

EVALUACIÓN DE SOFTWARE EN EL CONTROL METROLÓGICO DEL ESTADO: EL DOCUMENTO OIML D 31 Y LA GUÍA WELMEC 7.2

V. Marcos Lucas⁽¹⁾ y S. Ruiz González⁽²⁾

^(1 y 2)Centro Español de metrología, Calle del Alfar 2, 28760, Tres Cantos (Madrid)

⁽¹⁾ Teléfono: 918074700. Correo electrónico: vmarcos@cem.es

RESUMEN:

El ya derogado Real Decreto 889/2006, de 21 de julio, por el que se regula el control metrológico del Estado sobre instrumentos de medida [1], indicaba algunos requisitos que debía cumplir el software de los instrumentos de medida. Con la entrada en vigor de la Ley 32/2014, de 22 de diciembre, de Metrología [2] se introdujo claramente en el alcance del control metrológico del Estado los programas informáticos que sirven para medir o contar. Los requisitos que deben satisfacer dichos programas se encuentran recogidos en el Real Decreto 244/2016, de 3 de junio, por el que se desarrolla la Ley 32/2014, de 22 de diciembre, de Metrología [3], ampliando así, los requisitos que estableció el RD 889/2006.

Esta ponencia pretende por un lado, presentar la implantación de la evaluación de software de instrumentos de medida según el RD 244/ 2016 y la problemática en su aplicación, y por otro lado, comparar dos documentos recomendados por dicho Real Decreto para realizar esta evaluación.

1. INTRODUCCIÓN

La Ley 32/2014, de 22 de diciembre, de Metrología, define en su artículo 7, el control metrológico del Estado, indicando su alcance. Entre los elementos de dicho alcance se encuentran los programas informáticos que sirven para medir o contar.

Posteriormente, entró en vigor el Real Decreto 244/2016 de 3 de junio por el que se desarrolla la Ley 32/2014 de 22 de diciembre, de Metrología, el que se definen los requisitos que debe cumplir el software legalmente relevante. En concreto, en su anexo IV, se regulan los requisitos del software legalmente relevante de los instrumentos de medida que se deben analizar durante la evaluación de la conformidad, como son la identificación del software, su protección, almacenamiento de datos a largo plazo, actualización, separación de software, descarga externa y el registro de suceso y de errores, entre otros.

Para analizar estos requisitos, el Real Decreto 244/2016 da la posibilidad de utilizar normas armonizadas, Recomendaciones internacionales OIML u otros documentos aprobados por organismos nacionales e internacionales como UNE-EN/ISO, OIML o WELMEC.

Con este propósito, la OIML (Organización Internacional de Metrología Legal) elabora el Documento Internacional OIML D 31 [4] y WELMEC (Cooperación Europea en Metrología Legal), la guía WELMEC 7.2 [5].

El documento OIML D 31 está dirigido a proporcionar información técnica a los comités y subcomités técnicos de OIML para establecer los requisitos de software de instrumentos relacionados con las Recomendaciones OIML, así como orientar a los Estados miembros de OIML a implementar dichas Recomendaciones OIML en su legislación nacional, mientras que la guía WELMEC 7.2 está especialmente pensada para instrumentos incluidos en la Directiva de Instrumentos de Medida, aunque también da la posibilidad de ser utilizada en la evaluación de otros instrumentos e incluso en evaluaciones en otros ámbitos.

Durante el tiempo que ha transcurrido desde la entrada en vigor del RD 244/2016, se han encontrado una serie de problemas en su implantación que se pretenden exponer en este artículo.

2. DESARROLLO/DESCRIPCIÓN

2.1. Requisitos de software recogidos en el RD 244/2016

El anexo IV: Software legalmente relevante vinculado a la medición en los instrumentos de medida sometidos a control metrológico del Estado, regula el software legalmente relevante indicando los requisitos que deben cumplir los instrumentos de medida en la evaluación de conformidad para garantizar que cumplen los requisitos esenciales comunes y específicos del instrumento. Está compuesto por seis artículos:

- El artículo 1 define el objeto y ámbito de aplicación del anexo, que es la regulación del software legalmente relevante durante la evaluación de la conformidad para garantizar que cumple los requisitos esenciales comunes y específicos de los instrumentos de medida, para lo que habrá que analizar el software si disponen de él.
- El artículo 2 da una serie de definiciones relacionadas con el software.
- El artículo 3 indica algunas generalidades del software
 - Los resultados deben ser claros y tienen que ser generados por software sometido a control metrológico.
 - El software se debe poder evaluar fácilmente.
 - Se permite su modificación pero requiere la evaluación del organismo que lo evaluó previamente.
 - El fabricante define los requisitos y el organismo designado comprueba si son suficientes.
 - Indica una serie de procedimientos de ensayo que se pueden seguir para realizar la evaluación como son la utilización de normas armonizadas, Recomendaciones OIML, requisitos esenciales publicados por la Comisión Europea, u otros documentos como normas UNE-EN/ISO, OIML, WELMEC.
 - El software debe poder descargarse externamente.
 - La verificación e inspección deben poder realizarse de forma sencilla, sin medios adicionales o en caso contrario debe ser facilitados por el responsable de su comercialización y puesta en servicio.
 - El agente económico presentará una declaración en la que indique que no revelará el código fuente o datos para acceder a la modificación de parámetros legalmente relevantes.
 - El organismo que emite el certificado debe conservar la documentación utilizada para evaluar el software y una copia descargada.
 - Los resultados de actividades para evaluar el software deben recogerse en el correspondiente certificado.
- El artículo 4 trata sobre la modificación del software: Las modificaciones se deben comunicar al organismo que lo evaluó que deberá evaluar las modificaciones realizadas antes de poder aplicar dicha modificación, para ello le facilitará toda la documentación necesaria. La modificación no podrá eliminar ni alterar los registros.
- El artículo 5 recoge una serie de requisitos iniciales comunes:
 - El fabricante debe presentar la documentación técnica necesaria para evaluar la conformidad del software con los requisitos esenciales.

- El solicitante deberá presentar una declaración con una serie de compromisos relativos al software.
- Se deben facilitar instrucciones para leer el histórico de datos, errores del dispositivo y errores relativos a cambios accidentales o intencionados e inspección del registro de sucesos.
- No está permitido el borrado del registro de sucesos, ni de datos legalmente, salvo si se ha superado el periodo establecido en la regulación específica del instrumento.
- La actualización de la fecha y hora del instrumento no debe influir en la medición, en el registro de sucesos o en el histórico de datos almacenados, o en caso contrario estará sometido a control metrológico.
- El registro de sucesos debe incluir: la identificación del suceso, su valor, la fecha y hora del cambio y el agente que interviene. No se podrá eliminar o modificar y estará protegido contra cambios accidentales
- El registro de errores se utilizará si se pueden producir fallos de almacenamiento en dispositivos volátiles.
- El artículo 6 indica el contenido mínimo del certificado de conformidad

2.2. Comparación del documento OIML D 31 y la guía WELMEC 7.2

Como se ha indicado anteriormente éstos documentos se pueden utilizar para evaluar el software de los instrumentos de medida sometidos a control metrológico. En este apartado se pretende compararlos y para ello se tomará como referencia la guía WELMEC 7.2 para facilitar la comparación.

Ambos documentos comienzan dando una serie de definiciones utilizadas a lo largo de ellos e instrucciones para su uso.

La guía WELMEC define dos configuraciones básicas tipo P ó U en función de si el software está integrado en el instrumento creado para un propósito específico o si utiliza un ordenador universal, respectivamente También define cuatro configuraciones de tecnología de la información (TI): Extensión L (Almacenamiento a largo plazo), T (Transmisión de datos), S (Separación de software) y D (Actualización de software). Además se incluye las extensiones de la I1 a la I10, relativas a requisitos específicos de cada tipo de instrumento que se recogen en los anexos de esta guía. Cada una de estas configuraciones tiene una serie de bloques de requisitos que debe cumplir el instrumento, y para analizarlos será necesario seleccionar una de las dos configuraciones básicas y las configuraciones TI que se hayan aplicado, así como las específicas del instrumento.

A continuación se debe seleccionar la clase de riesgo. Los riesgos están causados por tres factores: protección inadecuada del software, examen inadecuado y no conformidad con el tipo. La clase de riesgo combina estos tres factores y se aplican una serie de contramedidas clasificadas en niveles bajo, medio y alto para cada uno de estos factores de riesgo. De esta forma se definen seis clases de riesgo: de la clase de riesgo A a la F (Tabla 1), de las que actualmente sólo se utilizan las clases de B, C, y D.

| Clase de riesgo | Protección del software | Examen del software | Grado de conformidad del software |
|-----------------|-------------------------|---------------------|-----------------------------------|
|-----------------|-------------------------|---------------------|-----------------------------------|

| | | | |
|---|-------|-------|-------|
| A | bajo | bajo | bajo |
| B | medio | medio | bajo |
| C | medio | medio | medio |
| D | alto | medio | medio |
| E | alto | alto | medio |
| F | alto | alto | alto |

Tabla 1. Clases de riesgo

Cada uno de los bloques de requisitos se estructura de la siguiente forma: título, una declaración sobre lo que se pretende con este requisito, notas específicas (alcance, explicaciones adicionales, casos excepcionales), la documentación que se debe facilitar en función del riesgo, guías de validación en función del riesgo y posibles ejemplos para cumplir con el requisito.

El Documento OIML D 31 por su parte, define los dispositivos construidos para un propósito y dispositivos universales, pero no especifica uno u otro a la hora de tratar los requisitos y define las configuraciones específicas donde incluye la separación de partes legalmente relevantes y especificaciones de las interfaces, almacenamiento de datos, transmisión de datos mediante líneas de comunicación, compatibilidad de los sistemas operativos y el hardware, conformidad de los dispositivos fabricados con el tipo certificado y mantenimiento y reconfiguración. Este último se refiere a la actualización de software

Este documento determina los niveles de riesgo con unos límites menos estrictos. Para seleccionar los niveles de riesgo se puede tener en cuenta el riesgo de fraude, la conformidad exigida, la confiabilidad requerida, la motivación del defraudador y la posibilidad de repetir una medición o interrumpirla.

De esta forma divide las clases de riesgo en básica (I) y elevada (II) y describe cinco métodos (Tabla 2) utilizados para la evaluación del software. Estos métodos se pueden combinar en función de la clase de riesgo, para los que el documento presenta una posible combinación de métodos.

| Abreviatura | Descripción | Aplicación | Condiciones previas, herramientas para la aplicación | Habilidades especiales para actuar. |
|-------------|--|---|--|-------------------------------------|
| AD | Análisis de la documentación y evaluación del diseño (7.3.2.1) | Siempre | Documentación | - |
| VFTM | Verificación por pruebas funcionales de funciones metrológicas (7.3.2.2) | Corrección de los algoritmos, incertidumbre, compensación y algoritmos de corrección, reglas para el cálculo de precios. | Documentación, muestra | |
| VFTSw | Verificación por pruebas funcionales de las funciones del software (0) | Correcto funcionamiento de la comunicación, indicación, evidencia de intervención, protección contra errores de operación, protección de parámetros, detección de defectos significativos | Documentación, muestra | |
| DFA | Análisis de flujo de | Separación de software, | Código fuente, | Conocimiento de |

| Abreviatura | Descripción | Aplicación | Condiciones previas, herramientas para la aplicación | Habilidades especiales para actuar. |
|-------------|---|---|---|---|
| | datos metrológicos (7.3.2.4) | evaluación del impacto de los comandos en las funciones del instrumento | herramientas para analizar código fuente | lenguajes de programación |
| CIWT | Inspección y recorrido del código (7.3.2.5) | Todos los propósitos | Código fuente, herramientas para analizar código fuente | Conocimiento de lenguajes de programación |
| SMT | Pruebas de módulos de software (7.3.2.6) | Todos los propósitos cuando la entrada y la salida se pueden definir claramente | Código fuente, entorno de prueba | Conocimiento de lenguajes de programación |

Tabla 2. Métodos de evaluación según el Documento OIML D 31

Este documento, a diferencia de la guía WELMEC se estructura de forma completamente distinta, de forma que en primer lugar explica todos los requisitos dando una serie de ejemplos para cada uno y posteriormente explica los métodos de evaluación y las posibles combinaciones de métodos.

En ambos documentos se indica la información que debería incluirse en el certificado, la documentación que se debe presentar para realizar la evaluación y una serie de listas de comprobación que facilitan la comprobación del cumplimiento de cada requisito. Además el Documento OIML D 31 incluye una serie de verificaciones que pueden realizarse en la fase de instrumentos en servicio.

La versión de 2022 de la guía WELMEC introduce una nueva extensión sobre los requisitos que debe cumplir el sistema operativo (extensión O), que es de aplicación únicamente a la extensión U. Con esta introducción se ha conseguido acercar aún más los requisitos establecidos en ambos documentos.

A continuación se van a indicar los bloques de requisitos que incluye la guía WELMEC 7.2, sin incluir la extensión I, y se indicarán, si existen, las diferencias encontradas con respecto al Documento OIML D 31.

2.2.1. Requisitos específicos para tipo P/U

- P1/U1: Documentación: indica el contenido que debe influir la documentación
- P2/U2: Identificación de software: El software legalmente relevante debe estar identificado claramente mediante un identificador que debe ser mostrado en el instrumento o mediante un comando. El Documento OIML D 31 incluye que si el instrumento no tiene pantalla, se podrá enviar mediante una interfaz de comunicación para que se muestre o imprima en otro componente.
- P3/U3: Influencia a través de interfaces de usuario: Los comando mediante interfaces de usuario no pueden influir en el software legalmente relevante, en los parámetros específicos del dispositivo o en los datos de medida.
- P4/U4: Influencia a través de interfaces de comunicación: Los comando mediante interfaces de comunicación no pueden influir en el software legalmente relevante, en los parámetros específicos del dispositivo o en los datos de medida.

- P5/U5: Protección contra cambios accidentales o involuntarios: Se debe proteger el software legalmente relevante y los parámetros específicos del dispositivo contra este tipo de cambios.
- P6/U6: Protección contra cambios intencionales inadmisibles: Se debe proteger el software legalmente relevante y los parámetros específicos del dispositivo contra este tipo de cambios.
- P7/U7: Protección de parámetros: Los parámetros específicos del dispositivo deben estar protegidos contra modificaciones inadmisibles, por ejemplo mediante precintado y los cambios se deben registrar en un registro de sucesos. En el Documento OIML D 31 se habla de registros de auditoría en lugar de registro de sucesos, además se habla de marcas de tiempo que indican el momento en que se toma una media u ocurre un evento; se leen en el reloj y deben estar protegidas.
- P8/U8: Autenticidad de datos de medida mostrados. Se debe garantizar la autenticidad de los datos de medida mostrados
- U9: Influencia de otro software: Este requisito está relacionado con la separación del software ya que el software legalmente no relevante no debe influir inadmisiblemente sobre el software legalmente relevante.

2.2.2. Extensión O

- O1: Hardware: La parte que ejecuta el sistema operativo legalmente relevante debe protegerse contra el acceso inadmisibles
- O2: Proceso de arranque: La configuración del arranque debe proporcionar el mismo entorno configurado para la ejecución del software legalmente relevante y debe estar protegido.
- O3: Recursos del sistema: Debe garantizarse que son suficientes para el funcionamiento de la aplicación legalmente relevante.
- O4: Protección durante el uso: El sistema operativo debe estar configurado de forma que no influya inadmisiblemente en el software legalmente relevante. Tampoco debe influir otro software.
- O5: Interfaces de protección: Las funciones del sistema operativo desde interfaces abiertas no deben influir inadmisiblemente en el software legalmente relevante
- O6: Identificación del sistema operativo y su configuración: La identificación se muestra mediante comando o durante la operación.
- O7: Protección del sistema operativo: protección que muestre evidencias de una posible intervención.

2.2.3. Extensión L

- L1: Integridad de los datos de medida almacenados: Todos los datos deben ser completos y poder rastrearse hasta la medición que los originó
- L2: Protección contra cambios accidentales o involuntarios: Debe existir un método para proteger los datos de medida almacenados contra este tipo de cambios.
- L3: Integridad de datos: Los datos de medida almacenados deben protegerse contra cambios intencionados
- L4: Trazabilidad de los datos de medida almacenados: Los datos de medida almacenados deben poder vincularse a la medición y al instrumento que los origina.

- L5: Confidencialidad de las claves: Las claves se deben mantener en secreto y protegerse
- L6: Recuperación, verificación e indicación de los datos de medida almacenados: Se debe poder indicar los datos de medida almacenados y deben indicar una posible violación de la trazabilidad e integridad
- L7: Almacenamiento automático: Los datos deben almacenarse automáticamente al finalizar la medición.
- L8: Capacidad de almacenamiento y continuidad: se debe prever una capacidad suficiente de almacenamiento, y se debe advertir una advertencia si el almacenamiento está lleno, o se retira y sólo se pueden sobrescribir datos obsoletos. El documento OIML D 31 adicionalmente permite eliminarlos si se liquida la transacción o los datos son impresos por un dispositivo sujeto a control legal.

2.2.4. Extensión T

- T1: Integridad de los datos transmitidos: Los datos transmitidos deben tener toda la información necesaria para presentar o procesar el resultado de medida.
- T2: Protección contra cambios accidentales o involuntarios: Los datos transmitidos se deben proteger contra este tipo de cambios. Se deben detectar errores de transmisión.
- T3: Integridad de los datos: Los datos de medida se deben proteger contra cambios intencionados que puedan producirse en redes abiertas
- T4: Trazabilidad de los datos transmitidos Los datos transmitidos mediante redes abiertas deben poder rastrearse hasta el instrumento de medida y a la medición que los originó.
- T5: Confidencialidad de las claves: Las claves se deben mantener en secreto y protegerse
- T6: Recepción, verificación y manejo de los datos de medida transmitidos: El software legalmente relevante debe recibir, verificar y manejar los datos transmitidos y deben indicar una posible violación de la trazabilidad e integridad:
- T7: Retraso de transmisión: La medición no debe estar influenciada inadmisiblemente por un retraso de transmisión
- T8: Disponibilidad de los servicios de transmisión: Si estos servicios no están disponibles deberá garantizarse que no se pierden datos. El documento OIML D 31 permite aceptar una pérdida de datos transmitidos si las medidas son repetibles fácilmente.

2.2.5. Extensión S

- S1: Realización de la separación de software: El software y parámetros legalmente relevantes estarán separados de otras partes del software.
- S2: Indicación mixta: La información generada por el software legalmente no relevante se mostrará de forma que no se confunda con la generada por el software legalmente relevante.
- S3: Interfaz de software de protección: el intercambio de datos entre el software legalmente relevante y legalmente no relevante se llevará a cabo a través de una interfaz de software de protección.

2.2.6. Extensión D

- D1: Mecanismo de descarga: La transmisión e instalación del software serán automáticas y no afectarán a la protección del software legalmente relevante
- D2: Autenticación del software transmitido: Se debe garantizar que el software transmitido sea auténtico
- D3: Integridad del software descargado: Se debe garantizar que el software no se haya cambiado durante la transmisión.
- D4: Trazabilidad de la descarga de software legalmente relevante: Las descargas de software se deben rastrear en el instrumento y para ello debería quedar constancia en el registro de sucesos o registros de auditoría, dependiendo del documento utilizado. Además el Documento OIML añade que en el certificado debe incluirse cómo ver los registros de auditoría y que el usuario debe dar su consentimiento para realizar la actualización.

2.3. Problemática en la implantación de la evaluación de software

Desde la implantación del RD 244/2016 se han encontrado una serie de problemas a la hora de evaluar el software.

Por un lado, los avances de la tecnología está llevando a que en algunos instrumentos el almacenamiento de los resultados de medida se realice en la nube, por lo que debería garantizarse que la comunicación para esta transmisión de datos esté protegida y en caso de producirse fallos en la comunicación se debe garantizar que no hay una pérdida o alteración de los datos, así como garantizarse que los datos almacenados en la nube no se pueden modificar y que son almacenados el tiempo establecido.

Por otro lado, hay instrumentos de medida muy sencillos que no permiten la descarga del software, lo cual supone un problema de cara a una posible inspección de los instrumentos en servicio.

El avance del estado del arte está generando instrumentos de medida que utilizan dispositivos de carácter universal como teléfonos móviles, tabletas (*tablets*), asistentes personales digitales (*pda*), cámaras. Esto hace que no se pueda determinar de forma estricta la arquitectura asociada al instrumento y por lo tanto al software.

3. CONCLUSIONES

En esta ponencia se ha tratado de exponer los requisitos de carácter obligatorios necesarios para evaluar el software de los instrumentos de medida que introdujo el RD 244/2016 con su entrada en vigor y las dificultades que se han encontrado en su aplicación.

Por otro lado, se ha demostrado que los documentos OIML D 31 y la guía WELMEC 7.2 nombrados en el RD 244/2016 como posibles soluciones para evaluar el software, son muy similares en cuanto a los requisitos que se deben aplicar para realizar dicha evaluación.

4. REFERENCIAS

[1] *Real Decreto 889/2006, de 21 de julio, por el que se regula el control metrológico del Estado sobre instrumentos de medida*, Boletín Oficial del Estado núm. 183, de 2 de agosto de 2006.

- [2] *Ley 32/2014, de 22 de diciembre, de Metrología*, Boletín Oficial del Estado núm. 309, de 23 de diciembre de 2014.
- [3] Real Decreto 244/2016, de 3 de junio, por el que se desarrolla la Ley 32/2014, de 22 de diciembre, de Metrología, Boletín Oficial del Estado núm. 137, de 7 de junio de 2016
- [4] *OIML D 31 General requirements for software controlled measuring instruments*, International Organization of Legal Metrology, 2019
- [5] *WELMEC 7.2 Software Guide (Measuring Instruments Directive 2014/32/EU)*, European cooperation in legal metrology, 2022.