SUMÁRIO

1 OBJETIVO

Esta Norma estabelece os procedimentos a serem utilizados na análise de software para avaliação de modelo de medidores eletrônicos de água potável fria e água quente.

2 CAMPO DE APLICAÇÃO

Esta Norma aplica-se à Dimel/Disme/Sinst.

3 RESPONSABILIDADE

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

4 DOCUMENTOS DE REFERÊNCIA

Portaria Inmetro nº 295 de 29/06/2018	Aprova o RTM sobre de medidores eletrônicos de água potável fria e água quente e seu Anexo – Requisitos Técnicos de Segurança de Software e Hardware
Portaria Inmetro nº 232 de 08/05/2012	Vocabulário Internacional de Metrologia: Conceitos fundamentais e gerais e termos associados (VIM) - 1a. Edição Luso-brasileira
Portaria Inmetro nº 150 de 29/03/2016	Vocabulário Internacional de Termos de Metrologia Legal
OIML D 31/2008	General requirements for software controlled measuring instruments
OIML D 11/2004	General requirements for electronic measuring instruments

(Continua)

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

Não aplicável.

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.

AM	Avaliação de Modelo
AMD	Análise do Memorial Descritivo
EFS	Ensaio Funcional de Software
NIST	National Institute of Standards and Technology
OTP	One-time programmable
RTM	Regulamento Técnico Metrológico
VIM	Vocabulário Internacional de Metrologia
VIML	Vocabulário Internacional de Metrologia Legal

6.2 Termos

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

6.2.2 Assinatura digital - Código atribuído a um arquivo digital de forma a atestar sua integridade, autenticidade e não repúdio.

6.2.3 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.

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

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

6.2.6 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.
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.

6.2.7 Legalmente relevante – Todos os módulos de software (programas, sub-rotinas, objetos, etc.) que executam funções legalmente relevantes ou que contêm domínios de dados legalmente relevantes formam a parte de software legalmente relevante de um instrumento de medição. Mais especificamente, isso inclui todos os módulos de software que:
a) têm impacto no cálculo de uma unidade de medida legal;
b) contribuem para funções como: exibir, proteger e armazenar dados legalmente relevantes;
c) identificam os softwares legalmente relevantes ou
d) executam carga de software legalmente relevante.

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

6.2.9 Não legalmente relevante – Todo software/hardware/dados presentes no instrumento que não são legalmente relevantes.

6.2.10 Requerente - É toda pessoa jurídica, pública ou privada, nacional ou estrangeira, sediada no Brasil, que desenvolva atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de instrumentos.

6.2.11 Requisitos gerais de software – O software e o hardware considerados legalmente relevantes devem satisfazer à totalidade dos requisitos gerais do RTM em questão

6.2.12 Requisitos específicos de software – O software e o hardware legalmente relevantes que empregarem funcionalidades tecnológicas específicas devem satisfazer à totalidade dos requisitos específicos do RTM em questão.

6.2.13 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.

6.2.14 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.

7 ORIENTAÇÕES GERAIS

7.1 A análise de software dos medidores eletrônicos de água potável fria e água quente para avaliação de modelo será baseada nas seguintes fontes de evidências:
a) Documentação técnica, conforme descrito na Norma NIT-Sinst-003;
b) Ensaios funcionais;

7.1.2 Ao se iniciar a análise de software de medidores eletrônicos de água potável fria e água quente, o técnico responsável deverá realizar o estudo preliminar do pacote de documentação técnica de forma a familiarizar-se com o instrumento.

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

7.1.4 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.

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

7.2 Métodos de análise

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

7.2.2 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.

7.2.2.1 O técnico responsável deve verificar se os documentos fornecidos pelo fabricante evidenciam o cumprimento dos requisitos do Anexo da Portaria Inmetro 295/2018, e se as soluções tecnológicas empregadas são adequadas para garantir a integridade e segurança da medição e do instrumento em si.

7.2.2.2 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 da Portaria 295/2018.

7.2.3 Ensaio funcional de software (EFS): consiste na análise do comportamento do software do instrumento 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 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) Transferência de dados;
f) Carga de software legalmente relevante;
g) Carga de software não legalmente relevante;
h) Arquiteturas com componentes eletrônicos imutáveis;
i) Arquitetura com utilização de interfaces;
j) Arquiteturas com separação de software e/ou hardware;
k) Arquiteturas com assinatura digital.

7.2.3.3 A relação de ensaios funcionais passíveis 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 nos casos de teste, manual operacional, memoriais descritivos e padrão de funcionamento do instrumento e equipamentos de teste.

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 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.

8 REQUISITOS GERAIS DE SOFTWARE E HARDWARE

8.1 Versão do software legalmente relevante

8.1.1 Deve ser avaliado se o instrumento atende os requisitos do item 3.2 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

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

8.2 Correção dos algoritmos e funções

8.2.1 Deve ser avaliado se o instrumento atende os requisitos do item 3.3 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

8.2.2 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.

8.3 Proteção de software e hardware

8.3.1 Deve ser avaliado se o instrumento atende os requisitos do item 3.4 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

8.3.2 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.

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

8.3.5 O requerente deve fornecer arquivos binários, 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 a proteção contra mudanças acidentais.

8.4 Detecção de falhas

8.4.1 Deve ser avaliado se o instrumento atende os requisitos do item 3.5 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

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

8.5 Documentação requerida para os requisitos gerais

8.5.1 Deve ser avaliado se a documentação entregue pelo requerente encontra-se completa de acordo com o exigido no item 3.6 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

9 REQUISITOS ESPECÍFICOS DE SOFTWARE E HARDWARE

9.1 Transferência de dados

9.1.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 4.2 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A)

9.1.2 Avaliar o software do computador tipo U que verifica dados recebidos por este. Esta avaliação pode ser dispensada sob todas as seguintes condições:

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

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

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

9.2 Carga de software legalmente relevante

9.2.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 4.3 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

9.2.2 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.

9.2.3 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;
c) Implementação de comando de protocolo de comunicação que possibilite habilitar a expiração da chave (senha) de autenticação, se aplicável;

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

9.2.5 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.

9.3 Carga de software não legalmente relevante

9.3.1 O software não legalmente relevante não é passível de aprovação conforme indicado no item 4.4.1 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

9.3.2 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.

9.4 Arquitetura com componentes eletrônicos imutáveis

9.4.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 4.5 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

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

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

9.5 Arquiteturas com utilização de interfaces

9.5.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 4.6 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

9.5.2 Com respeito à alteração de parâmetros legalmente relevantes, são requisitos mínimos:
a) Uso compulsório de autenticação aprovada segundo a versão mais atual do documento NIST Special Publication 800-57 Part 1;

b) Implementação de comando de protocolo de comunicação que possibilite a alteração da chave (senha) de autenticação;
c) Implementação de comando de protocolo de comunicação que possibilite habilitar a expiração da chave (senha) de autenticação;

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

9.6 Arquiteturas com separação de software e/ou hardware

9.6.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 4.7 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

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

9.7 Arquiteturas com assinatura digital

9.7.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 4.8 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A)

9.7.2 As chaves criptográficas devem ser únicas para cada instrumento.

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

9.8 Documentação requerida para os requisitos específicos

9.8.1 Deve ser avaliado, onde aplicável, se a documentação entregue pelo requerente encontra-se completa de acordo com o exigido no item 4.9 do RTM aprovado pela Portaria Inmetro nº 295/2018 (Anexo A).

10 DISPOSIÇÕES GERAIS

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

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

11 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens revisados
00	Junho/2018	▪ Emissão inicial

Quadro de aprovação		
	Nome	**Atribuição**
Elaborado por:	Fabiano de Oliveira Leitão	Pesquisador-tecnologista em metrologia e qualidade
Verificado por:	Carlos Eduardo Cardoso Galhardo Marcos Trevisan Vasconcellos Juliana Wilm Guedes Amsterdam de J. S. M. de Mendonça	Coordenador da qualidade do Sinst Pesquisador-tecnologista em metrologia e qualidade Estagiária Coordenador da qualidade da Dimel
Aprovado por:	Bruno Erthal Abreu	Chefe do Sinst

/ANEXO A

ANEXO A - ENSAIOS FUNCIONAIS DE SOFTWARE

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
1	3.2	Versão do software legalmente relevante	Identificador de versão, estrutura e acesso.	1. Verificar se o identificador de versão existe, como é acessado e se é idêntico ao descrito na documentação. Verificar a estrutura do identificador de versão. 2. Verificar se o identificador de versão de software legalmente relevante é claramente apresentado
2	3.3	Correção dos algoritmos e funções	Exatidão metrológica da medição de água	1. A ser executado pelo Seflu de acordo com a norma NIT-Seflu-014.
3	3.4	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. Reação do instrumento a modificações acidentais ou não autorizadas de seu software. Reação do instrumento a modificações acidentais ou não autorizadas de seus parâmetros legalmente relevantes. Influência das partes legalmente relevantes do instrumento por outras partes do sistema de medição. Procedimento de verificação de integridade, sucesso da verificação, falha da verificação.	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 software ou parâmetros legalmente relevantes. 3. 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 software ou parâmetros legalmente relevantes. 4. Simular situações de falha acidental/não autorizada no software do instrumento e observar se a reação está de acordo com o memorial descritivo. 5. 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.
4	3.5	Detecção de falhas	Reação às falhas descritas e verificação do desempenho do instrumento.	1. Colocar o instrumento no estado das falhas detectáveis e verificar se as reações contra as mesmas ocorrem do modo descrito no memorial descritivo.
5	4.2	Transferência de dados	Garantia da autenticidade, integridade e carimbo de tempo dos dados transferidos	1. Verificar se os mecanismos que garantem autenticidade, integridade e carimbo de tempo dos

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Atrasos de transferência Carimbo de tempo	dados transmitidos correspondem àqueles referenciados no memorial descritivo. 2. Verificar se os dados transmitidos têm sua autenticidade e integridade checadas após a recepção. 3. Simular situação de falha da autenticidade e integridade dos dados 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.
6	4.3	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 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	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. 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 9.2.3 desta norma.

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
				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 uso da versão da anterior. Alternativamente o instrumento pode 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.
7	4.5	Arquiteturas com componentes eletrônicos imutáveis	Imutabilidade de componentes eletrônicos	1. A critério do técnico responsável pela avaliação de modelo, podem ser efetuados testes complementares que comprovem a imutabilidade de componente eletrônico responsável por processamento de informação legalmente relevante.
8	4.6	Arquitetura com utilização de interfaces	Proteção do instrumento Funções ativadas pela interface Alteração de parâmetros legalmente relevantes Registro de auditoria de alteração de parâmetros legalmente relevantes	1. Verificar se os meios técnicos utilizados para proteger partes do instrumento correspondem àqueles referenciados no memorial descritivo. 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

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Leitura de parâmetros legalmente relevantes em uso no instrumento Método de verificação de integridade do firmware legalmente relevante	autorização do usuário e se este procedimento se dá conforme apresentado no memorial descritivo. 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. 11. Verificar se a ferramenta de verificação de integridade fornecida atesta como íntegro um firmware íntegro carregado no instrumento/sistema de medição. 12. Verificar se a ferramenta de verificação de integridade fornecida atesta como não íntegro um firmware não íntegro carregado no instrumento/sistema de medição 13. Verificar a conformidade do método de verificação de integridade do firmware por meio da interface de verificação metrológica, de acordo com a Norma NIT-Sinst-020
11	4.7	Arquiteturas com separação de software e/ou hardware	Identificação das partes legalmente relevantes e não legalmente relevantes Comunicação entre as 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. 2. Verificar se todas as comunicações entre as partes legalmente relevantes e não legalmente relevantes são

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Influência das partes legalmente relevantes Comportamento da medição	realizadas 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. 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.
12	4.8	Arquiteturas com assinatura digital	Ferramentas fornecidas pelo fabricante Armazenamento de dados Gestão de chaves criptográficas	1. Verificar a ferramenta de publicação e conferência dos dados assinados. 2. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação. 3. Simular situação de falha na chave pública e verificar se a ferramenta indica tal situação. 4. Verificar a ferramenta de reconstituição do valor final da medição a partir dos dados assinados. 5. Simular situação de falha nos dados assinados e verificar se a ferramenta indica tal situação. 6. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação. 7. Verificar se os dados ou valores assinados, juntamente com a respectiva assinatura digital, são armazenados por, no mínimo, 60 dias. 8. Verificar se as chaves criptográficas privadas são mantidas secretas e seguras internamente ao instrumento.

Fonte: Dimel/Disme/Sinst