SUMÁRIO

1 OBJETIVO

Esta norma estabelece os procedimentos a serem utilizados na análise de *software* para avaliação de modelo de medidores de vazão de gás natural, biometano e gás liquefeito de petróleo (GLP) em fase gasosa.

2 CAMPO DE APLICAÇÃO

Esta norma aplica-se aos laboratórios designados e/ou acreditados e ao Dimel/Dgtec/Sinst.

3 RESPONSABILIDADE

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

4 DOCUMENTOS DE REFERÊNCIA

Portaria Inmetro nº 156 de 30/03/2022	Aprova o RTM de medidores de vazão de gás natural, biometano e gás liquefeito de petróleo (GLP) em fase gasosa e seu Anexo – Requisitos Técnicos de Segurança da Informação
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 (VIML)

(continua)

OIML D 31/2008	*General requirements for software controlled measuring instruments*
OIML D 11/2004	*General requirements for electronic measuring instruments*
WELMEC Software Guide 7.2 2015	*Measuring instruments directive 2014/32/EU – WELMEC*
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	Protocolo de comunicação serial para verificação de integridade de *software* em instrumentos de medição

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
AMD	Análise do Memorial Descritivo
EFS	Ensaio Funcional de *Software*
FIPS	*Federal Information Processing Standards*
NIST	*National Institute of Standards and Technology*
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 e que contém *software* legalmente relevante.

7.2 Assinatura digital

Código atribuído a um arquivo digital de forma a atestar 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 sua selagem principal.

7.4 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; ou
d) executam carga de *software* legalmente relevante.

7.5 Memorial descritivo

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

7.6 Não legalmente relevante

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

7.7 Requerente

Pessoa jurídica (ou seu representante legal), 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 e que requer a avaliação de modelo de instrumento.

7.8 Requisitos gerais de *software*

Requisitos de *software* e *hardware* do RTM em questão que todos os instrumentos (medidores de vazão de gás natural, biometano e gás liquefeito de petróleo (GLP) em fase gasosa) devem satisfazer.

7.9 Requisitos específicos de *software*

Os requisitos que tratam de aspectos técnicos específicos referentes às tecnologias empregadas na concepção do medidor de vazão de gás natural, biometano e gás liquefeito de petróleo (GLP) em fase gasosa ou inserção de funcionalidades complementares. O instrumento que possuir esses aspectos técnicos ou empregar essas funcionalidades tecnológicas específicas deve satisfazer o requisito específico do RTM em questão.

7.10 Selagem principal

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

7.11 Verificação de integridade

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

8 ORIENTAÇÕES GERAIS

8.1 A análise de *software* dos medidores de vazão de gás natural, biometano e gás liquefeito de petróleo (GLP) em fase gasosa para avaliação de modelo será baseada nas seguintes fontes de evidências:

a) análise da documentação técnica, conforme descrito na Norma NIT-Sinst-003; e
b) resultados obtidos durante a realização dos ensaios funcionais de *software* descritos no Anexo A dessa norma;

8.1.1 Ao se iniciar a análise de *software*, o técnico responsável deverá realizar o estudo preliminar do pacote de documentação técnica de forma a familiarizar-se com o instrumento.

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

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 instrumento e auxiliar na avaliação de modelo.

8.2 Métodos de análise

8.2.1 Os métodos de análise de *software* para fins de avaliação de modelo são a seguir relacionados.

8.2.2 Análise do memorial descritivo (AMD): consiste na leitura e análise do memorial descritivo de *software* e demais documentos fornecidos pelo fabricante, 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 fabricante evidenciam o cumprimento dos requisitos do Anexo B da Portaria Inmetro 156/2022, 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 requerida 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 156/2022.

8.2.3 Ensaios funcionais de *software* (EFS): consiste na análise do comportamento do *software* legalmente relevante do instrumento em condições de operação real.

8.2.3.1 Os EFS devem ser aplicados quando necessário de forma a evidenciar, assegurar, ratificar ou respaldar o que o que foi verificado durante a AMD.

8.2.3.2 Os EFS devem 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) verificação de integridade;
f) separação de *software* e/ou *hardware*;
g) armazenamento e transmissão de dados;
h) carga de *software* legalmente relevante; e
i) arquiteturas com assinatura digital.

8.2.3.3 Uma relação de EFS passíveis de serem realizados encontra-se no Anexo A.

8.2.3.4 Os procedimentos específicos dos EFS devem tomar por subsídio as informações contidas nos casos de teste descritos na documentação entregue para análise.

8.2.3.5 Através da realização de EFS, as características de desempenho descritas nos memoriais descritivos e manual operacional devem ser verificadas em procedimentos práticos. Os resultados obtidos devem ser registrados, apresentados e mantidos em relatório.

8.2.3.6 Através dos EFS, deve ser analisada a operação normal do instrumento. Todas as chaves ou teclas e combinações descritas devem ser empregadas e a reação do instrumento avaliada. Para interfaces gráficas de usuário, todos os menus e demais elementos gráficos devem ser ativados e avaliados.

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 156/2022.

9.1.2 Devem ser realizados os EFS 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 156/2022.

9.2.2 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*.

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 156/2022.

9.3.2 Devem ser realizados os EFS constantes no Anexo A desta norma.

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 156/2022.

9.4.2 Devem ser realizados os EFS constantes no Anexo A desta norma.

9.5 Verificação de Integridade

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 156/2022.

9.5.2 O processo de verificação de integridade verifica se os dados/*software*/parâmetros legalmente relevantes não foram alterados durante o uso, reparo, manutenção, transferência ou armazenamento sem que haja autorização do Inmetro.

9.5.3 Para instrumentos contendo interfaces, o fabricante deve fornecer um método de verificação de integridade do *firmware* legalmente relevante presente no instrumento quando comparado com o *firmware* legalmente relevante aprovado no processo de avaliação de modelo. O método de verificação disponibilizado deve estar de acordo com o que está disposto na Norma NIT-Sinst-020.

9.5.4 Para instrumentos que não possuam interfaces, devem ser fornecidos meios necessários para realizar a verificação de integridade em bancada para o *firmware* presente no instrumento em comparação ao *firmware* legalmente relevante aprovado no processo de avaliação de modelo.

9.5.5 Devem ser realizados os EFS 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 156/2022.

10 REQUISITOS ESPECÍFICOS DE *SOFTWARE* E *HARDWARE*

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

10.1.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 2.9 do Anexo B do RTM aprovado pela Portaria Inmetro nº 156/2022.

10.1.2 Devem ser realizados os EFS constantes no Anexo A desta norma.

10.2 Armazenamento e Transmissão de dados

10.2.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 2.10 do Anexo B do RTM aprovado pela Portaria Inmetro nº 156/2022.

10.2.2 Devem ser realizados os EFS 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 2.11 do Anexo B do RTM aprovado pela Portaria Inmetro nº 156/2022.

10.3.2 Para instrumentos que permitam a carga de *software* em campo sem rompimento de lacre, se a assinatura digital for adotada pelo fabricante 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 avaliação de modelo.

10.3.3 Com respeito à autenticação 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 Devem ser realizados os EFS constantes no Anexo A desta norma.

10.3.5 O requerente deve fornecer arquivos binários assinados, assim como o procedimento e ferramentas necessárias para carrega-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 2.12 do Anexo B do RTM aprovado pela Portaria Inmetro nº 156/2022.

10.5 Arquiteturas com assinatura digital

10.5.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 2.13 do Anexo B do RTM aprovado pela Portaria Inmetro nº 156/2022.

10.5.2 As chaves criptográficas devem ser únicas para cada unidade produzida para o instrumento.

10.5.3 Devem ser realizados os EFS constantes no Anexo A desta norma.

10.6 Documentação requerida para os requisitos específicos

10.6.1 Deve ser avaliado, onde aplicável, se a documentação entregue pelo requerente encontra-se completa de acordo com o exigido no item 2.14 do Anexo B do RTM aprovado pela Portaria Inmetro nº 156/2022.

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.

11 HISTÓRICO DE REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens revisados
00	Ago/2023	Emissão inicial.

Quadro de aprovação		
	Nome	**Atribuição**
Elaborado por:	Fabiano de Oliveira Leitão	Pesquisador Tecnologista em Metrologia e Qualidade
Verificado por:	Juliana Wilm Guedes Rogerio Possidonio Nunes	Auxiliar Administrativo Pesquisador Tecnologista em Metrologia e Qualidade
Aprovado por:	Icaro dos Santos França	Chefe do Sinst, substituto

/ANEXO A

ANEXO A - ENSAIOS FUNCIONAIS DE *SOFTWARE*

Tabela 1 – Ensaios funcionais de *software* baseados nos requisitos do Anexo B do RTM da Portaria Inmetro nº 156/2022

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
1	2.2	Versão do *software* legalmente relevante	Identificador de versão, estrutura e acesso.	1. Verificar se o identificador de versão de *software* existe, como é acessado e se esse processo é idêntico ao descrito na documentação. Verificar a estrutura do identificador de versão. 2. Verificar se o identificador de versão de *software* legalmente relevante é claramente apresentado.
2	2.3	Correção dos algoritmos e funções	Exatidão metrológica da medição.	1. A ser executado pelo Seflu. Se necessário, deve ser possível examinar os algoritmos e funções de medição por meio de EFS.
3	2.4	Proteção de *software* e *hardware*	Possibilidade de uso impróprio ou fraudulento do instrumento Selagem mecânica. Outros meios de proteção do *software* e *hardware* do instrumento. Influência das partes legalmente relevantes do instrumento por outras partes do sistema de medição. Proteção do *software* e dos parâmetros legalmente relevantes Proteção contra alterações inadmissíveis, troca indevida de unidades de memória e carga de *software* não autorizada. Características requeridas para o registro de alteração de parâmetros Segurança dos componentes que armazenam registros de auditoria	1. Avaliar eventuais fragilidades com o objetivo de fazer uso fraudulento do instrumento (por exemplo, é possível a modificação de parâmetro legalmente relevante sem rompimento de lacre ou autenticação?). 2. Verificar se a selagem mecânica protege o instrumento contra modificações não autorizadas de seu *software* ou parâmetros legalmente relevantes. 3. Verificar se os outros meios de proteção do instrumento (eletrônicos, criptográficos, etc.) são robustos e eficazes (de acordo com documentos FIPS NIST) contra modificações acidentais/não autorizadas de seu *software* ou parâmetros legalmente relevantes. 4. Verificar se o *software* e os parâmetros legalmente relevantes são protegidos contra alterações inadmissíveis ou acidentais/não autorizadas, carga de *software* não autorizada e modificações causadas pela troca indevida de unidades de memória. 5. Avaliar 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*. 6. Verificar se os parâmetros que definem características metrológicas do instrumento são armazenados de forma segura e se são alterados somente mediante procedimento documentado pelo fabricante. 7. Verificar se o registro de auditoria está conforme disposto nos itens de 2.4.8 a 2.4.15 do Anexo B do RTM aprovado pela Portaria Inmetro n.º 156/2022. 8. O requerente deve fornecer arquivos binários contendo alterações intencionais, de forma a permitir a realização de ensaios que evidenciem a proteção do instrumento contra mudanças acidentais de *software* e/ou parâmetros legalmente/relevantes. 9. Deve ser avaliado se, por meio de alguma interface de comunicação do instrumento

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
				(de usuário, comunicação ou verificação metrológica) e do *software* de comunicação e configuração do fabricante, é possível realizar intrusão ou modificações não autorizadas no *software* ou nos parâmetros legalmente relevantes.
4	2.5	Detecção de falhas	Reação às falhas descritas na documentação e verificação do desempenho do instrumento.	1. Verificar se o instrumento possui funções de detecção de falhas. 2. Verificar se a função de detecção de falhas está descrita na documentação apresentada. 3. Colocar o instrumento no estado das falhas detectáveis e verificar se as reações contra as mesmas ocorrem do modo descrito no memorial descritivo. 4. Reproduzir TODAS as falhas factíveis de serem provocadas em laboratório e verificar se a reação do instrumento ocorre conforme descrito em seu manual operacional. 5. Adicionalmente, verificar se, para cada falha detectada, o instrumento realiza as seguintes ações: a. corrige automaticamente a falha ou; b. impede apenas o funcionamento do dispositivo com falha, caso este não faça parte da cadeia legalmente relevante ou; c. impede o funcionamento de todo o instrumento, caso este faça parte da cadeia legalmente relevante, emitindo alarme visível ou audível, até que a causa da falha seja eliminada.
5	2.6	Verificação de Integridade	Método de verificação de integridade do *firmware* legalmente relevante	1. Para instrumentos contendo interfaces de comunicação, verificar a conformidade do método de verificação de integridade do *firmware* fornecido pelo fabricante em relação à descrição contida na norma NIT-Sinst-020. 2. Para instrumentos sem interface de comunicação, avaliar a correção/validade do método de verificação fornecido pelo fabricante para realizar a verificação de integridade de *firmware* em relação ao *firmware* legalmente relevante aprovado no processo de avaliação de modelo. 3. Para qualquer um dos casos, verificar se o método de verificação de integridade fornecido atesta como íntegro um *firmware* íntegro carregado no instrumento. 4. Para qualquer um dos casos, verificar se o método de verificação de integridade fornecido atesta como não íntegro um *firmware* não íntegro carregado no instrumento.
6	2.9	Separação de *software* e/ou *hardware*	Identificação das partes legalmente relevantes e não legalmente relevantes	1. Verificar se a distribuição física das partes legalmente relevantes e não legalmente relevantes está de acordo com o memorial descritivo de *software*. 2. Verificar se a comunicação entre as partes legalmente relevantes e não legalmente

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Comunicação entre as partes legalmente relevantes e não legalmente relevantes Influência das partes legalmente relevantes Comportamento da medição	relevantes é realizada exclusivamente através da interface de separação de *software* e/ou *hardware*. 3. 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. 4. Verificar a completude dos comandos emitidos via interface de separação. 5. Verificar a influência das partes legalmente relevantes por comandos não documentados recebidos através da interface de separação de *software* e/ou *hardware*. 6. Verificar se a medição é comprometida por atrasos ou bloqueios ocorridos pela realização de outras tarefas.
7	2.10	Armazenamento e transmissão de dados	Garantia da autenticidade, integridade e carimbo de tempo dos dados transferidos Atrasos de transferência Carimbo de tempo	1. Verificar se os mecanismos que garantem autenticidade, integridade e carimbo de tempo dos dados transmitidos correspondem àqueles referenciados no memorial descritivo. 2. Verificar se os dados armazenados/transmitidos têm sua autenticidade e integridade checadas após a sua leitura/recepção. 3. Simular situação de falha da autenticidade e integridade dos dados armazenados/transmitidos e observar o descarte destes dados. 4. Simular situação de atraso de transferência e verificar se o resultado de medição é influenciado. 5. 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. 6. Verificar a transmissão dos dados armazenados quando do restabelecimento dos sistemas de transferência após uma interrupção. 7. Verificar se o carimbo de tempo é obtido conforme apresentado no memorial descritivo de *software*.
8	2.11	Carga de *software* legalmente relevante	Aprovação do *software* pelo Inmetro Automação da carga de *software* Comportamento do instrumento durante e ao final da carga de *software*	1. Verificar se os mecanismos que garantem que o *software* tenha sido aprovado pelo Inmetro correspondem àqueles referenciados no memorial descritivo. 2. Verificar se a carga de *software* é automática, ou seja, uma vez iniciada independe do operador. 3. Verificar se o instrumento realiza medições durante o processo de carga de *software*.

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Autenticação de usuário para efetuar carga de *software* Garantia da autenticidade e integridade do *software* a ser carregado Registro de auditoria da carga de *software*	4. Verificar se após a carga de *software* o ambiente de proteção retorna ao mesmo nível de segurança declarado no processo de avaliação de modelo. 5. Atestar a existência de autenticação de usuário para realização da carga de *software*. Esta autenticação deve atender às exigências do item 9.3 desta norma. 6. Verificar se os mecanismos que garantem a autenticidade e a integridade do *software* correspondem àqueles referenciados no memorial descritivo. 7. Simular situação de falha da autenticidade e integridade do *software* a ser carregado e observar seu descarte e o uso da versão anterior. Alternativamente, o instrumento deve tornar-se inoperante. 8. Verificar se a carga de *software* ocorre apenas quando há abertura de proteção física ou acesso autenticado. 9. Verificar se há registro da carga de *software*. O registro de auditoria da carga de *software* 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. 10. Verificar se os registros de auditoria são armazenados por, no mínimo, 5 (cinco) anos. 11. Verificar a disponibilização dos registros de auditoria para leitura.
9	2.13	Arquitetura com assinatura digital	Ferramentas fornecidas pelo fabricante Armazenamento de dados Gestão de chaves criptográficas	1. Avaliar e verificar a validade das ferramentas fornecidas pelo fabricante para verificação, publicação e reconstituição do valor final da medição a partir dos dados assinados. 1.1 Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação. 1.2 Simular situação de falha na chave pública e verificar se a ferramenta indica tal situação. 1.3 Avaliar a ferramenta de reconstituição do valor final da medição a partir dos dados assinados. 1.4 Simular situação de falha nos dados assinados e verificar se a ferramenta indica tal situação. 2. Verificar se as chaves criptográficas privadas são mantidas secretas e seguras internamente ao instrumento. Verificar se a localização das chaves criptográficas utilizadas no instrumento possui proteções contra acesso físico e/ou lógico conforme descrito na documentação.

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
				3. Verificar se é gerado registro de auditoria para o caso de tentativa de acesso indevido às chaves criptográficas, conforme descrito no item 2.13.5.2 do RTM aprovado pela Portaria Inmetro n.º 156/2022, bem como a indicação de falha no instrumento até que ocorra uma operação de inspeção metrológica.