo fabricante, entre a medição realizada pelo dispositivo transdutor e o valor registrado pelo dispositivo controlador. 2. O procedimento descrito em (1) só é aplicável se tanto dispositivo transdutor quanto dispositivo calculador totalizaram sinais de modulação pulsada.
15	8.3d	Detecção de falhas	Acesso não autorizado	1. Verificar se o instrumento interrompe o funcionamento caso sejam detectadas tentativas de acesso não autorizadas no instrumento, tanto por meios físicos como por meios lógicos. 2. Realizar o ensaio simulando repetidas tentativas fracassadas de acesso até a interrupção de funcionamento do instrumento.
16	8.3e	Detecção de falhas	Interrupção do funcionamento	1. Verificar se em caso de interrupção do funcionamento do instrumento devido a algum dos motivos elencados no item 3.4.3 do Anexo A do RTM aprovado pela Portaria Inmetro 559/2016, uma mensagem de erro é ser exibida no dispositivo indicador até que seja realizada uma operação de manutenção.
17	8.3f	Detecção de falhas	Registro de interrupções de funcionamento	1. Verificar se o Registro de Interrupções de Funcionamento segue o disposto no item 3.4.5 ao item 3.4.6 do Anexo A do RTM aprovado pela Portaria Inmetro 559/2016. 2. Utilizar um dispositivo adequado de leitura para verificar se o evento que causou a interrupção é armazenado no Registro de Interrupções de Funcionamento do instrumento. 3. Realizar novas intervenções que resultem em interrupções de funcionamento do instrumento e verificar se o armazenamento dos eventos no Registro de Interrupções de Funcionamento do instrumento ocorre em ordem cronológica indexada por um índice monotonicamente crescente. 4. Alterar a data do instrumento para 4 anos e 11 meses adiante no futuro e realizar, pelo menos, mais uma intervenção que resulte em interrupção de funcionamento do instrumento e verificar se as interrupções registradas anteriormente neste ensaio são mantidas. 5. Verificar se é possível remover, adulterar, trocar ou substituir os componentes que armazenam registros de auditoria. 6. Verificar se todas as informações especificadas no item 3.4.6 do RTM aprovado pela Portaria Inmetro 559/2016 são armazenadas corretamente.

(Continua)

18	8.3g	Detecção de falhas	Registro de eventos de manutenção	1. Verificar se o Registro de Eventos de Manutenção segue o disposto do item 3.4.7 ao item 3.4.8 do Anexo A do RTM aprovado pela Portaria Inmetro 559/2016. 2. Utilizar um dispositivo adequado de leitura para verificar se a realização da operação de manutenção é armazenada no Registro de Eventos de Manutenção do instrumento. 3. Realizar novas intervenções que resultem em interrupções de funcionamento do instrumento e posterior manutenção, verificando se o armazenamento da realização das operações de manutenção armazenadas no Registro de Eventos de Manutenção do instrumento ocorre em ordem cronológica indexada por um índice monotonicamente crescente. 4. Alterar a data do instrumento para 4 anos e 11 meses adiante no futuro e realizar, pelo menos, mais uma intervenção que resulte em interrupção de funcionamento do instrumento e posterior manutenção, verificando se os registros de operações de manutenção armazenadas anteriormente neste ensaio são mantidas. 5. Verificar se é possível remover, adulterar, trocar ou substituir os componentes que armazenam registros de auditoria. 6. Verificar se todas as informações especificadas no item 3.4.8 do RTM aprovado pela Portaria Inmetro 559/2016 são armazenadas corretamente.
19	8.4a	Comunicação entre dispositivos de hardware da bomba medidora	Comunicação por protocolo	1. Verificar se a comunicação realizada entre o dispositivo transdutor e o dispositivo controlador da bomba medidora de combustível é realizada através de protocolo de comunicação. 2. Verificar a composição e assinatura do pacote de dados de abastecimento especificado no item 3.5.14 do Anexo A do RTM aprovado pela Portaria Inmetro 559/2016 através da conexão com a interface de verificação metrológica do instrumento.
20	8.4b	Comunicação entre dispositivos de hardware da bomba medidora	Especificação do protocolo de comunicação	1. Verificar se a especificação do protocolo de comunicação utilizado foi fornecida para o processo de avaliação de modelo, juntamente com declaração de completude dos comandos.
21	8.4c	Comunicação entre dispositivos de hardware da bomba medidora	Identificador unívoco do dispositivo transdutor	1. Verificar se o dispositivo transdutor armazena internamente um identificador unívoco que o permita referenciá-lo sem ambiguidade. 2. Verificar se o identificador unívoco do dispositivo transdutor é protegido contra alterações de qualquer natureza.

(Continua)

22	8.4d	Comunicação entre dispositivos de hardware da bomba medidora	Armazenamento de chaves criptográficas	1. Verificar se o dispositivo transdutor armazena par de chaves criptográficas assimétricas para realização de assinatura digital, utilizando circuito integrado aprovado pelo Inmetro.
23	8.4e	Comunicação entre dispositivos de hardware da bomba medidora	Colisão de chaves	1. Verificar como é garantido que não haja geração e utilização de pares de chaves criptográficas idênticos em dispositivos de um mesmo fabricante.
24	8.4f	Comunicação entre dispositivos de hardware da bomba medidora	Inextricabilidade da chave privada	1. Verificar como a chave privada do dispositivo transdutor é armazenada de modo inviolável e inextricável do meio físico e lógico e que garantias são fornecidas para este armazenamento seguro.
25	8.4g	Comunicação entre dispositivos de hardware da bomba medidora	Armazenamento de chaves	1. Verificar se os identificadores únicos e chaves públicas dos dispositivos transdutores são armazenados nos dispositivos controlador e indicador.
26	8.4h	Comunicação entre dispositivos de hardware da bomba medidora	Verificação de identificador e chave pública	1. Verificar se, antes de cada abastecimento, o dispositivo controlador verifica o identificador unívoco e a chave pública do dispositivo transdutor. 2. Realizar o abastecimento com um dispositivo transdutor cujo identificador e chave pública seja conhecido do dispositivo controlador, observando a ocorrência de sucesso na operação. 3. Realizar o abastecimento com um dispositivo transdutor cujo identificador e chave pública seja desconhecido do dispositivo controlador, observando a ocorrência de falha na operação.
27	8.4i	Comunicação entre dispositivos de hardware da bomba medidora	Impedimento de funcionamento do dispositivo transdutor	1. Verificar se, em caso de falha na verificação do identificador unívoco e da chave pública do dispositivo transdutor pelo dispositivo controlador, o funcionamento do dispositivo transdutor correspondente é impedido. 2. Realizar o abastecimento com um dispositivo transdutor cujo identificador e chave pública seja conhecido do dispositivo controlador, observando a ocorrência de sucesso na operação. 3. Realizar o abastecimento com um dispositivo transdutor cujo identificador e chave pública seja desconhecido do dispositivo controlador, observando a ocorrência de falha na operação.
28	8.4j	Comunicação entre dispositivos de hardware da bomba medidora	Registro de interrupções de funcionamento	1. Utilizar um dispositivo adequado de leitura para verificar se a ocorrência de falha na verificação do identificador unívoco e da chave pública do dispositivo transdutor pelo dispositivo controlador é armazenado no Registro de Interrupções de Funcionamento do instrumento.

(Continua)

29	8.4k	Comunicação entre dispositivos de hardware da bomba medidora	Registro de interrupções de funcionamento	1. Verificar se o Registro de Interrupções de Funcionamento, armazenado no instrumento, possui: identificação do tipo de evento que gerou a interrupção do funcionamento do instrumento, identificador unívoco do dispositivo associado à falha e data e hora da falha.
30	8.4l	Comunicação entre dispositivos de hardware da bomba medidora	Registro de eventos de manutenção	1. Verificar se a operação de manutenção para sanar a falha 8.4i cuja ocorrência foi armazenada no Registro de Interrupções de Funcionamento foi também armazenada no Registro de Eventos de Manutenção
31	8.4m	Comunicação entre dispositivos de hardware da bomba medidora	Registro de eventos de manutenção	1. Verificar se o Registro de Eventos de Manutenção, armazenado no instrumento, possui: identificação do nível de acesso do responsável pela manutenção do instrumento, resultado da operação de manutenção, identificação do dispositivo ou parte da bomba medidora que foi alvo da manutenção e data e hora da operação.
32	8.4n	Comunicação entre dispositivos de hardware da bomba medidora	Envio de pacote de dados de abastecimento	1. Verificar se, ao final de cada abastecimento e na interrupção de fluxo de combustível, o dispositivo transdutor envia ao dispositivo controlador as informações de totalização da medição em um pacote de dados assinado digitalmente com a chave privada do dispositivo transdutor. 2. Realizar um abastecimento e verificar, através da interface de verificação metrológica, se o pacote de dados de abastecimento corresponde ao respectivo evento. 3. Realizar um novo abastecimento, interromper o fluxo de combustível (liberando o gatilho do bico) e verificar, através da interface de verificação metrológica, se o pacote de dados de abastecimento corresponde ao respectivo evento.
33	8.4o	Comunicação entre dispositivos de hardware da bomba medidora	Composição do pacote de dados de abastecimento	1. Realizar um abastecimento e verificar se o pacote de dados de abastecimento possui, pelo menos, as seguintes informações: identificação unívoca do dispositivo transdutor, identificação unívoca do dispositivo controlador, identificador unívoco do abastecimento, quantidade de pulsos e/ou informação de medição de volume do abastecimento registrado pelo dispositivo transdutor, constante de calibração do dispositivo transdutor, volume abastecido total calculado pelo dispositivo transdutor, valor monetário total da transação, preço por litro do combustível, data e hora do abastecimento.

(Continua)

34	8.4p	Comunicação entre dispositivos de hardware da bomba medidora	Verificação da assinatura digital	1. Realizar um abastecimento e verificar se o pacote de dados de abastecimento é assinado digitalmente pela chave privada do dispositivo transdutor. 2. Realizar a conferência da assinatura digital com a chave pública correspondente, utilizando o pacote de dados de abastecimento.
35	8.4q	Comunicação entre dispositivos de hardware da bomba medidora	Instalação de novo dispositivo transdutor	1. Verificar se, na instalação de um novo dispositivo transdutor no instrumento, o dispositivo controlador o habilita e verifica sua identidade.
36	8.4r	Comunicação entre dispositivos de hardware da bomba medidora	Informações de abastecimento	1. Verificar se, ao final do abastecimento, o dispositivo indicador apresenta as informações de volume abastecido, valor monetário da transação e preço por litro do combustível e se estas conferem com o pacote de dados de abastecimento.
37	8.4s	Comunicação entre dispositivos de hardware da bomba medidora	Apresentação da conferência da assinatura digital no dispositivo indicador	1. Realizar um abastecimento e verificar se, ao seu término, o dispositivo indicador apresenta a informação de que a assinatura digital do pacote de dados de abastecimento foi conferida e o resultado desta conferência.
38	8.4t	Comunicação entre dispositivos de hardware da bomba medidora	Falha na conferência da assinatura digital no dispositivo indicador	1. Instalar um dispositivo transdutor com certificado digital inválido. 2. Realizar um abastecimento de combustível utilizando o bico associado a este dispositivo transdutor. 3. Verificar se, em caso de falha na conferência da assinatura digital do pacote de dados de abastecimento, o funcionamento do dispositivo transdutor é impedido e uma mensagem de erro é apresentada no dispositivo indicador.
39	8.4u	Comunicação entre dispositivos de hardware da bomba medidora	Registro de interrupções de funcionamento	1. Utilizar um dispositivo adequado de leitura para verificar se a ocorrência da interrupção de funcionamento 8.4t do dispositivo transdutor devido à falha da verificação da assinatura digital no dispositivo indicador é armazenada no Registro de Interrupções de Funcionamento do instrumento.
40	8.4v	Comunicação entre dispositivos de hardware da bomba medidora	Registro de interrupções de funcionamento	1. Utilizar um dispositivo adequado de leitura para verificar se o Registro de Interrupções de Funcionamento armazenado no instrumento possui: identificação do tipo de evento que gerou a interrupção do funcionamento do instrumento, identificador unívoco do dispositivo transdutor associado à falha e data e hora do evento.
41	8.4w	Comunicação entre dispositivos de hardware da bomba medidora	Registro de eventos de manutenção	1. Utilizar um dispositivo adequado de leitura para verificar se a operação de manutenção para sanar a falha 8.4t cuja ocorrência foi armazenada no Registro de Interrupções de Funcionamento é armazenada no Registro de Eventos de Manutenção.

(Continua)

42	8.4x	Comunicação entre dispositivos de hardware da bomba medidora	Registro de eventos de manutenção	1. Utilizar um dispositivo adequado de leitura para verificar se os dados armazenados no registro de eventos de manutenção possuem: identificação do nível de acesso do responsável pela manutenção do instrumento, resultado da operação de manutenção, identificação do dispositivo ou parte da bomba medidora que foi alvo da manutenção e data e hora da operação.
43	8.4y	Comunicação entre dispositivos de hardware da bomba medidora	Comunicação de equipamentos auxiliares não constantes na solicitação de avaliação de modelo.	1. Verificar se a comunicação do instrumento com equipamentos auxiliares, não constantes da solicitação de avaliação de modelo, só é realizada mediante interface de comunicação própria e dedicada a este fim, cujo ponto de acesso deve estar disponível fora da área selada do instrumento.
44	8.4z	Comunicação entre dispositivos de hardware da bomba medidora	Presença de equipamentos auxiliares não constantes na solicitação de avaliação de modelo.	1. Verificar se há conexões de equipamentos auxiliares, não constantes na solicitação de avaliação de modelo, diretamente nas placas eletrônicas do dispositivos transdutor, controlador ou indicador.
45	8.4aa	Comunicação entre dispositivos de hardware da bomba medidora	Proteção das interfaces de comunicação com equipamentos auxiliares	1. Verificar se as interfaces de comunicação do instrumento com equipamentos auxiliares externos são protegidas contra tentativas de acesso não autorizados ou indevidos ao instrumento.
46	8.4ab	Comunicação entre dispositivos de hardware da bomba medidora	Proteção dos comandos de interface	1. Verificar se comandos dos protocolos de interface de comunicação com equipamentos externos podem alterar parâmetros, dados ou software legalmente relevante de forma diferente daquela declarada pelo fabricante.
47	8.5a	Verificação de integridade de software	Existência de interface de verificação metrológica	1. Verificar se está disponível uma interface de verificação metrológica no dispositivo controlador, padrão Bluetooth, especificada na Norma NIT-Sinst-020.
48	8.5b	Verificação de integridade de software	Realização do procedimento de verificação de integridade	1. Realizar o procedimento de verificação de integridade, conforme Norma NIT-Sinst-20, do software dos dispositivos transdutores e indicadores. 2. Verificar se o procedimento de verificação de integridade confirma a correspondência com o software em avaliação de modelo.
49	8.5c	Verificação de integridade de software	Indicação do nome da interface bluetooth	1. Verificar se o nome do dispositivo Bluetooth da interface de verificação metrológica está afixado em área visível sobre a superfície do instrumento, conforme descrito no item 7 (Inscrições Obrigatórias) da Portaria Inmetro 559/2016.
50	8.5d	Verificação de integridade de software	Emparelhamento da interface bluetooth	1. Iniciar uma operação de abastecimento. 2. Verificar se é possível, a partir do início do abastecimento, emparelhar um dispositivo com interface *bluetooth* com o instrumento.

(Continua)

47	9.2a	Separação de software	Identificação das partes	1. Verificar se todos os módulos de software e hardware dos dispositivos transdutor e indicador, que realizem tarefas legalmente relevantes, são corretamente identificados como partes legalmente relevantes do instrumento.
48	9.2b	Separação de software	Proteção das partes legalmente relevantes	1. Verificar se partes legalmente relevantes do hardware ou software do instrumento podem ser inadmissivelmente influenciadas por comandos recebidos através de interfaces de comunicação ou de partes não legalmente relevantes do instrumento.
49	9.2c	Separação de software	Correspondência dos comandos	1. Verificar se todo comando emitido por uma interface (de usuário, de verificação metrológica, de comunicação ou se separação de software e/ou hardware) possui uma correspondência unívoca e não ambígua com respectiva função iniciada no software legalmente relevante ou alteração de dados realizada na parte legalmente relevante.
50	9.2d	Separação de software	Interface de separação	1. Verificar e identificar a existência de uma interface de separação de software e/ou hardware que realize a comunicação entre a parte legalmente relevante e a parte não legalmente relevante.
51	9.2e	Separação de software	Declaração de completude	1. Verificar a existência de declaração de completude de comandos da interface de separação de software.
52	9.2f	Separação de software	Efeitos de atrasos ou bloqueios	1. Verificar se atrasos ou bloqueios resultantes da realização de tarefas não legalmente relevantes pode implicar no comprometimento do resultado da medição.
53	9.3a	Armazenamento e transmissão de dados em meio inseguro	Autenticidade e integridade	1. Verificar se os dados legalmente relevantes têm sua autenticidade e integridade garantidas. A assinatura digital pode ser uma solução segura, se adequadamente implementada.
54	9.3b	Armazenamento e transmissão de dados em meio inseguro	Assinatura digital	1. Verificar se, no caso do uso de assinatura digital para garantia de autenticidade e integridade, esta assinatura é verificada pelo software ou hardware responsável pela sua publicação ou processamento (toda assinatura deve ser verificada, não há sentido em assinar se não verificar).
55	9.3c	Armazenamento e transmissão de dados em meio inseguro	Uso dos dados	1. Verificar se, no caso de sucesso na verificação da assinatura digital, os dados de medição são corretamente utilizados (isto é, não são alterados após a conferência da assinatura).
56	9.3d	Armazenamento e transmissão de dados em meio inseguro	Descarte dos dados	1. Verificar se, no caso de falha na verificação da assinatura digital, os dados de medição são descartados (dados incorretos ou com verificação falha não podem ser usados).
57	9.3e	Armazenamento e transmissão de dados em meio inseguro	Inextricabilidade das chaves	1. Verificar se as chaves criptográficas privadas empregadas são mantidas secretas e seguras internamente ao instrumento.

(Continua)

58	9.4a	Carga de software legalmente relevante	Aprovação do software carregado	1. Verificar se somente software legalmente relevante submetido pelo requerente e aprovado no processo de avaliação de modelo pode ser carregado no instrumento.
59	9.4b	Carga de software legalmente relevante	Comportamento do instrumento durante a carga	1. Verificar se, durante a carga de software legalmente, o instrumento para de realizar medições.
60	9.4c	Carga de software legalmente relevante	Restauração do nível de segurança.	1. Verificar se ao final do procedimento de carga e instalação de software legalmente relevante, o ambiente de proteção retorna ao mesmo nível de segurança declarado no processo de avaliação de modelo. Os ensaios 1, 5, 8, 9, 14 devem ser executados novamente após a realização de nova carga de software.
61	9.4d	Carga de software legalmente relevante	Autenticidade e integridade do software carregado	1. Verificar se os meios técnicos para garantir a autenticidade e integridade do software a ser carregado são adequados.
62	9.4e	Carga de software legalmente relevante	Descarte do software sem autenticidade e integridade verificadas	1. Verificar que, se a autenticidade ou integridade do novo software não puder ser verificada, o instrumento o descarta, utiliza a versão anterior ou torna-se inoperante.
63	9.4f	Carga de software legalmente relevante	Evidencia e registro de carga de software	1. Verificar se a carga e a tentativa de carga de software implicam no rompimento de lacres físicos, bem como no registro desta ação em memória não volátil (registro de carga de software).
64	9.4g	Carga de software legalmente relevante	Composição do registro da carga	1. Verificar se o registro da carga e tentativa de carga de software contém: identificação do nível de acesso do responsável pela carga, data e hora da carga, sucesso ou insucesso da carga e as versões do software anterior e posterior à carga.
65	9.5a	Carga de software não legalmente relevante	Carga de software não legalmente relevante	1. Verificar se a carga de software não legalmente relevante pode ser realizada sem necessidade de aprovação pelo Inmetro, ou seja, sem um certificado digital, válido ou inválido.
66	9.6a	Disposições gerais	Inviolabilidade do dispositivo transdutor	1. Verificar se ao dispositivo transdutor a manutenção, sem clara violação física ou lógica, não é permitida.
67	9.6b	Disposições gerais	Identificação do software e firmware	1. O software e firmware do instrumento devem ter suas versões e hash registrados e identificados para publicação na Portaria de Aprovação de Modelo.
68	9.7c	Disposições gerais	Armazenamento das chaves	1. Verificar como o fabricante assegura o ambiente seguro de gestão das chaves criptográficas dos dispositivos transdutores (as chaves devem ser mantidas seguras dentro dos dispositivos transdutores, preferencialmente geradas por eles).