REQUISITOS PARA LA EVALUACIÓN DE LA CONFORMIDAD DE SOFTWARE DE INSTRUMENTOS O SISTEMAS DE MEDICIÓN

Requisitos para el Análisis de la documentación y validación del diseño (AD)

La evaluación de la conformidad del software se realizará en una muestra del modelo base y en una muestra adicional por cada variante del modelo, a fin de determinar sus características específicas y verificar su conformidad con los requisitos establecidos en la presente norma. Si durante o después de los ensayos del modelo se introducen modificaciones que afecten únicamente a ciertas partes del medidor, se realizará una evaluación para definir si es suficiente llevar a cabo pruebas específicas en aquellas características potencialmente impactadas por dichas modificaciones.

Requisitos Generales

La documentación requerida debe ser entregada completa y en formato digital, en idioma español, salvo información técnica específica como códigos fuente, manuales técnicos de componentes o sistemas (datasheets, bibliotecas, etc.). Se deberá adjuntar una suma de comprobación (checksum) para cada documento, garantizando así la autenticidad e integridad de la información entregada. La lista de documentos con sus sumas de comprobación debe consolidarse en un documento maestro.

Para consultas o entrega online, comunicarse al correo: metrologia@inacal.gob.pe.

1. Requisitos generales previos

1.1. Datos de la empresa solicitante
- 1.1.1. Nombre completo de la empresa solicitante del servicio.
- 1.1.2. Domicilio completo de la empresa.

1.2. Datos del fabricante
- 1.2.1. Nombre del fabricante.
- 1.2.2. Domicilio del fabricante.
- 1.2.3. Marca del medidor.
- 1.2.4. Designación del modelo.

1.3. Datos generales del software
- 1.3.1. Nombre comercial del software.
- 1.3.2. Identificación y/o número de versión(es) del software.
- 1.3.3. Marca, familia y modelo(s) del medidor de energía eléctrica en los que opera el software/firmware.
- 1.3.4. Sumas de comprobación binaria de cada uno de los módulos de software legalmente relevantes del medidor de energía eléctrica.

1.4. Datos generales del hardware
- 1.4.1. Nombre comercial del hardware.
- 1.4.2. Identificación y/o número de versión(es) del hardware.

1.5. Características metrológicas del medidor
- 1.5.1. Descripción de los principios de medición.
- 1.5.2. Especificaciones metrológicas, como la clase de exactitud y las condiciones de funcionamiento nominales.
- 1.5.3. Cualquier acción que deba realizarse antes de ensayar el medidor.

1.6. Datos específicos del Software
- 1.6.1. Sistema operativo en los que el Software opera (en caso aplique).
- 1.6.2. Hardware requerido para que el Software opere correctamente.
- 1.6.3. Dibujos, diagramas e información general del software, explicando la construcción y el funcionamiento.

1.7. Datos específicos del Hardware
- 1.7.1. Dibujo de la placa de características en escala 1:1.
- 1.7.2. Descripción general del hardware del sistema (por ejemplo, interfaces de comunicación, memorias, controladores, procesamiento de señales, etc)
- 1.7.3. Diagrama de bloques con una descripción funcional de los componentes dispositivos.

1.8. Datos relacionados a las interfaces de comunicación del software
- 1.8.1. Descripción de las interfaces de comunicación, tanto interiores como exteriores. Se considera como interfaz de comunicación interior a aquella cuyo acceso se encuentra protegido por el gabinete del dispositivo, mientras que una interfaz de comunicación exterior es aquella que se accede desde el exterior.

1.8.2. Protocolo de comunicación de las interfaces de comunicación del software
1.9. Manual de usuario / instrucciones
1.10. Manual de instalación
1.11. Manual de software externo en caso sea necesario para la realización de las pruebas funcionales.

2. Requisitos para ensayo documentario y validación de diseño

2.1. Identificación del software
2.1.1. Identificación del software y la descripción de cómo se genera dicha indicación.
2.1.2. La descripción de cómo está unívocamente ligada al software cargado.
2.1.3. La descripción de cómo se visualiza y cómo se estructura para diferenciar entre cambios de versión que necesiten o no certificación.
2.1.4. Las medidas implementadas para proteger la identificación del software frente a la falsificación y la descripción de dichas medidas.
2.2. Idoneidad de algoritmos y funciones legalmente relevantes
2.2.1. Descripción de la exactitud de los algoritmos de medición, por ejemplo, algoritmo de redondeo, filtrado de resultados de la conversión analógica a digital, generación del valor de medición final en base a ingreso de parámetros, etc. Mostrar de forma clara los parámetros que intervienen en estos cálculos.
2.3. Protección del Software
2.3.1. La descripción de las medidas implementadas para proteger el software y los datos frente a modificaciones no intencionadas (por ejemplo, deterioro de la memoria de almacenamiento, etc.)
2.3.2. La descripción de las medidas implementadas para comprobar la efectividad de la protección.
2.3.3. La descripción de las medidas implementadas para garantizar que el software legalmente relevante y los datos de medición no pueden ser modificados ilícitamente.
2.3.4. La lista de todos los comandos que pueden introducirse a través de la interfaz de usuario.
2.3.5. La descripción del significado de los comandos que se ingresan a través de la interfaz de usuario y su efecto en las funciones y datos del instrumento o sistema para medición.
2.3.6. El procedimiento para comprobar la influencia sobre el software a través de la interfaz de usuario de todos los comandos.
2.3.7. La lista completa de todos los comandos introducidos a través de las interfaces de comunicación.
2.3.8. La descripción del significado de cada comando introducido a través de las interfaces de comunicación y su efecto en las funciones y datos del instrumento de medición.
2.3.9. El procedimiento para comprobar la influencia sobre el software a través de la interfaz de comunicación de todos los comandos.
2.3.10. En caso existan comandos de otras interfaces de hardware incluirlas. Las listas de comandos solicitadas deben incluir una declaración de integridad.
2.3.11. Indicar el comportamiento del software frente a comandos no válidos en cada una de sus interfaces.
2.3.12. Descripción de los precintos u otros medios de protección.
2.3.13. Descripción del procedimiento de borrado o modificación del registro que almacena la energía total.
2.4. Soporte de las características de Hardware
2.4.1. La lista de las fallas detectables mediante el software y la descripción de estas.
2.4.2. La respuesta esperada ante las fallas detectables.
2.4.3. Descripción del algoritmo que detecta las fallas.
2.4.4. Descripción del procedimiento que realiza para la protección de durabilidad.
2.4.5. Lista de errores de durabilidad que detecta el software y, si es necesario para su comprensión, una descripción de los algoritmos de detección.
2.4.6. Procedimiento implementado para recuperarse ante fallos en el flujo correcto del software (por ejemplo, mecanismos de watchdog, etc.)
2.5. Separación de partes legalmente relevantes
2.5.1. La lista de todos los parámetros legalmente relevantes, sus valores nominales e intervalos.
2.5.2. La descripción funcional de todos los parámetros legalmente relevantes, la ubicación donde se almacenan, forma de visualizarse, en que condiciones, o por medio de que comandos se modifican.
2.5.3. Descripción de la protección de los parámetros legalmente relevantes ante intentos de modificación no autorizada y/o accidental.
2.5.4. La descripción de las medidas implementadas para verificar la integridad de los parámetros legalmente relevantes (por ejemplo, suma de comprobación, copias de respaldo, etc). Indicar con que periodicidad se realiza la verificación.
2.5.5. Cómo indica el medidor la detección de una inconsistencia en los parámetros y en qué estado queda el mismo.

2.5.6. Descripción de los programas informáticos/bibliotecas/módulos, etc que constituyen el software legalmente relevante y de cada una de sus funciones. Deberá incluir una declaración que todas las funciones legalmente relevantes están incluidas en la descripción presentada.
2.5.7. Descripción del software legalmente no relevante y de cada una de sus funciones.
2.5.8. Descripción de la implementación de la separación de software.
2.5.9. Descripción de las interfaces de software que comunica el software legalmente relevante con otras partes de software y de los comandos y flujos de datos a través de esta(s) interfaz(ces), incluida una declaración de integridad.
2.5.10. Descripción de todas las interfaces, funciones y los dominios del software legalmente relevante que evidencie la separación de software.
2.5.11. Descripción de medidas de seguridad implementadas para impedir la programación de comandos que eludan la interfaz del software legalmente relevante.
2.5.12. Descripción de medidas de seguridad implementadas para impedir que las funciones de medición del software legalmente relevante sean retrasadas, bloqueadas o ambas, por otros procesos.
2.5.13. Descripción de las medidas de seguridad implementadas para evitar que un programa legalmente no relevante altere las funciones legalmente relevantes.
2.5.14. Listado y descripción de los componentes de hardware considerados legalmente relevantes.

2.6. Integridad del software y presentación de resultados
2.6.1. Procedimiento implementado para verificar la integridad del software cargado en el equipo (por ejemplo, autodiagnóstico, suma de comprobación, etc.)
2.6.2. El resultado de la suma de comprobación binaria del software legalmente relevante.
2.6.3. Descripción de la periodicidad en la realización de la verificación de integridad.
2.6.4. La descripción de las medidas de protección implementadas contra el uso indebido, incluyendo la simulación ilícita del software legalmente relevante.
2.6.5. Descripción de cómo indica el medidor la detección de una inconsistencia y el estado en el que queda.
2.6.6. En los casos en los que se habilite el acceso para realizar modificaciones de cualquier tipo utilizando claves de acceso, detallar como se establecen y modifican dichas claves.

2.7. Si el dispositivo permite modificaciones en forma remota, detallar:
2.7.1. El procedimiento a utilizar para llevar a cabo cada modificación.
2.7.2. El protocolo de comunicación utilizado.
2.7.3. El detalle de cada uno de los comandos que se pueden utilizar en forma remota.
2.7.4. Los mecanismos de seguridad implementados para evitar manipulaciones fraudulentas.
2.7.5. El mecanismo de registro de las modificaciones realizadas.

2.8. Almacenamiento de datos
2.8.1. Características generales y específicas del medio de almacenamiento utilizado.
2.8.2. La descripción de las medidas implementadas para garantizar la integridad y protección de los datos almacenados.
2.8.3. Diagrama de bloques donde se especifica el algoritmo de almacenamiento, detección de fallas, eliminación de datos almacenados, límite de la capacidad de datos almacenados, etc.

2.9. Transmisión de datos
2.9.1. Características generales y específicas del(os) medio(s) de transmisión utilizado(s).
2.9.2. La descripción de las medidas implementadas para garantizar la integridad y protección de los datos transmitidos.
2.9.3. Diagrama de bloques donde se especifica el algoritmo de transmisión de datos, detección de fallas, etc.

2.10. Marca de tiempo
2.10.1. Descripción completa del registro de marca de tiempo, como se genera, formato de visualización, almacenamiento, transferencia.
2.10.2. Descripción del reloj en tiempo real utilizado.
2.10.3. El procedimiento para programar el reloj en tiempo real.
2.10.4. Descripción de las medidas de protección para la configuración del reloj.

2.11. Mantenimiento y reconfiguración
2.11.1. Descripción del procedimiento de carga de software. Describir el tipo de memoria en que se almacena.
2.11.2. Descripción del procedimiento mediante el cual se comprueba la carga realizada.
2.11.3. Descripción del procedimiento mediante el cual se garantiza el nivel de protección al finalizar el proceso de carga.
2.11.4. Descripción de la respuesta del instrumento o sistema de medición cuando se produce una falla en la carga.

2.11.5. Descripción de las medidas implementadas para impedir la modificación de la parte fija del software legalmente relevante.

2.12. Registro de eventos – Bitácora de auditoría
- 2.12.1. Lista de eventos que se registran
- 2.12.2. Descripción de la estructura, campos, formatos numéricos, etc.
- 2.12.3. Descripción de la forma de acceso.
- 2.12.4. El tipo de memoria en el cual se almacena.
- 2.12.5. Descripción de las operaciones permitidas sobre el mismo (borrado, modificación, etc)
- 2.12.6. Descripción de los mecanismos implementados para evitar borrados o modificaciones no autorizadas.

Se recomienda presentar la documentación del software utilizando diagramas de bloques, flujogramas, diagramas de uso, diagramas temporales, máquinas de estado, etc. que faciliten la comprensión y evaluación del software.
Asimismo, es recomendable presentar el plan de desarrollo de software y ciclo de vida.
Se debe presentar la documentación en idioma español.

NOTA: La documentación entregada tiene carácter de declaración jurada del fabricante, quien, a su vez, expresa haber declarado todos los comandos que reconoce el equipo y todas sus características funcionales.

Requisitos para la Evaluación mediante Ensayo Funcional de las Funciones del Software (VFTSw)

La evaluación de la conformidad del software mediante ensayo funcional se llevará a cabo en una muestra del modelo base y en una muestra adicional por cada variante del modelo, con el objetivo de verificar exhaustivamente el cumplimiento de todas las funcionalidades y especificaciones técnicas descritas en la respectiva Norma Metrológica Peruana (NMP).

En casos específicos en los que se realicen modificaciones al medidor, ya sea durante o posterior al ensayo documental, y que afecten únicamente a ciertos aspectos específicos del instrumento, se efectuará una evaluación adicional para definir si es suficiente realizar pruebas limitadas dirigidas exclusivamente a las características afectadas por dichas modificaciones.

Responsabilidades del Solicitante

El solicitante es responsable de proporcionar a la Dirección de Metrología del INACAL todos los elementos necesarios para la correcta ejecución del ensayo funcional, incluyendo, pero no limitándose a:

- Modelo o prototipo completo del instrumento de medición.
- Componentes adicionales necesarios para su plena operatividad.
- Interfaces de comunicación específicas, cables adecuados y compatibles con los equipos proporcionados.
- Software externo indispensable para la comunicación, configuración, monitoreo y otras operaciones asociadas al medidor.
- Licencias necesarias del software utilizado durante los ensayos.
- Manuales de usuario, manuales técnicos y cualquier documentación necesaria para el correcto manejo de los sistemas proporcionados.

Todos los elementos suministrados serán devueltos al solicitante al concluir satisfactoriamente los ensayos funcionales.

Documentación Técnica Requerida

La documentación asociada al software y hardware debe entregarse de manera completa y en formato digital, preferentemente en idioma español. Se permite la entrega en otro idioma únicamente para documentación técnica específica como códigos fuente, hojas técnicas de componentes (datasheets), documentación técnica de bibliotecas, entre otros.

Cada documento entregado deberá ir acompañado obligatoriamente de una suma de comprobación (checksum) que permita verificar su autenticidad e integridad. Además, todos estos documentos deberán estar listados claramente en un documento maestro que incluya las respectivas sumas de comprobación.

En el caso de emplear sistemas informáticos adicionales (software externo) para configurar, monitorear o interactuar con el medidor, se requiere documentación detallada incluyendo nombre del software, número de versión y sumas de comprobación específicas.

Aspectos Específicos del Ensayo Funcional

1. Información General

- Nombre comercial, modelo y versión exacta del medidor.
- Especificaciones técnicas completas necesarias para el correcto funcionamiento durante las pruebas.

2. Información del Software

- Identificación precisa del software instalado y sus versiones.
- Procedimiento detallado para la instalación, carga, configuración y validación del software.

3. Información del Hardware

- Descripción técnica completa del hardware (interfaces, memorias, controladores).
- Diagrama funcional claro del hardware involucrado.

4. Interfaces de Comunicación

- Descripción técnica completa de las interfaces internas y externas.

- Protocolos específicos y documentación relacionada con cada interfaz.
- Medios físicos como cables y conectores necesarios.

5. Verificación de Funciones del Software

- Procedimientos específicos para verificar:
  - Identificación correcta y autenticidad del software.
  - Correcta implementación de algoritmos metrológicos y funciones relevantes.
  - Protección contra modificaciones no autorizadas del software y datos.
  - Comportamiento ante comandos válidos e inválidos.
  - Funcionalidades de protección en modificaciones remotas (cuando aplique).
  - Integridad del software, parámetros y datos críticos.

6. Almacenamiento y Transmisión de Datos

- Procedimientos prácticos para verificar la integridad, protección y precisión en almacenamiento y transmisión de datos.

7. Marca de Tiempo

- Procedimientos específicos para validar la exactitud y seguridad del reloj interno y generación de registros de tiempo.

8. Mantenimiento y Recuperación del Software

- Procedimientos prácticos para evaluar la carga, actualización y recuperación del software ante fallos.

9. Registro de Eventos (Bitácora de Auditoría)

- Procedimientos para verificar la correcta creación y protección contra modificaciones no autorizadas en los registros de auditoría.

Notas Importantes

- La documentación técnica entregada deberá ser clara, detallada y apoyarse en recursos gráficos (diagramas técnicos, diagramas de bloques, flujogramas) que faciliten la ejecución precisa y completa de los ensayos funcionales.
- Toda la documentación y elementos entregados son considerados declaración jurada por parte del fabricante, quien garantiza la integridad, exactitud y exhaustividad de dicha información.
- La ejecución de los ensayos funcionales está condicionada a la aprobación previa de la etapa de Análisis Documental y Validación del Diseño (AD).

Para cualquier consulta adicional o para entrega online, comunicarse al correo electrónico: **metrologia@inacal.gob.pe**.