

CONTROL METROLÓGICO DE INSTRUMENTOS CON SOPORTE EN LA NUBE

Pedro de Migue Anasagasti⁽¹⁾ y Juan Manuel González García⁽²⁾

⁽¹⁾Catedrático jubilado de la Universidad Politécnica de Madrid.

⁽²⁾Profesor Titular de la Universidad Politécnica de Madrid E.T.S.I.I. José Gutiérrez Abascal, 2, 28006 Madrid.

⁽²⁾ Telf: 910677200. Correo: juanmanuel.gonzalez@upm.es.

RESUMEN: Se desarrolla el concepto de instrumento con soporte en la nube y se plantean los cuatro componentes que lo forman: unidad de campo, servidor de instrumentos, plataforma hardware y software y administrador.

A continuación, se analizan las alternativas de diseño: nube auxiliar, nube propietaria y solución como un Servicio o Solution as a Service (SaaS).

Seguidamente, se plantea el soporte que se suministra en la nube, analizándose las distintas funcionalidades que puede incluir.

Se continúa con la evaluación de la conformidad de los instrumentos de campo y de la nube, que incluye el examen de tipo de la aplicación software específica para dichas unidades de campo y el examen de tipo de la plataforma hardware y software que alberga dicha aplicación software.

Finalmente, se plantean la conformidad con el tipo y la verificación periódica de la nube, terminando con unas conclusiones.

1 INTRODUCCIÓN

La **nube** se refiere a la computación remota bajo demanda. Es un tipo de sistema informático basado en Internet, donde los recursos compartidos y la información se proporcionan bajo demanda.

Los componentes de un instrumento en la nube se muestran en la Figura 1 y son los siguientes:

- **Instrumento de campo** con conexión remota, que genera información metrológica relevante y la envía al servidor en la nube. Puede recibir órdenes desde la nube.

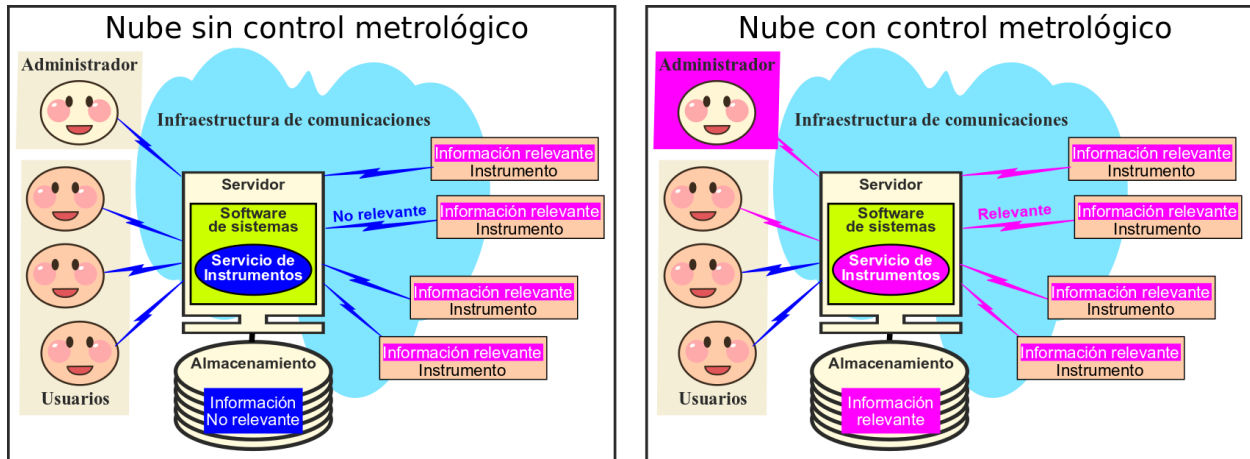


Figura 1 Elementos de un instrumento con soporte en la nube.

- **Servicio de instrumentos**, aplicación software que reconoce y dialoga con el instrumento para aceptar, almacenar y procesar la información generada por el instrumento y, en su caso, para enviarle órdenes. Además, permite a los usuarios acceder a la información del instrumento y, en su caso, solicitar órdenes para el mismo.
- **Plataforma** en la que ejecuta el servicio de instrumentos. Esta plataforma constará de:
 - Infraestructura de comunicaciones, que será en muchos casos Internet, sobre la que puede o no estar implementada una red virtual.
 - Infraestructura de servidor, que incluye hardware de procesamiento y de almacenamiento, además de software de sistema. Se encarga de gestionar las comunicaciones y de dar cobijo y soporte al servicio de instrumentos.
- **Administrador**, encargado de gestionar y mantener el servicio de instrumentos y la plataforma de la nube.

En el diseño de la nube se hace un amplio uso de:

- **Técnicas criptográficas** para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
- **Redundancia** para garantizar la disponibilidad del servicio y de la información.

La nube es un elemento evolutivo, puesto que ha de adaptarse a los cambios tecnológicos y a los retos de seguridad que vayan apareciendo. Además, los problemas que ocurran en la nube pueden afectar a una gran población de usuarios. Es, por tanto, fundamental **certificar los procedimientos** internos de la empresa que suministra el servicio, para garantizar la autenticidad, integridad, disponibilidad y persistencia del servicio y de la información relevante.

2 ALTERNATIVAS DE DISEÑO

Los registradores en la nube, se clasifican en las tres alternativas siguientes, de acuerdo a su relevancia metrológica y a la plataforma: Nube auxiliar, nube de propietario y Solución como un Servicio o Solution as a Service (SaaS).

Nube auxiliar

En esta solución, la información relevante se almacena en el instrumento de campo, enviándose a la nube por un procedimiento no controlado metrológicamente, por lo que pierde su validez legal. Sin embargo, estos datos pueden ser explotados para la gestión de los bienes controlados, aunque no tengan garantía legal.

Nube propietaria

La solución de nube propietaria se presenta cuando una empresa, además de tener los instrumentos de campo, instala y mantiene su propia plataforma de nube con control metrológico. Por ejemplo, una empresa de logística que tiene su propia nube.

Los datos almacenados y posiblemente manipulados en dicha nube son exclusivamente los suministrados por los instrumentos de campo de dicha empresa.

Solución como un Servicio o *Solution as a Service (SaaS)*

En este caso, una empresa crea una nube con conformidad metrológica para determinados instrumentos, para dar servicio a toda una serie de clientes. Cada cliente dispone de sus instrumentos, pero utiliza el servicio en nube suministrado por la SaaS. Por ejemplo, un fabricante de registradores de temperatura suministra el servicio de nube a las distintas empresas de transporte que utilizan sus registradores.

La entidad que ofrece el SaaS puede tener su propia plataforma, en la que ejecuta el servicio de instrumentos, o puede utilizar una *Platform as a service (PaaS)* pública proporcionada por un tercero, como puede ser Amazon, Microsoft, Google, IBM, etc., para albergar su servicio de instrumentos. Las PaaS públicas suelen estar certificadas ISO/IEC 27001.

3 ALCANCE DEL DISEÑO

El alcance del diseño dependerá de las funciones que se implementen en la nube. Dependerá de la sofisticación del servicio de instrumentos, el que incluya más o menos funciones. Las principales funciones que se pueden dar son las siguientes:

Comunicación. Esta función incluye la transmisión de los datos relevantes generados por el instrumento, así como las posibles órdenes que se le puedan enviar. Un aspecto importante en esta función es la identificación mutua de instrumento y servidor para evitar aceptar información falsa o enviar información a servidores no autorizados.

Almacenamiento de información relevante. Uno de los objetivos primarios de la nube es el almacenamiento de la información relativa a los instrumentos y enviada por éstos. Este almacenamiento debe ser estable y persistente de forma que no se pierda la información, aunque ocurran fallos en el sistema de almacenamiento.

Procesamiento de la información relevante. La información recibida puede ser transformada o procesada por la aplicación del instrumento en la nube antes de ser almacenada o utilizada (por ejemplo, puede ser almacenada en una base de datos, filtrada, combinada, etc.). Esta función no es necesaria en todas las instalaciones, pero sí es bastante frecuente.

Generación de informes legalmente relevantes. Esta funcionalidad ha de considerarse si la información relevante es enviada desde la nube a los usuarios en forma de informes o documentos electrónicos con validez legal (por ejemplo, documentos con integridad y autenticidad asegurada mediante fecha y firma electrónica).

Presentación electrónica de información relevante. Esta funcionalidad ha de considerarse si la información relevante es enviada desde la nube a los usuarios para su visualización electrónica, conservando su validez legal.

Control de los instrumentos. Esta función consiste en la capacidad de enviar órdenes a los instrumentos que puedan influir en datos relevantes generados por los mismos.

Administración. Funciones de gestión de usuarios y de registros de eventos y auditoría.

4 INTRODUCCIÓN A LA EVALUACIÓN DE LA CONFORMIDAD Y VERIFICACIONES DE INSTRUMENTOS EN SERVICIO

La evaluación de la conformidad aplicable a la comercialización y puesta en servicio de los registradores de temperatura comprende el examen de tipo y la conformidad con el tipo, mientras que para los instrumentos en servicio deberán realizar la verificación periódica o la verificación después de reparación o modificación.

Es necesario evaluar, por un lado, la conformidad de todos los componentes de los instrumentos de campo, y, por otro lado, la conformidad de la nube.

Conformidad de los instrumentos de campo

La conformidad de los instrumentos de campo es similar a la de los instrumentos convencionales sin soporte en la nube. Esto incluye, como se ha indicado anteriormente, el examen de tipo y la conformidad con el tipo. Además, los instrumentos en servicio requieren verificación después de reparación y verificación periódica. No abordaremos aquí la conformidad de los instrumentos de campo, centrándonos en las peculiaridades de la conformidad de la nube.

Conformidad de la nube

La conformidad de la nube debe abordar dos aspectos complementarios.

- Conformidad del software que proporciona el **servicio de instrumentos**.
- Conformidad de la **plataforma** que da soporte a dicho servicio del instrumento.

5 EXAMEN DE TIPO DEL SERVICIO DE INSTRUMENTOS

El examen de tipo del servicio de instrumentos se ha de basar en un análisis documental de su diseño y en pruebas funcionales, para lo cual nos podemos referir a la guía Welmec 7.2 [2] y a las recomendaciones de WELMEC 7.3 [3].

Siguiendo Welmec 7.2 se utilizará el tipo U de instrumento y la clase de riesgo D.

En un primer paso, es necesario determinar las funciones incluidas en el diseño, tales como:

- Comunicación. Siempre será necesaria.
- Almacenamiento de información relevante. Siempre será necesaria.
- Procesamiento de la información relevante.
- Generación de informes legalmente relevantes.
- Presentación electrónica de información relevante.
- Actualización del servidor del instrumento.
- Control de los instrumentos.
- Funciones de administración y auditoría.

Seguidamente indicaremos las consideraciones más importantes a tener en cuenta, de acuerdo a las secciones consideradas en Welmec 7.2.

5.1 Requisitos básicos

La **documentación** general se centrará en el servidor del instrumento y debe cubrir los siguientes aspectos:

- a) Descripción del software que compone el servidor del instrumento.
- b) Listado de componentes software del servicio de instrumentos.
- c) Manual de usuario del servidor del instrumento.
- d) Manual del administrador del servicio.

Se han de identificar tanto los módulos del servidor del instrumento, así como sus ficheros de configuración y los del software estándar que afecte a la información relevante.

Con respecto a la influencia a través de interfaces de usuario hay que analizar las protecciones y restricciones impuestas a los diferentes roles habilitados, así como las medidas de auditoría implantadas.

Hay que analizar la influencia a través de interfaces de comunicaciones, tanto con los instrumentos de campo como con los usuarios y administradores.

Hay que analizar la protección contra cambios no intencionados.

Hay que analizar la protección contra cambios intencionados.

Hay que analizar la protección de parámetros.

Hay que analizar la autenticidad de los resultados y medidas presentadas.

Hay que analizar la influencia de otro software.

5.2 Transmisión de información relevante. Extensión T

Se han de considerar todos los canales de comunicación de información relevante y de configuración que utilice el servidor del instrumento, tanto hacia los instrumentos de campo como hacia los usuarios o a los operadores y administradores del sistema informático.

Se deberán utilizar los datos del sistema a plena carga, es decir, con el máximo número posible de unidades funcionando a pleno rendimiento. Además, hay que considerar las operaciones de mantenimiento, tanto del software como del hardware, de la plataforma utilizada.

5.3 Almacenamiento de información relevante. Extensión L

El almacenamiento se realiza sobre el soporte de almacenamiento de la plataforma en la que ejecuta el servidor del instrumento, por lo que se analizarán los requisitos adicionales, como la política de respaldo de información (Backus), en el análisis de la plataforma.

5.4 Actualización de software del servidor del instrumento. Extensión D

Esta actualización puede ser automática o manual.

Para el caso de actualización manual de software se aplicarán las secciones D2, D3 y D4, entendiéndose que, en este caso, “transmitido” o “descargado” debe sustituirse por “proporcionado por el fabricante”.

5.5 Separación de software. Extensión S

5.6 Informes legalmente relevantes en fichero o pantalla.

En estos informes se ha comprobado que se cumplen los tres requisitos siguientes:

- Completitud de los datos.
- Autenticidad de los datos.
- Integridad de los datos.

5.7 Administración del servidor del instrumento

Aunque esta figura no se contempla en la guía Welmec 7.2, dependiendo de la complejidad del servidor del instrumento, éste puede requerir funciones de administración, tales como:

- dar de alta usuarios.
- asignar roles y protecciones.
- analizar el registro de eventos o auditoría que genere el servidor del instrumento.

5.8 EXAMEN DE TIPO DE LA PLATAFORMA

El examen de tipo de la plataforma se centrará en asegurar que ésta permita garantizar las siguientes propiedades:

- Disponibilidad del servicio, con un tiempo de respuesta adecuado.
- Persistencia, autenticidad e integridad de la información.

Para conseguir estas propiedades es necesario:

- Que el hardware de la plataforma tenga capacidad suficiente para soportar al servidor de instrumentos en su máxima carga de trabajo, considerando, además, la carga de las posibles operaciones de mantenimiento y administración de la plataforma.
- Que la capacidad de almacenamiento permita almacenar toda la información generada durante su tiempo de validez.
- Que exista un procedimiento automático de salvaguarda de la información (bakup).
- Que el alojamiento del hardware cumpla unos requisitos de seguridad física y ambientales adecuados.
- Que exista una correcta gestión y administración de la nube que garantice su disponibilidad y seguridad. Dicha gestión y administración deberá estar:
 - Programada y documentada.
 - Ejecutada por personal formado y motivado.
 - Incluir un mecanismo de auditoría que permita trazar las operaciones realizadas por el personal.

5.9 Plataforma con certificación ISO/IEC 27001

Si la plataforma está certificada ISO/IEC 27001 la evaluación consiste en verificar que las medidas para garantizar la autenticidad, integridad, disponibilidad o persistencia del servicio y

de la información son adecuadas y que las medidas preventivas correspondientes a cada riesgo también sean adecuadas.

5.10 Plataforma sin certificación ISO/IEC 27001

Será necesario seguir un procedimiento similar al ISO/IEC 27001.

Es necesario hacer un análisis de riesgos que considere todos los riesgos que pueden afectar a la autenticidad, integridad, disponibilidad o persistencia de la información y hay que analizar que las medidas preventivas correspondientes a cada riesgo sean adecuadas. Se han de considerar riesgos como los siguientes:

- Riesgos no intencionales.
 - Riesgos naturales: como eventos meteorológicos o terremotos.
 - Medio ambiente: como incendios o inundaciones/daños por agua.
 - Fallos del equipo: como fallos en los equipos informáticos, de comunicación, de distribución de energía o de aire acondicionado.
 - Fallos en las aplicaciones.
 - Interacción humana: como errores en el mantenimiento, administración o la operación.
 - Mantenimiento: como mantenimiento inapropiado o supervisión de mantenimiento no adecuado.
- Riesgos intencionales.
 - **Ciberataques.**
 - Interacción humana: como la mala conducta de los empleados o el comportamiento criminal.
 - Robo o destrucción de equipos.
 - Robo, modificación, destrucción o diseminación de la información.
 - Sabotaje.

También se han de verificar que cumplen adecuadamente los puntos siguientes de ISO/IEC 27001:

- A.5.1.1 Políticas para la seguridad de la información.
- A.6.1.1 Roles y responsabilidades en seguridad de la información.
- A.6.1.2 Segregación de tareas.
- A.6.1.3 Contacto con las autoridades.
- A.7 Seguridad relativa a los recursos humanos.
- A.8.1 Responsabilidad sobre los activos.
- A.8.3 Manipulación de los soportes.
- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad física y del entorno.
- A.12 Seguridad de las operaciones.
- A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.16 Gestión de incidentes de seguridad de la información.
- A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio.
- A.18.2 Revisiones de la seguridad de la información.

6 CONFORMIDAD CON EL TIPO DE LA NUBE

Con respecto al servicio de instrumentos, al tratarse de un software, no se requiere conformidad con el tipo, puesto que no hay proceso de fabricación; basta con el examen de tipo.

Con respecto a la plataforma de la nube, dada la singularidad de cada instancia, no parece posible separar la aprobación del diseño de la plataforma (examen de tipo) de su implantación en una instalación específica (examen de conformidad con el tipo).

Por ello, parece más adecuado integrar ambas funciones en el examen de tipo, que deberá incluir la o las diferentes instalaciones que se pongan en marcha.

7 VERIFICACIÓN PERIÓDICA DE LA NUBE

La certificación ISO/IEC 27001 suele durar tres años, pero las organizaciones deben realizar auditorías internas de rutina como un proceso de mejora continua. Una vez certificado, un organismo de certificación generalmente realizará una evaluación anual para monitorear el cumplimiento.

Por tanto, se deberá realizar una evaluación anual para comprobar:

- Que la certificación ISO/IEC 27001 sigue vigente, para el caso de plataformas con esta certificación.
- Que se están cumpliendo correctamente todas las condiciones y procedimientos de seguridad, administración, mantenimiento, etc. incluidas en el examen de tipo.

8 CONCLUSIONES

La conformidad de los instrumentos de campo es similar a la de los instrumentos convencionales sin soporte en la nube.

La conformidad del servicio de instrumentos consistirá en el examen de tipo, que puede basarse en las recomendaciones de la guía Welmec 7.2 con tipo U de instrumento y clase de riesgo D.

En cuanto a la nube, es fundamental certificar los procedimientos internos de la empresa que suministra el servicio, introduciendo el factor humano de gestión y administración, para lo que se puede seguir la norma ISO/IEC 27001.

El examen de conformidad de la nube debería integrarse con el examen de tipo. Pudiendo añadirse cada instalación como un anexo de la misma.

Es necesario realizar una revisión periódica de la nube, para comprobar que se cumplen los procedimientos incluidos en el examen de tipo.

9 REFERENCIAS

[1] UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

[2] WELMEC Guide 7.2:2021. European Cooperation in Legal Metrology.

[3] WELMEC 7.3:2020. European Cooperation in Legal Metrology.