

	ANÁLISE DE SOFTWARE PARA AVALIAÇÃO DE MODELO DE MEDIDORES DE UMIDADE DE GRÃOS	NORMA Nº NIT-SINST-006	REV Nº 00
		PUBLICADO EM JAN/2023	PÁGINA 1/18

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 medidores de umidade de grãos.

2 CAMPO DE APLICAÇÃO

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

3 RESPONSABILIDADE

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

4 DOCUMENTOS DE REFERÊNCIA

Portaria Inmetro nº 047 de 07/02/2022	Aprova o regulamento técnico metrológico consolidado para medidores de umidade de grãos
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)
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>
WELMEC <i>Software Guide</i> 7.2 2015	<i>Measuring instruments directive 2014/32/EU – WELMEC</i>
NIST <i>Special Publication</i> 800-57 Part 1 Revision 4	<i>Recommendation for key management – Part 1: General</i>

	NIT-SINST-006	REV. 00	PÁGINA 2/18
---	----------------------	--------------------	------------------------

5 DOCUMENTOS COMPLEMENTARES

NIT-Sinst-003	Organização da documentação para o processo de avaliação de software
NIT-Sefiq-005	Exame/ensaios de AM dos medidores de umidade de grãos
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>.

AD	Análise da documentação
AM	Avaliação de modelo
AMD	Análise do memorial descritivo
EFS	Ensaio funcional de <i>software</i>
MUG	Medidor de umidade de grãos
NIST	<i>National Institute of Standards and Technology</i>
OS	<i>Operating System</i>
OTP	<i>One-time programmable</i>
PC	<i>Personal Computer</i>
RBMLQ-I	Rede Brasileira de Metrologia Legal e Qualidade - Inmetro
RTM	Regulamento Técnico Metrológico

7 TERMOS E DEFINIÇÕES

Para os efeitos deste documento, além das definições que constam nos documentos de referência, aplicam-se os seguintes 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* (que uma vez iniciada independe do operador) para o instrumento de medição usando qualquer meio apropriado local ou remoto, sem a necessidade de romper sua selagem principal.

	NIT-SINST-006	REV. 00	PÁGINA 3/18
---	----------------------	--------------------	------------------------

7.4 Componente imutável

Componentes e dispositivos eletrônicos do instrumento de medição (comercialmente disponíveis) que sejam não programáveis, ou que não permitam alteração do seu *firmware* interno, ou que sejam dotados de memória de programação apenas do tipo OTP.

7.5 Computador tipo U

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

7.6 Documentação

Documentos contidos no pacote de entrega. Sinônimo de documentação de *software*.

7.7 Instrumento com computador tipo P

Instrumento com computador caracterizado por:

- a) o seu *software* embarcado é construído exclusivamente para fins de medição. Adicionalmente também são consideradas outras funções implementadas no instrumento com o propósito de medição, tais como proteção do *software* e dos dados, transmissão de dados e carga de *software*, também são consideradas;
- b) a interface do usuário é dedicada ao propósito de medição;
- c) um sistema operacional (OS) ou subsistemas podem ser incluídos apenas se o *software* legalmente relevante possui comunicação externa; se não permite a carga ou alteração de programas, parâmetros ou dados; se não permite a execução de programas; se não permite alterar o ambiente da aplicação legalmente relevante; se inclui controle de acesso; e se não permite uma mudança na configuração deste controle de acesso, subsequentemente; 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.

7.8 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.

7.9 Memorial descritivo

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

	NIT-SINST-006	REV. 00	PÁGINA 4/18
---	---------------	------------	----------------

7.10 Não legalmente relevante

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

7.11 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.

7.12 Requisitos gerais de *software* e *hardware*

Requisitos de *software* e *hardware* do RTM em questão que todos os instrumentos (medidores de umidade de grãos) devem satisfazer.

7.13 Requisitos específicos de *software* e *hardware*

Os requisitos que tratam de aspectos técnicos específicos referentes às tecnologias empregadas na concepção do medidor de umidade de grãos ou inserção de funcionalidades complementares. O instrumento MUG que possuir esses aspectos técnicos ou empregar essas funcionalidades tecnológicas específicas deve satisfazer o requisito específico do RTM em questão.

7.14 Selagem principal

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

7.15 Verificação de integridade

Processo/procedimento que tem como objetivo atestar que o(s) *software(s)*/dado(s)/parâmetro(s) instalado(s) no instrumento em verificação corresponde(m) exatamente à versão previamente aprovada para utilização no instrumento. Ou seja, um 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 umidade de grãos para avaliação de modelo será baseada nas seguintes fontes de evidências:

- a) documentação técnica, conforme descrito na norma NIT-Sinst-003; e
- b) ensaios funcionais.

	NIT-SINST-006	REV. 00	PÁGINA 5/18
---	----------------------	--------------------	------------------------

8.1.1 Ao se iniciar a análise de *software* de medidores de umidade de grãos, o técnico responsável deve 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.

8.1.4 O requerente deve fornecer todos os periféricos que se comunicam com o instrumento 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:

- a) análise do memorial descritivo (AMD);
- b) análise da documentação (AD);
- c) análise de código fonte [quando pertinente]; e
- d) ensaios funcionais de *software* (EFS).


8.2.2 Análise do memorial descritivo: 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.

8.2.3 Análise da documentação: o técnico responsável, na AD, deve verificar se os documentos fornecidos pelo fabricante evidenciam o cumprimento dos requisitos do Anexo B da Portaria Inmetro nº 047/2022, e se as soluções tecnológicas empregadas são adequadas para garantir a integridade e segurança da medição e do instrumento em si.

8.2.4 Documentação adicional pode ser requerida ao requerente caso a análise do memorial descritivo e demais documentos não forneça evidências adequadas do cumprimento dos requisitos do Anexo B da Portaria Inmetro nº 047/2022.

8.2.5 Análise de código fonte: consiste na análise de todo ou de parte do código fonte do *software* [legalmente relevante]. Esta análise torna-se necessária quando:

- a) não for possível demonstrar a completa ausência de “portas” de entrada para a interface de usuário, para comprovar/testar a influência da interface de entrada de dados num MUG. Nesses casos, existindo “portas” e comandos, ou na impossibilidade de comprovação da inexistência de comandos pelo esquemático, o requerente deve fornecer o código fonte completo e comentado do *software* do medidor de umidade de grãos sujeito à análise; e
- b) algum requisito específico de *software* e *hardware* for aplicável ao medidor de umidade de grãos. Nesses casos, será necessária a disponibilização ao Inmetro de todo o código fonte comentado do *software* legalmente relevante sujeito à análise.

	NIT-SINST-006	REV. 00	PÁGINA 6/18
---	----------------------	--------------------	------------------------

8.2.6 Ensaio funcional de *software*: consiste na análise do comportamento do *software* do instrumento em situações de operação real.

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

8.2.6.2 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) proteção e atualização dos parâmetros de configuração
- e) detecção de falhas;
- f) validação do *software*;
- g) composição do resultado de uma medição;
- h) confidencialidade de chaves;
- i) transferência de dados;
- j) carga de *software* legalmente relevante;
- k) carga de *software* não legalmente relevante;
- l) arquiteturas com componentes eletrônicos imutáveis;
- m) arquitetura com utilização de interfaces;
- n) arquiteturas com separação de *software* e/ou *hardware*; e
- o) arquiteturas com assinatura digital.

8.2.6.3 Uma relação de ensaios funcionais passíveis de serem realizados encontra-se no Anexo A desta norma.

8.2.6.4 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 (quando houver).

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

8.2.6.6 Através do ensaio funcional de *software*, 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.

	NIT-SINST-006	REV. 00	PÁGINA 7/18
---	---------------	------------	----------------

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 2.3 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.1.2 Podem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma para verificar a versão do *software* legalmente relevante instalado no instrumento.

9.2 Correção dos algoritmos e funções

9.2.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.4 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.2.1.1 Deve ser avaliado se a documentação descreve os algoritmos de medição (cálculo e arredondamentos dos resultados).

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 dos itens 2.5, 2.6 e 2.7 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

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

9.3.3 O requerente, quando necessário, 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.

9.3.4 Deve ser avaliado se o *software* legalmente relevante é protegido contra modificações inadmissíveis, cargas remotas não autorizadas e substituição de memória, se o gabinete do medidor de umidade de grãos é seguro (inviolável) e se a memória física não pode ser removida sem autorização.

9.3.4.1 Checar se a documentação fornece garantias de que o *software* legalmente relevante não pode ter modificações inadmissíveis, sendo que as medidas de proteção tomadas contra mudanças intencionais devem estar destacadas.

9.3.5 Podem ser realizados ensaios funcionais de *software*, constantes no Anexo A desta norma, para comprovar o atendimento dos requisitos.

	NIT-SINST-006	REV. 00	PÁGINA 8/18
---	---------------	------------	----------------

9.4 Proteção e atualização dos parâmetros de configuração

9.4.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.8 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.4.2 Deve ser avaliado se todos os parâmetros que fixam as características legalmente relevantes do medidor de umidade de grãos são protegidos contra modificações não autorizadas.

9.4.3 Deve ser avaliado se modificações das constantes de calibração são previamente autorizadas pelo Inmetro e se o Inmetro, como responsável, assina digitalmente os novos parâmetros.

9.4.4 Deve ser avaliado se o *software* do medidor de umidade de grãos somente pode efetuar mudanças em constantes de calibração após verificação (validação) da assinatura digital do Inmetro.

9.4.5 Deve ser avaliado se a mudança de uma constante de calibração configura um evento que, necessariamente, é registrado (em log de eventos).

9.4.6 Deve ser avaliado se a assinatura digital das constantes de medição tem validade máxima de 24 meses contados a partir da data de assinatura.

9.4.7 Com respeito à alteração de parâmetros legalmente relevantes, quando aplicáveis, 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;

9.4.8 Podem ser realizados ensaios funcionais de *software*, constantes no Anexo A desta norma, para comprovar o atendimento dos requisitos.

9.5 Detecção de falhas

9.5.1 Deve ser avaliado se o instrumento possui função de detecção de falhas e atende os requisitos do item 2.9 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.5.2 Checar se tanto o processo de detecção, quanto a reação à falha estão de acordo com o descrito na documentação constante do processo de aprovação de modelo.

9.5.2.1 A documentação deve conter a lista de falhas que são detectáveis, os respectivos algoritmos de detecção e as reações desencadeadas.

9.5.3 Podem ser realizados ensaios funcionais de *software*, constantes no Anexo A desta norma, para comprovar o atendimento dos requisitos.

	NIT-SINST-006	REV. 00	PÁGINA 9/18
---	---------------	------------	----------------

9.6 Validação do *software*

9.6.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.10 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.6.2 Checar se a documentação contém descrição dos casos de testes realizados para a validação do *software* frente aos requisitos do RTM e os resultados obtidos.

9.6.3 Se necessário, podem ser reproduzidos os casos de testes realizados, pelo requerente, para a validação do *software* frente aos requisitos do RTM e comparados os resultados obtidos.

9.7 Composição do resultado de uma medição

9.7.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.11 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.7.2 Deve ser avaliado se o resultado da medição do MUG contém os itens/campos obrigatórios estabelecidos em “I - quando exibido no display do medidor” e “II - quando impresso ou transmitido para outro sistema” do subitem 2.11.1 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.7.3 Checar se na documentação há:

- a) a descrição de todos os campos legais pertinentes exibidos no display; e
- b) a descrição de todos os campos legais pertinentes impressos ou enviados para outro sistema juntamente com a descrição dos algoritmos de assinatura utilizados, bem como dos mecanismos de criação e manutenção das chaves criptográficas.

9.7.4 Podem ser realizados ensaios funcionais de *software* para comprovar o atendimento dos requisitos.

9.8 Confidencialidade de chaves

9.8.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.12 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022.

9.8.2 Podem ser realizados ensaios funcionais de *software* para comprovar o atendimento dos requisitos.

10 REQUISITOS ESPECÍFICOS DE *SOFTWARE* E *HARDWARE*

10.1 Separação das partes legalmente relevantes

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 047/2022.

10.1.2 Podem ser realizados ensaios funcionais de *software*, constantes no Anexo A desta norma, para comprovar o atendimento dos requisitos.

 INMETRO	NIT-SINST-006	REV. 00	PÁGINA 10/18
--	---------------	------------	-----------------

10.2 Transmissão dos dados através de redes de comunicação

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 047/2022.

10.2.2 Podem ser realizados ensaios funcionais de *software*, constantes no Anexo A desta norma, para comprovar o atendimento dos requisitos.

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 047/2022.

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 Podem ser realizados ensaios funcionais de *software*, constantes no Anexo A desta norma, para comprovar o atendimento dos requisitos.

10.3.5 O requerente, quando necessário, 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.

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.

 INMETRO	NIT-SINST-006	REV. 00	PÁGINA 11/18
--	---------------	------------	-----------------

10.5 Comportamento dinâmico

10.5.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.5 do Anexo B do RTM aprovado pela Portaria Inmetro nº 047/2022 sobre comportamento dinâmico do processo de medição na coexistência de software não legalmente relevante com software legalmente relevante.

10.5.2 Podem ser realizados ensaios funcionais de *software* para comprovar o atendimento dos requisitos.

10.6 Capacidade de processamento

10.6.1 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 047/2022.

10.6.2 Podem ser realizados ensaios funcionais de *software* para comprovar o atendimento dos requisitos.

10.7 Capacidade de autodiagnóstico de falhas

10.7.1 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 047/2022.

10.7.2 Podem ser realizados ensaios funcionais de *software* para comprovar o atendimento dos requisitos.

10.8 Arquiteturas especiais

10.8.1 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 047/2022.

10.8.2 Podem ser realizados ensaios funcionais de *software* para checar o atendimento dos requisitos.

11 DISPOSIÇÕES GERAIS

11.1 Todas as evidências para o convencimento quanto ao cumprimento dos requisitos técnicos de *software* estabelecidos no RTM aprovado pela Portaria Inmetro nº 047/2022 devem ser providas pelo requerente.

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

	NIT-SINST-006	REV. 00	PÁGINA 12/18
---	----------------------	--------------------	-------------------------

12 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens revisados
00	Jan/2023	▪ Emissão inicial.

Quadro de aprovação		
	Nome	Atribuição
Elaborado por:	Rogerio Possidonio Nunes	Pesquisador-Tecnologista em Metrologia e Qualidade
Verificado por:	Alexandre Arosa Saturnino de Oliveira	Técnico em Metrologia e Qualidade
Aprovado por:	Ícaro dos Santos França	Chefe Substituto do Sinst

/ANEXO A

ANEXO A - ENSAIOS FUNCIONAIS DE SOFTWARE

Tabela 1 – Ensaaios funcionais de *software* baseados nos requisitos do Anexo B do RTM da Portaria Inmetro nº 047/2022

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
1	2.3	Versão do <i>software</i> legalmente relevante	Identificador de versão, estrutura e acesso.	1. Verificar se o identificador de versão do <i>software</i> existe, como é acessado e se é idêntico ao descrito na documentação. 2. Verificar a estrutura do identificador de versão. 3. Verificar se o identificador de versão de <i>software</i> legalmente relevante é claramente apresentado.
2	2.4	Correção dos algoritmos e funções	Exatidão metrológica da medição de umidade.	1. A ser executado pelo Sefiq de acordo com a norma NIT-Sefiq-005.
3	2.5, 2.6 e 2.7	Proteção de <i>software</i> e <i>hardware</i>	<p>Possibilidade de uso impróprio ou fraudulento do instrumento</p> <p>Selagem mecânica. Outros meios de proteção do <i>software</i> e <i>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>	1. 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). 2. Verificar se a selagem mecânica protege o instrumento contra modificações não autorizadas de seu <i>software</i> , <i>hardware</i> (por ex., mudança de memória) ou parâmetros legalmente relevantes. 3. Verificar se o rompimento do lacre (selo) deixa evidências. 4. 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. 5. 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 (ou documentação). 6. 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 (ou documentação). 7. Verificar a inviolabilidade dos componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes. 8. Verificar se a ferramenta de verificação de integridade fornecida atesta como íntegro um <i>firmware</i> íntegro carregado no instrumento/sistema de medição. 9. Verificar se a ferramenta de verificação de integridade fornecida atesta como não íntegro um <i>firmware</i> não íntegro carregado no instrumento/sistema de medição 10. Verificar a conformidade do método de verificação de integridade do <i>firmware</i> por meio da interface de verificação metrológica, de acordo com a Norma NIT-Sinst-020.

(continua)

4	2.8	Proteção e atualização dos parâmetros de configuração	Autorização do Inmetro para uso de constantes de calibração [nas curvas]	<ol style="list-style-type: none"> 1. Verificar se as modificações das constantes de calibração são previamente autorizadas pelo Inmetro e se o Inmetro, como responsável, assina digitalmente os novos parâmetros. 2. Verificar se o <i>software</i> do medidor de umidade de grãos somente pode efetuar mudanças em constantes de calibração após verificação (validação) da assinatura digital do Inmetro. 3. Verificar os registros (log de eventos) para checar se a mudança de uma constante de calibração configura um evento que, necessariamente, é registrado. 4. Observar se a assinatura digital das constantes de medição tem validade máxima de 24 meses contados a partir da data de assinatura. <p>OBS: a data de validade das constantes de calibração pode ser observada no resultado legalmente e metrologicamente completo de uma medição (no <i>display</i> ou impresso).</p>
			Assinatura das constantes de calibração	
			Registro de eventos (registro de auditoria)	
			Validade das constantes de calibração	
			Registro de auditoria de alteração de parâmetros legalmente relevantes	<ol style="list-style-type: none"> 1. Verificar se os meios técnicos utilizados para proteger partes do instrumento correspondem àqueles referenciados no memorial descritivo (ou documentação). 2. Verificar se apenas as funções documentadas podem ser ativadas pelas interfaces de comunicação e de usuário. 3. Verificar se as funções de interface permitem o uso fraudulento do instrumento. 4. 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 (ou documentação). 5. Verificar se a alteração de parâmetros ocorre apenas quando há abertura de proteção física ou acesso autenticado. 6. Verificar se há registro de alteração 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. 7. Verificar se os registros de auditoria são armazenados por, no mínimo, 5 (cinco) anos. 8. Verificar a disponibilização dos registros de auditoria para leitura. 9. Verificar a disponibilização dos valores atuais dos parâmetros legalmente relevantes para leitura. 10. Verificar a inviolabilidade dos componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes.
			Leitura de parâmetros legalmente relevantes em uso no instrumento	
			Método de verificação de integridade do <i>firmware</i> legalmente relevante	
5	2.9	Detecção de falhas	Reação às falhas descritas e verificação do desempenho do instrumento.	<ol style="list-style-type: none"> 1. Checar se o MUG possui função de detecção de falhas. 2. Colocar o instrumento no estado das falhas detectáveis e verificar se as reações contra as mesmas ocorrem do modo descrito no memorial descritivo (ou documentação).

(continua)

6	2.10	Validação do <i>software</i>	Processo de validação do <i>software</i>	<p>1. Se necessário, reproduzir os casos de testes realizados, pelo requerente, para a validação do <i>software</i> frente aos requisitos do RTM. OBS: podem ser reproduzidos aleatoriamente alguns dos casos de testes, e não a totalidade deles.</p> <p>2. Comparar os resultados obtidos.</p>
7	2.11	Composição do resultado de uma medição	Resultado da medição do MUG	<p>1. Verificar se o resultado da medição do MUG contém os itens/campos obrigatórios estabelecidos em:</p> <p>a) quando exibido no display do medidor; e</p> <p>b) quando impresso ou transmitido para outro sistema.</p>
8	2.12	Confidencialidade de chaves	Mecanismos de proteção das chaves secretas/ privadas	<p>1. Verificar se as chaves secretas/privadas são mantidas em segredo e protegidas contra quaisquer possibilidades de comprometimento. OBS: observar durante os ensaios, se o acesso às chaves criptográficas secretas/privadas é impedido, por exemplo, por meio de selagem da caixa de um dispositivo construído para esta finalidade. Nesses casos, pode não ser necessária uma proteção adicional de <i>software</i>; exemplo: a chave secreta/privada é armazenada em uma peça de <i>hardware</i> fisicamente selada, sendo que o <i>software</i> não oferece qualquer recurso para exibir ou editar esses dados.</p>
9	3.2	Separação das partes legalmente relevantes	<p>Separação entre partes legalmente relevantes e partes não legalmente relevantes</p> <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>1. Verificar se a distribuição física das partes legalmente relevantes e não legalmente relevantes está de acordo com o memorial descritivo ou documentação.</p> <p>2. Verificar se há uma parte do <i>software</i> englobando todos os módulos e parâmetros legalmente relevantes, claramente separada dos outros componentes de <i>software</i>. OBS: caso não haja separação de <i>software</i> todo ele será considerado relevante.</p> <p>3. 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>. [Ou são realizadas através de uma interface protetora que abrange todas as interações e fluxos de dados.]</p> <p>3. Verificar se há uma atribuição inequívoca de cada comando enviado através da interface de <i>software</i> para uma função ou uma alteração de dados do <i>software</i> legalmente relevante.</p> <p>4. Verificar a completude dos comandos emitidos via interface.</p> <p>5. Verificar se há códigos e dados não declarados [na documentação]. Os códigos e dados que não são declarados e documentados como comandos não podem ter qualquer efeito sobre o <i>software</i> legalmente relevante. OBS: a interface deve ser completamente documentada e quaisquer outras interações (ou fluxo de dados) não documentadas não podem ser realizadas nem pelo programador do <i>software</i> legalmente relevante, nem pelos programadores do <i>software</i> não relevante.</p>

				<p>6. Verificar se as partes legalmente relevantes são influenciadas por comandos não documentados recebidos através da interface de separação de <i>software</i> e/ou <i>hardware</i>.</p> <p>7. Verificar se quaisquer informações geradas pelo <i>software</i> que não é legalmente relevante só podem ser exibidas pelo MUG caso elas não possam ser confundidas com as informações que se originam a partir da parte legalmente relevante.</p>
10	3.3	Transmissão dos dados através de redes de comunicação	<p>[Formato e segurança da transmissão de dados]</p> <p>Compleitude dos dados transmitidos</p> <p>Integridade dos dados transmitidos</p> <p>Autenticidade dos dados transmitidos</p> <p>Confidencialidade das chaves</p> <p>Manipulação de dados corrompidos</p> <p>Atraso de transmissão</p> <p>Procedimentos de proteção contra a interrupção da transmissão ou outros erros</p>	<p>Nota – O teste/verificação dos requisitos a seguir, se aplica apenas quando o medidor de umidade de grãos utiliza internamente à cadeia legalmente relevante uma rede de comunicação para transmitir e receber dados das medições:</p> <ol style="list-style-type: none"> 1. Verificar a completude dos dados transmitidos; 2. Verificar a integridade dos dados transmitidos; 3. Verificar a autenticidade dos dados transmitidos; 4. Verificar a confidencialidade das chaves criptográficas secretas/privadas; 5. Verificar se os dados que são detectados como corrompidos não podem ser utilizados; 6. Verificar o atraso de medição, pois uma medição não pode ser influenciada pela comunicação. Verificar se, mesmo sob as piores condições do meio de comunicação (alto tráfego, por exemplo), a medição não será invalidada; 7. Checar se o usuário não pode ser capaz de corromper dados das medições em função da supressão da transmissão. E mesmo que os serviços de rede de comunicação se tornem indisponíveis, não deve haver perda de dados das medições, devendo o dispositivo mostrador sinalizar tal situação.
11	3.4	Carga de <i>software</i> legalmente relevante	<p>Aprovação do <i>software</i> pelo Inmetro</p> <p>Permissão do operador (Controle de acesso)</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>	<ol style="list-style-type: none"> 1. Verificar se os mecanismos que garantem que o <i>software</i> tenha sido aprovado pelo Inmetro correspondem àqueles referenciados no memorial descritivo ou documentação. 2. Verificar se o <i>software</i> só pode ser carregado com a permissão explícita do operador do medidor de umidade de grãos. 3. Verificar se a carga de <i>software</i> é automática, ou seja, uma vez iniciada independe do operador. 4. Verificar se o instrumento realiza medições durante o processo de carga de <i>software</i>. 5. 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. 6. Atestar a existência de autenticação de usuário para realização da carga de <i>software</i>. 7. Verificar se os mecanismos que garantem a autenticidade e a integridade do <i>software</i> correspondem àqueles referenciados no memorial descritivo ou documentação.

			<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>8. Simular situação de falha da autenticidade e integridade do <i>software</i> a ser carregado e observar seu descarte e o uso da versão da anterior. Alternativamente o instrumento pode tornar-se inoperante.</p> <p>9. Verificar se a carga de <i>software</i> ocorre apenas quando há abertura de proteção física ou acesso autenticado.</p> <p>10. 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>11. Verificar se os registros de auditoria são armazenados por, no mínimo, 5 (cinco) anos.</p> <p>12. Verificar a disponibilização dos registros de auditoria para leitura.</p>
12	3.5	Comportamento dinâmico	Influência da coexistência de <i>software</i> não legalmente relevante no comportamento dinâmico do processo de medição	1. Caso haja um compartilhamento de recursos de processamento, verificar se o <i>software</i> legalmente tem sempre a disponibilidade necessária para o seu bom funcionamento (ex. prioridade superior ao software não relevante).
13	3.6	Capacidade de processamento	Capacidade de processamento nas situações de maior carga	<p>1. Verificar todos os elementos constituintes do medidor de umidade de grãos que tenham uso compartilhado (concentradores, redes de comunicação) e se eles estão dimensionados adequadamente em função dos instantes de maior carga.</p> <p>2. Verificar se a medição é comprometida por atrasos ou bloqueios ocorridos pela realização de outras tarefas.</p>
14	3.7	Capacidade de autodiagnóstico de falhas	Capacidade do MUG de diagnosticar um estado de mau funcionamento	<p>1. Reproduzir, se possível, os testes realizados pelo requerente para comprovar a capacidade de autodiagnóstico de falhas.</p> <p>OBS: este requisito se aplica apenas quando o medidor de umidade de grãos, além de prover detecção de falhas, é capaz de diagnosticar um estado de mau funcionamento.</p>
16	3.8	Arquiteturas especiais [com assinatura digital]	<p>Ferramentas fornecidas pelo fabricante</p> <p>Armazenamento de dados</p> <p>Gestão de chaves criptográficas</p> <p>OBS: 3.8.1 Para sistemas cujas grandezas de entrada sejam assinadas digitalmente antes a aplicação da função de medição da umidade de grão:</p>	<p>1. Verificar a ferramenta de publicação e conferência dos dados assinados.</p> <p>2. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação.</p> <p>3. Simular situação de falha na chave pública e verificar se a ferramenta indica tal situação.</p> <p>4. Verificar a ferramenta de reconstituição do valor final da medição a partir dos dados assinados.</p> <p>5. Simular situação de falha nos dados assinados e verificar se a ferramenta indica tal situação.</p> <p>6. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação.</p>

	NIT-SINST-006	REV. 00	PÁGINA 18/18
---	----------------------	--------------------	-------------------------

			<p>I - o Inmetro, após análise da arquitetura do medidor de umidade de grãos, pode dispensar a entrega de parte da documentação a que se refere o subitem 2.5.4;</p> <p>II - não é necessária a assinatura digital por parte do Inmetro, requisito estabelecido no subitem 2.8, dos parâmetros de calibração;</p>	<p>7. Verificar se os dados ou valores assinados, juntamente com a respectiva assinatura digital, são armazenados por, no mínimo, 60 dias.</p> <p>8. Verificar se as chaves criptográficas privadas são mantidas secretas e seguras internamente ao instrumento.</p>
--	--	--	---	--

Fonte: Dimel/Disme/Sinst