



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE INDUSTRIA, COMERCIO  
Y TURISMO

# Evaluación de software en el control metrológico del Estado: el Documento OIML D 31 y la Guía WELMEC 7.2

Virginia Marcos  
Salustiano Ruiz

7º Congreso Español de Metrología  
28 de septiembre de 2022



# Introducción

## Alcance del control metrológico del Estado:

- Ley 32/2014, de 22 de diciembre, de Metrología:

Instrumentos, medios, materiales de referencia, sistemas de medida y programas informáticos que sirvan para medir o contar y que sean utilizados por razones de interés público, salud y seguridad pública, orden público, protección del medio ambiente, protección o información a los consumidores y usuarios, recaudación de tributos, cálculo de aranceles, cánones, sanciones administrativas, realización de peritajes judiciales, establecimiento de las garantías básicas para un comercio leal, y todas aquellas que se determinen con carácter reglamentario

Anexo IV del Real Decreto 244/2016 de 3 de junio por el que se desarrolla la Ley 32/2014 de 22 de diciembre, de Metrología

- Real Decreto 889/2006, de 21 de julio, por el que se regula el control metrológico del Estado sobre instrumentos de medida (Derogado):

Instrumentos, aparatos, medios y sistemas de medida que sirvan para pesar, medir o contar, utilizados en aplicaciones de medida por razones de interés público, salud y seguridad pública, orden público, protección del medio ambiente, protección de los consumidores y usuarios, recaudación de impuestos y tasas, cálculo de aranceles, cánones, sanciones administrativas, realización de peritajes judiciales, establecimiento de las garantías básicas para un comercio leal y todas aquellas que puedan determinarse con carácter reglamentario



# Requisitos de software: Anexo IV del Real Decreto 244/2016

- **Artículo 1. Objeto y ámbito de aplicación**

Regula el software legalmente relevante indicando los requisitos que deben cumplir los instrumentos de medida en la evaluación de conformidad para garantizar que cumplen:

- Requisitos esenciales comunes
- Requisitos específicos del instrumento

- **Artículo 2. Términos y definiciones**

Definiciones relacionadas con el software



# Requisitos de software: Anexo IV del Real Decreto 244/2016

## • Artículo 3. Generalidades

- Resultados claros y generados por software sometido a control metrológico.
- Fácil evaluación del software.
- Modificación del software previa evaluación del organismo que hizo la evaluación inicial.
- El fabricante define los requisitos y el organismo designado comprueba si son suficientes.
- Procedimientos de ensayo que se pueden seguir para realizar la evaluación:
  - Normas armonizadas
  - Recomendaciones OIML
  - Requisitos esenciales publicados por la Comisión Europea
  - Otros documentos como normas UNE-EN/ISO, OIML, WELMEC
- Descarga externa del software.
- Verificación e inspección sencillas
- El organismo que emite el certificado debe conservar la documentación utilizada para evaluar el software y una copia descargada.
- El certificado debe incluir los resultados de actividades realizadas para evaluar el software



Documento Internacional OIML D 31  
Guía WELMEC 7.2



# Requisitos de software: Anexo IV del Real Decreto 244/2016

- **Artículo 4. Modificación del software**
  - Evaluación del software modificado
  - No eliminará registros
  - Documentación para la evaluación
- **Artículo 5. Requisitos iniciales comunes**
  - Documentación técnica para evaluar el software.
  - Declaración del fabricante con compromisos relativos al software.
  - Fecha y hora
  - Registro de sucesos
  - Registro de errores
- **Artículo 6. Certificado de conformidad**



# La Guía WELMEC 7.2 y el Documento OIML D 31

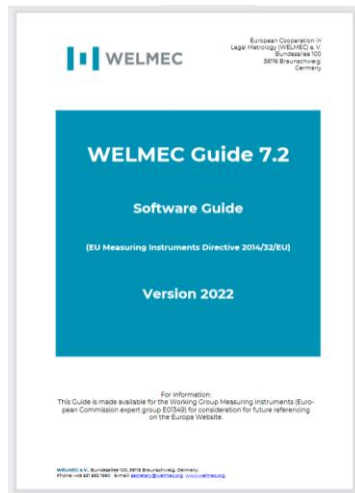
## Guía WELMEC 7.2

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.

## Documento Internacional OIML D 31

Proporciona información técnica a los comités y subcomités técnicos de OIML para establecer los requisitos de software de instrumentos relacionados con las Recomendaciones OIML.

Orientar a los Estados Miembros de OIML a implementar dichas Recomendaciones OIML en su legislación nacional.





# Guía WELMEC 7.2

## Configuraciones básicas:

- Tipo P: software está integrado en el instrumento creado para un propósito específico
- Tipo U: software en un ordenador universal (+ Extensión O: Sistema operativo)

+

## Configuraciones de tecnología de la información:

- Extensión L: Almacenamiento a largo plazo
- Extensión T: Transmisión de datos
- Extensión S: Separación de software
- Extensión D: Actualización de software

+

## Requisitos de software específicos del instrumento (I<sub>xx</sub>)

Seleccionar la clase de riesgo (A a F):

-Factores de riesgo:

- Protección inadecuada del software
- Examen inadecuado
- No conformidad con el tipo

-Niveles de contramedidas:

- Bajo
- Medio
- Alto

| 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                              |

| Risk Class B  | Risk Class C | Risk Class D |
|---|--------------|--------------|
| <p><b>P3: Influence via user interfaces</b><br/> <i>Commands entered via the user interfaces shall not inadmissibly influence the legally relevant software, device-specific parameters and measurement data.</i></p> <p><b>Specifying Notes:</b></p> <ol style="list-style-type: none"> <li>1. There shall be an unambiguous assignment of each command to an initiated function or data change.</li> <li>2. Commands that are not documented shall have no effect on legally relevant functions, device-specific parameters and measurement data.</li> <li>3. The respective parts of the software that interpret commands are considered to be legally relevant software.</li> </ol> |              |              |
| <p><b>Required Documentation:</b><br/>           If the instrument has the ability to receive commands, the documentation shall include:</p> <ul style="list-style-type: none"> <li>• Description of commands and their effect on legally relevant software, device-specific parameters and measurement data.</li> <li>• Description of how the legally relevant software, device-specific parameters and measurement data are protected from being influenced by other inputs.</li> </ul>  |              |              |
| <p><b>Validation Guidance:</b><br/> <i>Checks based on documentation:</i></p> <ul style="list-style-type: none"> <li>• Check that documented commands are admissible, i.e., that they have an allowed influence on the legally relevant software, device-specific parameters and measurement data).</li> <li>• Check the protection measures against influences from other inputs.</li> </ul> <p><i>Functional Checks:</i></p> <ul style="list-style-type: none"> <li>• Carry out practical tests (spot checks) with documented commands.</li> <li>• Check whether there are undocumented commands.</li> </ul>  |              |              |
| <p><b>Example of an Acceptable Solution:</b><br/>           There is a software module that receives and interprets commands from the user interface. This module belongs to the legally relevant software. It forwards only allowed commands to the other legally relevant software modules. All unknown or not allowed sequences of switch or key actuations are rejected and have no impact on the legally relevant software, device-specific parameters and measurement data.</p>   |              |              |

| Additions for Risk Class E  |
|---|
| <p><b>Required Documentation</b> (in addition to the documentation required for risk classes B to D):<br/>           Source code of the legally relevant software.</p>  |
| <p><b>Validation Guidance</b> (in addition to the guidance for risk classes B to D):<br/> <i>Checks based on the source code:</i></p> <ul style="list-style-type: none"> <li>• Check the software design whether data flow concerning commands is unambiguously defined and realised only in the legally relevant software.</li> <li>• Search inadmissible data flow from the user interface to domains to be protected.</li> <li>• Check with tools or manually that commands are decoded correctly.</li> <li>• Check the code for undocumented commands.</li> </ul> |



# Documento OIML D 31

### Dispositivos:

- Construidos para un propósito
- Universales

+

### Requisitos específicos para configuraciones:

- Separación de partes 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
- Mantenimiento y reconfiguración (Actualización de software)

### Seleccionar el nivel de riesgo:

#### -Factores de riesgo:

- riesgo de fraude
- conformidad exigida
- confiabilidad requerida
- motivación del defraudador
- posibilidad de repetir una medición o interrumpirla

#### -Clases de riesgo:

- Básica
- Elevada

| Método  | Aplicación  | Condiciones previas, herramientas                       | Habilidades para actuar                   |
|---|---|---|---|
| AD: Análisis de la documentación y evaluación del diseño                  | Siempre   | Documentación   |   |
| VFTM: Verificación por pruebas funcionales de funciones metrológicas      | Corrección de los algoritmos, incertidumbre, compensación y corrección de algoritmos, reglas para el cálculo de precios.  | Documentación, muestra                                  |   |
| VFTSw: Verificación por pruebas funcionales de las funciones del software | 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 datos metrológicos                              | Separación de software, evaluación del impacto de los comandos en las funciones del instrumento   | Código fuente, herramientas para analizar código fuente | Conocimiento de lenguajes de programación |
| CIWT: Inspección y recorrido del código                                   | Todos los propósitos  | Código fuente, herramientas para analizar código fuente | Conocimiento de lenguajes de programación |
| SMT: Pruebas de módulos de software                                       | Todos los propósitos cuando la entrada y la salida se pueden definir claramente   | Código fuente, entorno de prueba                        | Conocimiento de lenguajes de programación |



# El documento OIML D 31 y la guía WELMEC 7.2

## Guía WELMEC 7.2

### Requisitos

- P1/U1: Documentación
- P2/U2: Identificación de software
  - Mostrado por el instrumento permanentemente, por comando o durante la operación
- P3/U3: Influencia a través de interfaces de usuario
- P4/U4: Influencia a través de interfaces de comunicación
- P5/U5: Protección contra cambios accidentales o involuntarios
- P6/U6: Protección contra cambios intencionales inadmisibles.
- P7/U7: Protección de parámetros
  - Registro de sucesos
- P8/U8: Autenticidad de datos de medida mostrados.
- U9: Influencia de otro software

## Documento OIML D 31

### Requisitos

#### Identificación de software:

- si el instrumento no tiene pantalla, se podrá enviar mediante una interfaz de comunicación para que se muestre o imprima en otro componente.

#### Protección de parámetros:

- registros de auditoría
- marcas de tiempo: se leen en el reloj y deben estar protegidas.



# El documento OIML D 31 y la guía WELMEC 7.2

## Guía WELMEC 7.2 y Documento OIML D 31

### Requisitos del sistema operativo

- O1: Hardware
- O2: Proceso de arranque
- O3: Recursos del sistema
- O4: Protección durante el uso
- O5: Interfaces de protección
- O6: Identificación del sistema operativo y su configuración
- O7: Protección del sistema operativo



# El documento OIML D 31 y la guía WELMEC 7.2

## Guía WELMEC 7.2

### Almacenamiento de datos a largo plazo

- L1: Integridad de los datos de medida almacenados:
- L2: Protección contra cambios accidentales o involuntarios
- L3: Protección contra cambios intencionados no admisibles
- L4: Trazabilidad de los datos de medida almacenados
- L5: Confidencialidad de las claves
- L6: Recuperación, verificación e indicación de los datos de medida almacenados
- L7: Almacenamiento automático
- L8: Capacidad de almacenamiento y continuidad
  - sólo se pueden sobrescribir datos obsoletos.

## Documento OIML D 31

### Almacenamiento de datos a largo plazo

#### Almacenamiento

- Se permite eliminar registros si se liquida la transacción o los datos son impresos por un dispositivo sujeto a control legal.



# El documento OIML D 31 y la guía WELMEC 7.2

## Guía WELMEC 7.2

### Transmisión de datos

- T1: Integridad de los datos transmitidos
- T2: Protección contra cambios accidentales o involuntarios
- T3: Protección frente a cambios intencionados no admisibles
- T4: Trazabilidad de los datos transmitidos
- T5: Confidencialidad de las claves:
- T6: Recepción, verificación y manejo de los datos de medida transmitidos:
- T7: Retraso de transmisión
- T8: Disponibilidad de los servicios de transmisión
  - Si estos servicios no están disponibles deberá garantizarse que no se pierden datos.

## Documento OIML D 31

### Transmisión de datos

- Disponibilidad de los servicios de transmisión

- Se permite eliminar una pérdida de datos transmitidos si las medidas son repetibles fácilmente



# El documento OIML D 31 y la guía WELMEC 7.2

## Guía WELMEC 7.2

### Separación de software

- S1: Realización de la separación de software
- S2: Indicación mixta
- S3: Interfaz de software de protección

### Actualización de software

- D1: Mecanismo de descarga
- D2: Autenticación del software transmitido
- D3: Integridad del software descargado
- D4: Trazabilidad de la descarga de software legalmente relevante:
  - Registro de sucesos.

## Documento OIML D 31

### Separación de software

### Actualización de software

#### Trazabilidad de la descarga

- Registro de auditoría
- Incluir en el certificado cómo ver los registros de auditoría
- El usuario debe dar su consentimiento para realizar la actualización



# Problemática en la implantación de la evaluación de software

- Almacenamiento de resultados de medida en la nube
- Descarga de software no permitida
- Dispositivos de carácter universal: teléfonos móviles, tabletas, asistentes personales digitales y cámaras





GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE INDUSTRIA, COMERCIO  
Y TURISMO

# Gracias por su atención