Portaria n.º 47, de 22 de janeiro de 2016.

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA – Inmetro, no uso de suas atribuições, conferidas pelo parágrafo 3º do artigo 4º da Lei n.° 5.966, de 11 de dezembro de 1973, e tendo em vista o disposto nos incisos II e III do artigo 3° da Lei n.° 9.933, de 20 de dezembro de 1999, no inciso V do artigo 18 da Estrutura Regimental do Inmetro, aprovado pelo Decreto nº 6.275, de 28 de novembro de 2007, e pela alínea **a** do subitem 4.1 da Regulamentação Metrológica aprovada pela Resolução n° 11, de 12 de outubro de 1988, do Conselho Nacional de Metrologia, Normalização e Qualidade Industrial – Conmetro.

Considerando a Portaria Inmetro nº 375, de 24 de julho de 2013, que aprova o Regulamento Técnico Metrológico (RTM) sobre instrumentos de pesagem automáticos de veículos rodoviários em movimento e seu Anexo – Requisitos de software;

Considerando a Recomendação Internacional R 134-1: 2006 da Organização Internacional de Metrologia Legal da qual o Brasil é País-Membro;

Considerando o pleito do setor produtivo quanto à impossibilidade de atendimento aos erros máximos admissíveis especificados no RTM, aprovado pela Portaria Inmetro n° 375/2013, o que pode impedir a comercialização dos instrumentos de medição;

Considerando que a carência de instrumentos de pesagem automáticos de veículos no mercado consumerista pode prejudicar a fiscalização do excesso de peso nas rodovias brasileiras;

Considerando que o assunto foi amplamente discutido com as partes interessadas na regulamentação técnica metrológica sobre os instrumentos de pesagem automáticos de veículos rodoviários em movimento, no sentido de adaptar a condições exequíveis, resolve:

Art. 1° Substituir a Tabela 1 do subitem 3.1.1 do RTM, aprovado pela Portaria Inmetro nº 375/2013, que passará a viger, conforme segue:

Tabela 1

Percentagem do valor verdadeiro convencional da massa do veículo (6.6)	
Aprovação de Modelo, Verificação inicial e Verificação subsequente (±)	Inspeção em serviço (±)
2,5%	3%

Art. 2° Substituir a Tabela 2 do subitem 3.1.2.1 do RTM, aprovado pela Portaria Inmetro nº 375/2013, que passará a viger conforme segue:

Tabela 2

Percentagem do valor verdadeiro convencional da carga estática de referência por eixo isolado	
Aprovação de Modelo, Verificação inicial e Verificação subsequente (±)	Inspeção em serviço (±)
4%	5%

Art. 3° Substituir a Tabela 3 do subitem 3.1.2.2 do RTM, aprovado pela Portaria Inmetro nº 375/2013, que passará a viger conforme segue:

Tabela 3

Percentagem da média corrigida da carga por eixo e conjunto de eixos (6.10)	
Aprovação de Modelo, Verificação inicial e Verificação subsequente (±)	Inspeção em serviço (±)
4%	5%

Art. 4º Determinar que o subitem 1.2.3 da Portaria Inmetro nº 375/2013, incluído pela Portaria Inmetro nº 403, de 15 de agosto de 2013, passará a viger com a seguinte redação:

...

"1.2.3 Este regulamento não se aplica aos instrumentos utilizados para pesagem de veículos tanque transportando líquidos a granel." (NR)

...

Art. 5º Determinar que o art. 2º da Portaria Inmetro nº 403/2013, passará a viger com a seguinte redação:

...

"Art. 2º Estabelecer que os instrumentos de pesagem automáticos de veículos rodoviários em movimento, que possuem portaria de aprovação de modelo, publicada anteriormente à vigência da Portaria nº 375, de 24 de julho de 2013, não podem ser utilizados para pesagem de veículos tanque transportando líquidos a granel." (NR).

Art. 6º Substituir o Anexo – Requisitos de *Software,* da Portaria Inmetro nº 375/2013, pelo Anexo ora aprovado, denominado Requisitos Técnicos de Segurança de *Software* e *Hardware* para Instrumentos de Pesagem Automáticos de Veículos Rodoviários em Movimento.

Art. 7º Determinar que o art. 3° da Portaria Inmetro n° 375/2013, passará a viger com a seguinte redação:

...

"Art. 3° Estabelecer que os instrumentos que possuírem portaria de aprovação de modelo publicada anteriormente à vigência da Portaria Inmetro nº 375, de 24 de julho de 2013, poderão ser submetidos à verificação inicial até 30 de junho de 2016.

§ 1° Os instrumentos descritos no *caput* deverão atender aos erros máximos admissíveis para a verificação inicial, de acordo com o RTM ora aprovado.

§ 2° Para as verificações iniciais descritas no *caput* deverão ser aplicados os métodos de ensaio anexos às respectivas portarias de aprovação dos modelos.

§ 3° A partir de 1° de julho de 2016 apenas os instrumentos que possuírem portaria de aprovação de modelo publicada durante a vigência da Portaria Inmetro nº 375/2013, poderão ser submetidos à verificação inicial." (NR)

...

Art. 8º Determinar que o art. 4° da Portaria Inmetro n° 375/2013, passará a viger com a seguinte redação:

...

"Art. 4° Estabelecer que os instrumentos possuidores de portaria de aprovação de modelo publicada anteriormente à vigência da Portaria Inmetro nº 375/2013, e que permanecerem em uso, poderão ser submetidos às verificações subsequentes até 30 de junho de 2017." (NR)

...

Art. 9º Determinar que o art. 5° da Portaria Inmetro n° 375/2013, passará a viger com a seguinte redação:

...

"Art. 5° Estabelecer que a partir de 1° de julho de 2017 todos os instrumentos em uso deverão atender integralmente aos requisitos do RTM ora aprovado, inclusive quanto aos métodos de ensaio." (NR)

...

Art. 10 Esta Portaria entrará em vigor na data de sua publicação no Diário Oficial da União.

LUÍS FERNANDO PANELLI CESAR

ANEXO – REQUISITOS TÉCNICOS DE SEGURANÇA DE *SOFTWARE* E *HARDWARE* PARA INSTRUMENTOS DE PESAGEM AUTOMÁTICOS DE VEÍCULOS RODOVIÁRIOS EM MOVIMENTO

1. OBJETIVO E CAMPO DE APLICAÇÃO

1.1 Este anexo estabelece os requisitos técnicos de segurança de *software* e *hardware* a que devem atender os instrumentos de pesagem automáticos de veículos rodoviários em movimento e seus módulos, controlados por *software*, doravante denominados instrumentos, nos processos de avaliação de modelo, verificação inicial, verificações subsequentes e inspeções.

1.2 Este anexo objetiva garantir adequado nível de confiança na medição de massa de veículos, carga por eixo e por conjunto de eixos através do instrumento, assegurando medições que satisfaçam os erros máximos admissíveis e características que impeçam ou evidenciem a ocorrência de fraudes metrológicas.

1.3 Todas as evidências para o cumprimento dos requisitos técnicos de segurança de *software* e *hardware* estabelecidos no presente anexo devem ser providas pelo requerente do processo de avaliação de modelo.

1.4 O instrumento deve atender a totalidade dos requisitos gerais e, se implementados, os requisitos específicos correspondentes.

2. TERMINOLOGIA

2.1 Assinatura digital: esquema matemático para demonstrar a autenticidade de uma mensagem ou documento digital.

2.2 Autenticidade: garantia da identidade declarada/alegada de um usuário, processo, dispositivo ou dados.

2.3 Cadeia legalmente relevante: eventos do processo de medição que compreendem a aquisição dos dados, seu processamento e a publicação do valor da medição.

2.4 Carga de *software*: processo de transferência de *software* para os dispositivos de *hardware* do instrumento através de qualquer meio técnico apropriado.

2.5 Carimbo de tempo: valor de tempo único e monotonicamente crescente.

2.6 Computador universal ou computador tipo U: computador que não é construído para um propósito específico, mas que pode ser adaptado às tarefas metrológicas por *software*.

2.6.1 Em geral este *software* é executado através de um sistema operacional que permite a carga e execução de *software*s para propósitos específicos.

2.7 Dispositivo indicador: dispositivo que apresenta os resultados da medição.

2.8 Domínio de dados: local da memória que cada *software* necessita para efetuar o processamento de dados.

2.9 Integridade: garantia de que os dados, *software*, ou parâmetros não foram submetidos a alterações, intencionais ou não intencionais, durante o uso, reparo, manutenção, transferência ou armazenamento.

2.10 Interface de comunicação: qualquer tipo de interface (óptica, rádio, eletrônica etc.) que habilite a transferência de informações entre dispositivos do instrumento, ou com dispositivos externos.

2.11 Interface de usuário: interface que permite a troca de informações entre um usuário ou operador e o instrumento; por exemplo, chaves, teclados, mouses, displays, monitores, impressoras, telas sensíveis ao toque, janelas de *software* em uma tela, incluindo o *software* que as gera.

2.12 Interface de separação de *software*: conjunto de componentes de *hardware*/*software* que define a separação entre módulos de *software* legalmente relevantes e não legalmente relevantes.

2.13 Interface de verificação metrológica: interface que permite a troca de informações legalmente relevantes entre um agente metrológico e o instrumento ou seus componentes de *software* e *hardware*.

2.14 Irretratabilidade: garantia de não-repúdio à origem de informação ou dados oriundos de um instrumento.

2.15 Legalmente relevante: atributo de uma parte de um instrumento de medição, de um dispositivo, *software*, ou seus dados, submetidos ao controle legal (por exemplo, constantes de calibração).

2.16 Registro de auditoria: conjunto de registros cada qual contendo dados sobre um determinado evento e/ou alteração no instrumento, que sejam legalmente relevantes, e passíveis de influenciar suas características metrológicas.
2.17 Requisitos gerais: requisitos que tratam de aspectos técnicos referentes às tecnologias de uso geral em instrumentos controlados por *software*.
2.18 Requisitos específicos: requisitos que tratam de aspectos técnicos referentes às tecnologias específicas utilizadas no instrumento ou à inclusão de funcionalidades complementares.
2.19 Separação de *software*: separação do *software* de um instrumento nas partes legalmente relevante e não legalmente relevante, que se comunicam através de uma interface de separação de *software*.
2.20 Verificação de integridade: procedimento que verifica se um arquivo, *software* ou firmware corresponde a um arquivo, *software* ou firmware previamente conhecido.
2.21 Versão de *software*: sequência de caracteres que identifica univocamente um módulo de *software* e suas alterações.

3. REQUISITOS GERAIS DE *SOFTWARE* E *HARDWARE*
3.1 O *software* e o *hardware* considerados legalmente relevantes devem satisfazer à totalidade dos requisitos gerais.
3.2 Versão do *software* legalmente relevante
3.2.1 O *software* legalmente relevante do instrumento e/ou de suas partes deve possuir uma versão que o identifique univocamente.
3.2.2 Cada alteração no *software* legalmente relevante deverá possuir uma versão diferente das versões anteriores.
3.3 Correção dos algoritmos e funções
3.3.1 Os algoritmos e funções de medição do instrumento devem ser apropriados e funcionalmente corretos para a aplicação e tipo de instrumento.
3.3.2 Deve ser possível examinar os algoritmos e funções de medição através de ensaios metrológicos ou ensaios e exames de *software*, conforme norma NIT-Dinst-026.
3.4 Proteção de *software* e *hardware*
3.4.1 O *software* e o *hardware* do instrumento devem ser projetados e construídos de forma a impedir seu uso impróprio ou fraudulento, quer seja intencional, não intencional ou acidental.
3.4.2 As proteções do *software* compreendem métodos de selagem que utilizem meios mecânicos, eletrônicos e/ou criptográficos e devem garantir que intervenções ou alterações não autorizadas no *software* e/ou no *hardware* do instrumento, caso aconteçam, possam ser evidenciadas.
3.4.3 O *software* e os parâmetros legalmente relevantes devem ser protegidos contra modificações acidentais ou não autorizadas.
3.4.4 Partes legalmente relevantes do instrumento não podem ser influenciadas por outras partes do sistema de medição.
3.4.5 O gabinete do instrumento deve ser seguro e possuir lacre ou selo com plano específico de selagem, de forma que sua violação seja impedida ou evidenciada.
3.4.6 O fabricante deve fornecer método de verificação de integridade do firmware legalmente relevante presente no instrumento em relação ao firmware legalmente relevante aprovado no processo de avaliação de modelo, alternativamente de acordo com a Norma NIT-Dinst-020.
3.4.7 O requisito do item 3.5.6 não se aplica a componentes ou instrumentos que satisfaçam os requisitos de imutabilidade do item 4.6.
3.5 Detecção de falhas
3.5.1 O instrumento deve possuir funções de detecção de falhas através de implementações de *software* e/ou *hardware*.
3.5.2 Em caso de falha de um elemento que faça parte da cadeia legalmente relevante, a função de detecção de falhas deve sinalizar a falha e impedir a medição.
3.6 Autenticidade e integridade dos dados de medição

3.6.1 O instrumento deve, após o processo de captura dos dados de medição, assegurar a autenticidade e integridade dos mesmos ao longo da cadeia legalmente relevante.
3.6.2 Se um computador universal for utilizado para processar parte ou totalidade dos dados de medição, estes devem ter sua autenticidade e integridade asseguradas antes de ser enviado ao computador universal.
3.6.3 Deve ser possível, verificando-se as premissas de autenticidade e integridade dos dados de medição, reconstituir o valor do resultado de medição.
3.6.4 O resultado de medição deve conter identificador unívoco do veículo medido.
3.6.5 No caso de uso de assinatura digital para garantia de autenticidade e integridade dos dados de medição, devem ser seguidos os requisitos do item 4.9.
3.7 Documentação requerida para os requisitos gerais
3.7.1 As partes ou componentes do sistema de medição que realizem funções legalmente relevantes devem ser claramente identificadas, definidas e documentadas.
3.7.2 O requerente do processo de avaliação de modelo deve fornecer a documentação relacionada a seguir:
3.7.2.1 Descrição funcional do instrumento.
3.7.2.2 Manual operacional do instrumento.
3.7.2.3 Especificação do *hardware* contendo:
a) descrição completa do *hardware* contemplando arquitetura em módulos;
b) diagramas de blocos funcionais de cada módulo;
c) diagrama esquemático das placas e componentes;
d) descrição das interfaces de comunicação e de usuário.
3.7.2.4 Especificação do *software* contendo sua arquitetura e conceitos de projeto, características de implementação e principais blocos do *software* legalmente relevante.
3.7.2.5 Descrição de como a versão de *software* é construída, como é estruturada, e como pode ser visualizada.
3.7.2.6 Descrição dos algoritmos de medição utilizados.
3.7.2.7 Descrição das medidas de proteção contra uso impróprio ou fraudulento do instrumento, incluindo planos de selagem e meios mecânicos, eletrônicos e/ou criptográficos.
3.7.2.8 Descrição das proteções contra mudanças acidentais ou não autorizadas do *software* e dos parâmetros legalmente relevantes.
3.7.2.9 Lista de falhas detectáveis, descrição dos algoritmos ou métodos de detecção, descrição das reações do instrumento à detecção de cada falha.
3.7.2.10 Plano de selagem do(s) gabinete(s) do instrumento.
3.7.2.11 Descrição da solução de garantia de autenticidade e integridade dos dados de medição.

4. REQUISITOS ESPECÍFICOS DE *SOFTWARE* E *HARDWARE*

4.1 O *software* e o *hardware* legalmente relevantes que empregarem as funcionalidades ou arquiteturas descritas a seguir devem satisfazer a totalidade dos seus respectivos requisitos específicos.
4.2 Indicações compartilhadas
4.2.1 A exibição dos valores de medição deve ser realizada de modo a não ser confundida com a de outros dados não legalmente relevantes.
4.2.2 Se um instrumento fizer uso de separação de *software* e seu dispositivo indicador utilizar interface de usuário de múltiplas janelas, aplicam-se os requisitos 4.2.3 e 4.2.4
4.2.3 O *software* que realiza a indicação dos valores medidos e outras informações legalmente relevantes pertence à parte legalmente relevante.
4.2.4 A janela que contém estes dados deve ter a prioridade mais alta, isto é, não deve ser excluída por outro *software*, não deve ser sobreposta por janelas geradas por outro *software* nem minimizada ou tornada invisível enquanto a medição estiver acontecendo e os valores apresentados forem necessários a um propósito legalmente relevante.
4.3 Transferência de dados

4.3.1 A transferência de dados a que se refere este item ocorre, dentro da cadeia legalmente relevante, numa das seguintes formas:
a) Transmissão de dados através de canal inseguro;
b) Armazenamento de dados em um dispositivo.
4.3.2 Os dados transferidos devem ter sua autenticidade, integridade e carimbo de tempo da medição garantidos.
4.3.3 Após recuperação dos dados transferidos, estes devem ter sua autenticidade e integridade verificados.
4.3.4 Em caso de ocorrência de falha em alguma das verificações referidas no item anterior, os dados devem ser descartados e não utilizados.
4.3.5 Componentes de *software* que preparam dados legalmente relevantes para armazenamento ou transmissão, ou que realizam a verificação dos dados após leitura ou recepção, pertencem ao *software* legalmente relevante.
4.3.6 O dispositivo de armazenamento deve ter durabilidade e estabilidade adequadas para assegurar que os dados não sejam corrompidos em condições normais de armazenamento.
4.3.7 A medição não deve ser influenciada por atrasos de transferência.
4.3.8 Se os sistemas de transferência se tornarem indisponíveis, nenhum dado de medição pode ser perdido;
4.3.8.1 No caso a que se refere o item 4.3.8, o processo de medição deve ser interrompido para impedir a perda de dados, caso não possam ser armazenados no instrumento.
4.3.9 Para o requisito do item 4.3.8, deve-se ativar sinalização indicando tal situação.
4.3.10 No restabelecimento da disponibilidade a que se refere o item 4.3.8, os dados armazenados devem ser transmitidos.
4.3.11 O carimbo de tempo deve ser obtido a partir do relógio do instrumento ou sistema.
4.4 Carga de *software* legalmente relevante
4.4.1 Somente pode ser carregado no instrumento *software* submetido pelo requerente ao processo de avaliação de modelo e nele aprovado pelo Inmetro.
4.4.2 A carga de *software* legalmente relevante deve ser automática: uma vez iniciada, independe da intervenção do operador.
4.4.3 O instrumento não pode realizar medições durante o processo de carga de *software* legalmente relevante.
4.4.4 Ao final do procedimento de carga e instalação de novo *software*, o ambiente de proteção deve retornar ao mesmo nível de segurança declarado no processo de avaliação de modelo.
4.4.5 É necessária a autenticação de usuário para realização da carga de *software* legalmente relevante.
4.4.6 A autenticação de usuário para carga de *software* deve garantir que a intrusão indevida em um instrumento não implique em sua propagação para os demais.
4.4.7 Devem ser empregados meios técnicos para garantir a autenticidade e integridade do *software* a ser carregado.
4.4.8 Se a autenticidade ou integridade do novo *software* não puderem ser verificadas, o instrumento deve descartá-lo e utilizar a versão anterior, ou tornar-se inoperante.
4.4.9 A carga de *software* deve ser evidenciada através da abertura de proteções físicas ou acesso autenticado a proteções lógicas e/ou criptográficas, bem como o registro desta ação em memória não volátil (registro de auditoria).
4.4.10 Devem ser armazenados no registro de auditoria a que se refere o item 4.4.9 a identificação do nível de acesso do responsável pela carga, data e hora da carga, sucesso ou insucesso da carga, e as versões anterior e posterior à carga.
4.4.11 Os registros de auditoria a que se refere o item 4.4.9 devem ser armazenados em memória não volátil com prazo mínimo do armazenamento de 5 (cinco) anos.
4.4.12 Os registros de auditoria a que se refere o item 4.4.9 devem ser disponibilizados para leitura através da interface de usuário, de comunicação ou de verificação metrológica.

4.5 Carga de *software* não legalmente relevante
4.5.1 A carga de *software* não legalmente relevante deve ser realizada sem necessidade de aprovação pelo Inmetro.
4.6 Arquiteturas com componentes eletrônicos imutáveis
4.6.1 Os componentes eletrônicos de processamento de dados reconhecidamente imutáveis, não programáveis e comercialmente disponíveis utilizados no instrumento de medição, que não permitirem alterações de seu firmware interno, devem ser documentados na máxima extensão de forma a evidenciar seu comportamento e assegurar sua imutabilidade.
4.6.2 Os componentes eletrônicos a que se refere o item 4.6.1 serão eximidos do fornecimento do código-fonte de seu firmware interno e da correspondente verificação de integridade.
4.7 Arquitetura com utilização de interfaces
4.7.1 Além da possibilidade de uso de selagem mecânica, outros meios técnicos devem ser utilizados para proteger partes do instrumento que possuam interfaces de comunicação ou de usuário.
4.7.2 Somente funções claramente documentadas podem ser ativadas pelas interfaces de comunicação ou de usuário.
4.7.3 As funções de interface devem ser concebidas de forma a não permitir o uso fraudulento do instrumento.
4.7.4 A alteração de parâmetros legalmente relevantes somente pode ser realizada, através de interfaces, mediante procedimento documentado que verifique a autorização do usuário ou operador.
4.7.5 A alteração dos parâmetros legalmente relevantes a que se refere o item 4.7.4 deve implicar na abertura de proteções físicas ou acesso autenticado a proteções lógicas e/ou criptográficas, bem como compulsoriamente no registro desta ação em memória não volátil (registro de auditoria).
4.7.6 Devem ser armazenados no registro de auditoria a que se refere o item 4.7.5 a identificação do nível de acesso do responsável pela alteração, data e hora da alteração, tipo do parâmetro alterado e os valores anterior e posterior à alteração.
4.7.7 Os registros de auditoria a que se refere o item 4.7.5 devem ser armazenados em memória não volátil com prazo mínimo de armazenamento de 5 (cinco) anos.
4.7.8 Os registros de auditoria a que se refere o item 4.7.5 devem ser disponibilizados para leitura através da interface do usuário, de comunicação ou de verificação metrológica.
4.7.9 Deve ser possível recuperar os valores atuais dos parâmetros que definem características legalmente relevantes do instrumento através das interfaces de usuário, de comunicação ou de verificação metrológica.
4.7.10 Deve-se garantir que os componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes sejam fisicamente invioláveis.
4.8 Arquiteturas com separação de *software* e/ou *hardware*
4.8.1 Se a separação de *software* e/ou *hardware* não for possível ou for desnecessária, o *software* e/ou *hardware* como um todo será considerado legalmente relevante.
4.8.2 Todos os módulos de *software* (programas, sub-rotinas, bibliotecas) e *hardware* (placas eletrônicas, componentes, transdutores) que realizem funções legalmente relevantes ou que contenham dados legalmente relevantes formam a parte legalmente relevante do instrumento de medição.
4.8.3 As partes ou componentes do sistema de medição que realizem funções legalmente relevantes devem ser claramente identificadas e documentadas.
4.8.4 Todas as comunicações entre as partes legalmente relevantes e não legalmente relevantes devem ser realizadas exclusivamente através de uma interface de separação de *software* e/ou *hardware*, pertencente à parte legalmente relevante, definida especificamente para este fim.
4.8.5 Deve haver uma correspondência unívoca e não ambígua entre cada comando emitido via interface de separação de *software* e/ou *hardware* e cada função iniciada ou alteração de dados realizada na parte legalmente relevante.
4.8.6 O requerente do processo de avaliação de modelo deve declarar a completude dos comandos a que se refere o item 4.8.5.

4.8.7 Partes legalmente relevantes do instrumento – quer sejam de *software* ou de *hardware* – não podem ser influenciadas por comandos não documentados recebidos através da interface de separação de *software* e/ou *hardware*.
4.8.8 A funcionalidade de medição (realizada pelo *software* e/ou *hardware* legalmente relevante) não deve ser comprometida por atrasos ou bloqueios ocorridos pela realização de outras tarefas.
4.9 Arquiteturas com assinatura digital
4.9.1 No caso de o instrumento utilizar assinatura digital para assegurar integridade, autenticidade e irrefutabilidade dos dados de medição e/ou dos valores medidos ao longo da cadeia legalmente relevante, o requerente do processo de avaliação de modelo deve fornecer ferramentas para:
a) publicação e conferência dos dados assinados;
b) reconstituição do valor final da medição a partir dos dados assinados.
4.9.2 Os dados ou valores assinados, juntamente com a correspondente assinatura digital, devem ser tratados como parâmetros legalmente relevantes e armazenados por, no mínimo, 60 dias.
4.9.3 Chaves criptográficas privadas devem ser mantidas secretas e seguras internamente ao instrumento.
4.9.4 Os componentes que processam dados, após a realização da assinatura digital, serão eximidos do fornecimento do código-fonte de seu firmware interno e da correspondente verificação de integridade.
4.10 Documentação requerida para os requisitos específicos
4.10.1 Documentação requerida para indicações compartilhadas
4.10.1.1 Relação de dados exibidos no dispositivo indicador.
4.10.1.2 Descrição das janelas e informações publicadas pela parte legalmente relevante.
4.10.2 Documentação requerida para transferência de dados
4.10.2.1 Descrição dos métodos que garantem autenticidade e integridade na transferência de dados.
4.10.2.2 Especificação dos algoritmos criptográficos utilizados se for o caso.
4.10.2.3 Descrição do meio e protocolo de transmissão e/ou armazenamento.
4.10.2.4 Código-fonte completo e comentado do *software* legalmente relevante.
4.10.2.5 Descrição das medidas que garantem a segurança das chaves criptográficas se for o caso.
4.10.2.6 Descrição das medidas que garantem durabilidade e estabilidade do armazenamento de dados.
4.10.2.7 Descrição das medidas que mitigam a influência de atrasos na transferência de dados.
4.10.2.8 Descrição dos meios de proteção do ajuste do relógio.
4.10.3 Documentação requerida para carga de *software* legalmente relevante
4.10.3.1 Descrição do procedimento de carga de *software* legalmente relevante.
4.10.3.2 Descrição das medidas de proteção contra carga e modificações não autorizadas do *software* legalmente relevante.
4.10.3.3 Descrição dos meios pelos quais se garante autenticidade e integridade do *software* a ser carregado.
4.10.3.4 Descrição dos meios pelos quais se garante que o *software* legalmente relevante foi previamente avaliado e aprovado pelo Inmetro.
4.10.3.5 Descrição do procedimento de registro das atualizações de *software* e formato dos dados armazenados.
4.10.3.6 Descrição do procedimento de disponibilização e publicação dos registros de atualização de *software* legalmente relevante.
4.10.3.7 Código-fonte completo e comentado do *software* legalmente relevante.
4.10.4 Documentação requerida para arquiteturas com componentes imutáveis
4.10.4.1 Especificação e documentação técnica dos componentes reconhecidamente imutáveis.
4.10.5 Documentação requerida para instrumento com interfaces
4.10.5.1 Descrição funcional das interfaces do instrumento, incluindo menus, diálogos, protocolos e funções existentes.
4.10.5.2 Lista de todas as funções e comandos que podem ser ativadas através das interfaces, com as correspondentes ações passíveis de serem desencadeadas no instrumento.
4.10.5.3 Declaração de completude dos comandos de interfaces.

4.10.5.4 Código-fonte completo e comentado do *software* legalmente relevante.
4.10.5.5 Descrição do procedimento de acesso, alteração e disponibilização dos valores atuais dos parâmetros que definem características legalmente relevantes do instrumento.
4.10.5.6 Descrição do procedimento de acesso e disponibilização do registro de alterações dos parâmetros que definem características legalmente relevantes do instrumento.
4.10.5.7 Descrição do procedimento de verificação de integridade, incluindo o protocolo utilizado.
4.10.5.8 Descrição dos algoritmos e mecanismos de verificação de integridade.
4.10.6 Documentação requerida para separação de *software* e/ou *hardware*
4.10.6.1 Projeto da separação de *software* e/ou *hardware*; descrição e identificação dos módulos de *software* (programas, sub-rotinas, bibliotecas) e *hardware* (placas eletrônicas, componentes, transdutores) que realizem funções legalmente relevantes ou que contenham dados legalmente relevantes.
4.10.6.2 Descrição da interface de *software* e/ou *hardware*, compreendendo funções, domínios de dados, protocolos de comunicação e barramento de dados.
4.10.6.3 Código-fonte completo e comentado do *software* legalmente relevante, incluindo a interface de *software*.
4.10.6.4 Relação completa, descrição e funcionalidades de comandos de interface de separação de *software* e/ou *hardware*.
4.10.6.5 Declaração de completude dos comandos de interface de separação de *software* e/ou *hardware*.
4.10.6.6 Descrição do meio pelo qual se assegura que a funcionalidade de medição não seja comprometida por atrasos ou bloqueios ocorridos pela realização de outras tarefas.
4.10.7 Documentação requerida para arquiteturas com assinatura digital
4.10.7.1 Descrição do *software* e *hardware* que realiza a assinatura digital.
4.10.7.2 Especificação do(s) algoritmo(s) de assinatura digital, contemplando sua especificação completa.
4.10.7.3 Descrição do processo de publicação e de verificação da assinatura digital.
4.10.7.4 Descrição do processo de reconstituição do valor final da medição a partir dos dados assinados.
4.10.7.5 Código-fonte completo e comentado do *software* legalmente relevante.
4.10.7.6 Descrição das medidas que garantem a segurança das chaves criptográficas utilizadas.

5. DISPOSIÇÕES GERAIS
5.1 Avaliação de modelo
5.1.1 Todas as versões do *software* legalmente relevante do instrumento devem ser previamente avaliadas e aprovadas pelo Inmetro.
5.1.2 O Inmetro se reserva o direito de definir quais componentes de *software* e *hardware* são legalmente relevantes para fins de avaliação de modelo.
5.2 Inspeções
5.2.1 Nas inspeções do instrumento o procedimento de verificação de integridade deverá ser executado.
5.2.1.1 Em caso de falha, o instrumento deverá ser interditado até seu reparo e ser realizada com sucesso nova verificação de integridade.
5.3 Segurança das chaves criptográficas
5.3.1 É responsabilidade do fabricante do instrumento assegurar ambiente seguro de gestão das chaves criptográficas dos instrumentos por ele produzidos.
5.4 Dispositivos acessórios
5.4.1 O requerente do processo de avaliação de modelo deve fornecer o *software* e *hardware* necessários para que os requisitos deste Anexo possam ser avaliados, incluindo: dispositivos acessórios do instrumento, cabos de conexão, dispositivos de interfaces e ferramentas de *software* e *hardware* para configuração, carga de *software* e verificação do instrumento.
5.5 Ensaios funcionais de requisitos de *software*
5.5.1 Os ensaios funcionais descritos na norma NIT-Dinst-026 podem ser realizados para evidenciar o cumprimento dos requisitos gerais e específicos de segurança de *software* e *hardware*.
5.6 Fornecimento do código-fonte

5.6.1 Será dispensado o fornecimento do código-fonte do *software* legalmente relevante do componente que atender ao requisito 4.6.1.
5.6.2 É obrigatório o fornecimento do código-fonte completo e comentado da parte legalmente relevante para os instrumentos que atenderem aos requisitos 4.3, 4.4, 4.7, 4.8 e/ou 4.9.