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 se aplica à Dimel/Dgtec/Sinst e laboratórios acreditados.

3 RESPONSABILIDADE

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

4 DOCUMENTOS DE REFERÊNCIA

Portaria Inmetro nº 155 de 30/03/2022	Aprova o Regulamento Técnico Metrológico consolidado para medidores para consumo de água potável fria e água quente
Portaria Inmetro nº 232 de 08/05/2012	Adota, no Brasil, o Vocabulário Internacional de Metrologia: Conceitos fundamentais e gerais e termos associados (VIM) - 1a. Edição Luso-brasileira
Portaria Inmetro nº 150 de 29/03/2016	Adota, no Brasil, o Vocabulário Internacional de Termos de Metrologia Legal (VIML)
OIML D 31/2008	*General requirements for software controlled measuring instruments*

(continua)

OIML D 11/2004	*General requirements for electronic measuring instruments*
WELMEC *Software Guide* 7.2	*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 s*oftware*
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*
OS	*Operating System* (Sistema Operacional)
OTP	*One-time programmable*
RBMLQ-I	Rede Brasileira de Metrologia 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 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.

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 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, sem autenticação ou rompimento de selagem; 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.

7.7 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.

7.8 Memorial descritivo

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

7.9 Não legalmente relevante

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

7.10 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.

7.11 Requisitos gerais de *software*

Requisitos de *software* e *hardware* do RTM em questão que todos os instrumentos (medidores de água potável fria e água quente) devem satisfazer.

7.12 Requisitos específicos de *software*

Requisitos que tratam de aspectos técnicos específicos referentes às tecnologias empregadas na concepção do medidor 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.

7.13 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.

7.14 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 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; e
b) ensaios funcionais;

8.1.1 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.

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 desta norma.

8.2 Métodos de análise

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

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 155/2022, 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 155/2022.

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

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

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

a) versão do *software* legalmente relevante;
b) correção dos algoritmos e funções;
c) proteção de *software* e *hardware*;
d) detecção de falhas;
e) 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.

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

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

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

8.2.3.6 Através do ensaio funcional de *software*, deve ser analisada a operação normal do instrumento. 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 155/2022

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

9.2 Correção dos algoritmos e funções

9.2.1 Deve ser avaliado se o instrumento atende os requisitos do item 2.3 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

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 155/2022.

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

9.3.4 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.

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 155/2022

9.4.2 Devem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

9.5 Documentação requerida para os requisitos gerais

9.5.1 Deve ser avaliado se a documentação entregue pelo requerente encontra-se completa, de acordo com o exigido no item 2.6 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

10 REQUISITOS ESPECÍFICOS DE *SOFTWARE* E *HARDWARE*

10.1 Transferência de dados

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 155/2022.

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

10.1.2.1 A autenticidade e integridade dos dados transmitidos são garantidas pela utilização da assinatura digital destes dados.

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

10.1.3 Devem ser realizados, quando necessário, ensaios funcionais de *software* constantes no Anexo A desta norma.

10.2 Carga de *software* legalmente relevante

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 155/2022.

10.2.2 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, conforme requisitos do item 11 da NIT-Sinst-003.

10.2.3 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; e
c) implementação de comando de protocolo de comunicação que possibilite habilitar a expiração da chave (senha) de autenticação, se aplicável.

10.2.4 Devem ser realizados ensaios funcionais de *software* constantes no Anexo A desta norma.

10.2.5 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*.

10.3 Carga de *software* não legalmente relevante

10.3.1 O *software* não legalmente relevante não é passível de aprovação conforme indicado no item 3.4.1 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

10.3.2 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.

10.4 Arquitetura com componentes eletrônicos imutáveis

10.4.1 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 155/2022.

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

10.4.3 Devem ser realizados, quando necessário, ensaios funcionais de *software* constantes no Anexo A desta norma.

10.5 Arquiteturas com utilização de interfaces

10.5.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.6 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

10.5.2 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; e
c) implementação de comando de protocolo de comunicação que possibilite habilitar a expiração da chave (senha) de autenticação.

10.5.3 Devem ser realizados, quando necessário, ensaios funcionais de *software* constantes no Anexo A desta norma.

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

10.6.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.7 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

10.6.2 Devem ser realizados, quando necessário, ensaios funcionais de *software* constantes no Anexo A desta norma.

10.7 Arquiteturas com assinatura digital

10.7.1 Deve ser avaliado, se pertinente, se o instrumento atende os requisitos do item 3.8 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

10.7.2 As chaves criptográficas devem ser únicas para cada instrumento.

10.7.3 Devem ser realizados, quando necessário, ensaios funcionais de *software* constantes no Anexo A desta norma.

10.8 Documentação requerida para os requisitos específicos

10.8.1 Deve ser avaliado, onde aplicável, se a documentação entregue pelo requerente encontra-se completa, de acordo com o exigido no item 3.9 do Anexo B do RTM aprovado pela Portaria Inmetro nº 155/2022.

11 DISPOSIÇÕES GERAIS

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

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

12 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens revisados
01	Mar/2024	▪ Atualização dos requisitos da Portaria Inmetro nº 155, de 30 de março de 2022; ▪ Adequação a NIG-Gabin-040; e ▪ Alterações no Anexo A - Ensaios Funcionais nos itens 2.2, 2.4 e 3.8.

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*

#	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 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 *software* legalmente relevante é claramente apresentado
2	2.3	Correção dos algoritmos e funções	Exatidão metrológica da medição de água	1. Ensaio a ser executado pelo Seflu.
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. 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 a documentação. 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	2.5	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	3.2	Transferência de dados	Garantia da autenticidade, integridade e carimbo de tempo dos dados transferidos. Atrasos de transferência	1. Verificar se os mecanismos que garantem autenticidade, integridade e carimbo de tempo dos dados transmitidos correspondem àqueles referenciados no memorial descritivo.

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Carimbo de tempo	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	3.3	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, e que atendem às exigências do item 11 da NIT-Sinst-003. 2. Verificar se a carga de *software* é automática, ou seja, uma vez iniciada independe do operador. 3. Verificar se o instrumento não 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 10.2.3 desta norma. 6. Verificar se os mecanismos que garantem a

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
				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	3.5	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	3.6	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 Leitura de parâmetros legalmente relevantes em uso no instrumento	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 autorização do usuário e se este

#	ITEM	REQUISITO	CARACTERÍSTICAS ANALISADAS	DESCRIÇÃO DO ENSAIO FUNCIONAL
			Método de verificação de integridade do *firmware* legalmente relevante	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.
9	3.7	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.
10	3.8	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. Verificar se o ambiente de gestão das chaves criptográficas é eficaz na proteção contra extração e comprometimento com base nos critérios estabelecidos em documentos FIPS NIST. 3. Simular situação de falha na assinatura digital e verificar se a ferramenta indica tal situação. 4. Simular situação de falha na chave pública e verificar se a ferramenta indica tal situação. 5. Verificar a ferramenta de reconstituição do valor final da medição a partir dos dados assinados. 6. Simular situação de falha nos dados assinados 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/Dgtec/Sinst