ÍNDICE

Página

MODIFICACIONES RESPECTO A LA REVISIÓN ANTERIOR

Se añade el Anexo III – INTEGRIDAD DE DATOS UNE-EN ISO/IEC 17020

1. INTRODUCCIÓN

1.1 Objeto y ámbito

Este documento tiene como finalidad ser una guía para las entidades acreditadas por ENAC en el establecimiento de sistemas que les permitan asegurarse, y poder demostrar a terceros, que llevan a cabo una adecuada gestión y protección de los datos relevantes a sus actividades, principalmente en aquellos aspectos que garanticen que los datos son atribuibles, trazables, exactos y recuperables en todo su ciclo de vida.

El documento pretende como objetivo principal ser una ayuda para los organismos de evaluación de la conformidad, y no se circunscribe necesariamente a los conceptos y términos usados en las normas de acreditación, por lo que en ocasiones usa términos no utilizados en dichas normas y hace recomendaciones que, en algunos casos, pueden exceder los requisitos establecidos en ellas.

Las buenas prácticas recogidas en esta guía deberían ser consideradas en todas las actividades de evaluación de la conformidad que generen o gestionen datos y registros, siendo especialmente crítico para los datos cuya falta de integridad afecte a la veracidad de los resultados.

Estos datos están generalmente asociados, aunque no exclusivamente, a las siguientes fuentes:

- Sistemas informáticos para el procesado y gestión de datos.
- Equipos que generan datos primarios.
- Registros en papel (hojas de trabajo, formularios, etc.…) que sirvan de soporte a los datos.
- Información archivada en soporte electrónico o en papel.

El documento se estructura en:

- una parte general que establece recomendaciones aplicables en cualquier actividad de evaluación de la conformidad en el que la garantía de la integridad de los datos constituye un elemento intrínseco de la norma.
- Una serie de anexos con la concreción de los principios generales a normas de acreditación específicas[1]

1.2 Referencias normativas

- 21 CFR Part 11: Electronic Records; Electronic Signatures (1997).
- UNE-EN ISO/IEC 27000 "Tecnologías de la información. Sistemas de Gestión de la Seguridad de la Información. Visión de conjunto y vocabulario".
- FDA: Data Integrity and Compliance with CGMP. Q&A, Guidance for Industry (2018).

1.3 Términos y definiciones

- **Integridad de datos:**
  Es la confianza en que los datos son completos, coherentes y exactos, a lo largo de su ciclo de vida.

- **Datos Primarios:**
  Datos que no han sido procesados previamente a su uso, siendo el resultado directo de observaciones originales y actividades realizadas, y que son necesarios para reconstruir y evaluar los resultados de tales actividades.

- **Registro Primario:**
  Cualquier hoja, formulario cumplimentado o cuaderno de trabajo, registro, informe, notas o copias exactas de estos, en los que se recogen los datos primarios.

- **Datos Estáticos:**
  Datos mantenidos en un registro fijo, tal como un papel o una imagen electrónica.

[1] En el momento de la publicación de la Revisión 4 de este documento se han desarrollado solamente los anexos referentes a las normas ISO/IEC 17025, ISO 15189 e ISO(IEC 17020. Es voluntad de ENAC el elaborar, anexos similares para otras normas de acreditación.

- **Datos Dinámicos:**
  Datos mantenidos en un formato que permite la interacción entre el usuario y el contenido del registro.

- **Copia Verdadera:**
  Copia exacta y verificada de un registro que puede almacenarse utilizando el mismo o diferente formato que el utilizado en el registro original.

- **Registro electrónico:**
  Cualquier combinación de texto, gráficos, datos, audio, imágenes u otra información en forma digital creada, modificada, mantenida, archivada, recuperada o distribuida por un sistema informático.

- **Metadato:**
  Datos que describen los atributos de otros datos y proporcionan contexto y significado. Se trata de datos que describen la estructura, los elementos de los datos, las interrelaciones y otras características de los datos

- **Sistema híbrido:**
  Sistema que puede combinar procesos manuales y otros automatizados, o bien combinar datos en papel y datos en formato electrónico.

2. INTEGRIDAD DE DATOS: PRINCIPIOS Y EXPECTATIVAS

La integridad de los datos se confiere por la combinación de los siguientes atributos (*):

- Imputables al autor de los datos (**A**tribuibles).
- Claramente leíbles siempre que sea necesario (**L**egibles y permanentes).
- Registrados en el momento que son obtenidos (**C**ontemporáneos).
- Registrados la primera vez que se observan o generan (**O**riginales).
- Sin errores, precisos y correctos (Exactos - **A**ccurate).

Además de cumplir con estos atributos, los datos deben ser completos, coherentes (en su contexto), duraderos y disponibles (*).

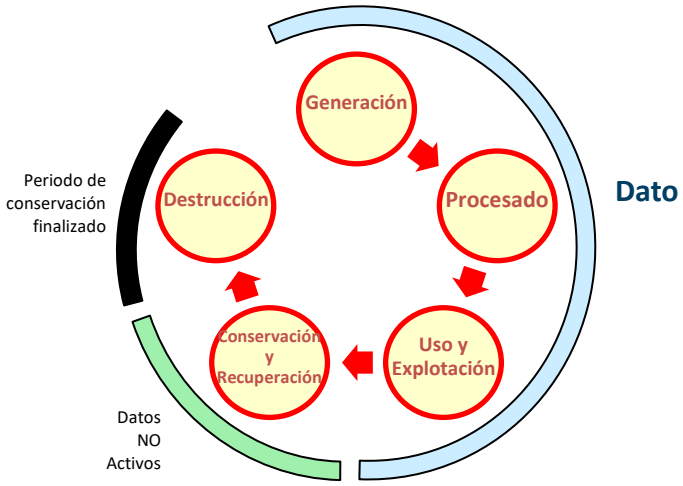
(*) La combinación de estos atributos en algunos sectores se plasman a través de los conceptos ALCOA y ALCOA+.

2.1 Ciclo de vida

La necesidad de garantizar la integridad de los datos comprende todo el ciclo de vida de estos, entendiendo como tal la siguiente secuencia:

1. Generación y registro.
2. Procesado, incluyendo análisis, transformación y migración.
3. Uso y explotación.
4. Conservación y recuperación.
5. Destrucción.

Cada una de estas etapas incluyen las medidas necesarias para garantizar que los datos cumplen con los atributos expuestos en el apartado anterior. El ciclo de vida de los datos puede representarse mediante el siguiente esquema:



La garantía de la integridad de los datos en todo su ciclo de vida hace necesaria la consideración de una visión global de los procesos por los que transcurren los datos. Estos procesos deberían ser analizados con el fin de identificar los posibles riesgos para la integridad.

El análisis de riesgos para la integridad de los datos debería considerar al menos:

a) El formato de los datos: electrónicos o en papel, ya que la necesidad de garantizar la integridad de los datos afecta a ambos soportes.
b) Las acciones manuales realizadas durante el ciclo y los procesos híbridos implicados.
c) La criticidad del dato y sus atributos, en cuanto al impacto que una deficiencia en su integridad puede tener en el resultado final de la actividad en la que se incluye el dato.

2.2 Medidas para garantizar la integridad de los datos

La necesidad de garantizar la integridad de los datos a lo largo de todo su ciclo de vida, y de mitigar los riesgos para tal integridad, conlleva la adopción de medidas de control que, en función de la naturaleza de los datos, su ciclo de vida y las operaciones incluidas en cada una de las etapas del ciclo pueden ser de tres tipos:

a) **Tecnológicas,** basadas en el diseño y capacidades funcionales de los equipos o sistemas relacionados con el dato.
b) **Operativas,** basadas en la concepción de los procesos de gestión de los datos y en los procedimientos relacionados con cada etapa de su ciclo de vida.
c) **Organizativas,** basadas en las responsabilidades sobre los datos y los equipos y sistemas que los soportan, asignadas a las personas que intervienen en las diferentes etapas del ciclo de vida.

2.3 Recomendaciones de carácter general para la integridad de los datos

A continuación, se detalla una serie de buenas prácticas de carácter general dirigidas a asegurar la integridad de los datos, basadas en una combinación de las medidas anteriormente indicadas:

1. Todos los procesos relacionados con la creación, modificación, revisión, archivado y destrucción de datos deberían estar documentados.
2. Los datos deberían ser registrados directamente en los soportes previstos para ello, evitando cuando sea posible las trascripciones.
3. En el caso que el soporte utilizado en el registro inicial de los datos no sea duradero (p.ej. papel térmico), es conveniente tomar medidas para asegurar la legibilidad de los datos a lo largo del tiempo. Los registros primarios se deben conservar durante un periodo de tiempo previamente establecido, coherente con las obligaciones contractuales, legales o las adquiridas con ENAC.
4. Cuando sea necesario modificar los datos primarios por alguna razón justificada, las modificaciones deben ser trazables a sus originales. Cualquier anulación de los datos primarios debe estar registrada.
5. Los procesos de revisión de los datos deberían incluir toda la información relacionada con los mismos (datos y metadatos).
6. Todos los datos registrados deben ser atribuibles a la persona que ha realizado su registro.
7. Es importante mantener la trazabilidad con todos los parámetros y elementos que han permitido obtener un dato concreto.
8. Se debe disponer de mecanismos que aseguren la apropiada conservación y protección de los datos a lo largo de todo su ciclo de vida.
9. El tiempo mínimo de conservación de la información debería estar documentado.

2.4 Recomendaciones adicionales para la gestión de los sistemas informáticos

La gestión de los sistemas informáticos, que intervienen en cualquier etapa del ciclo de vida de los datos, debería tener en consideración los siguientes aspectos:

1. Es recomendable disponer y mantener un listado o inventario actualizado de los equipos de generación de datos, que incluya al menos:
   - Instrumentos de medida que capturen o generen datos.
   - Sistemas informáticos que intervengan en las etapas del ciclo de vida del dato, asociados a procesos o equipos de medida, o que se utilicen en funciones de gestión u operaciones con los datos.
2. Los equipos, instrumentos y sistemas informáticos que generen, gestionen o almacenen datos deben ser validados de acuerdo con su uso previsto en el proceso en el cual están involucrados.
3. Los cambios en equipos, instrumentos o sistemas informáticos validados deberían llevarse a cabo de una manera ordenada y controlada, con el fin de evaluar el impacto del cambio en el rendimiento del equipo y la integridad de los datos gestionados, y debe validarse antes de su implantación.
4. Las interfaces entre sistemas deberían estar protegidas con el fin de asegurar la integridad de los datos durante su transmisión. La validación del sistema debe incluir algún tipo de comprobación de su correcto funcionamiento y transmisión de datos
5. Es aconsejable definir las responsabilidades aplicables a cada uno de los sistemas informáticos, valorando los riesgos para la integridad de los datos y tomando las acciones necesarias. Por ejemplo, estableciendo diferentes perfiles de usuario, o segregando las responsabilidades sobre los sistemas evitando que los administradores de los sistemas tengan también responsabilidades sobre la generación, revisión o aprobación de los datos.
6. Se debe disponer de mecanismos de seguridad para restringir el acceso al equipo sólo a personas autorizadas.

   Los controles de seguridad dependerán de la criticidad del sistema informático, por ejemplo:
   - Utilizar un sistema de autenticación con usuario y contraseña única para cada usuario. Las contraseñas serían estrictamente confidenciales, no se podrían revelar a terceras personas y deberían cambiarse con una frecuencia adecuada.
   - Desconexión de todos los usuarios al abandonar los sistemas.
   - Acceso de los usuarios únicamente a las funcionalidades necesarias para realizar su actividad
   - Asegurar que los usuarios tienen la formación necesaria para el uso de forma segura.
   - Impedir a los usuarios tener acceso directo de escritura/borrado a las carpetas con datos desde el sistema operativo, fuera de los mecanismos o funciones definidas por el software.
   - Etc.....

7. La seguridad en los sistemas informáticos se debería extender a todos los componentes críticos del mismo, incluyendo bases de datos y aplicaciones críticas. Únicamente debería ser aceptable el acceso sin contraseña a un sistema si este acceso es únicamente de lectura.
8. En función de los riesgos identificados, se deberían implementar medidas de protección en el equipo, tales como antivirus, antispyware, cortafuegos, etc...
9. En el caso de que el sistema trabaje en ausencia de un usuario, es aconsejable considerar un proceso de bloqueo de acceso. En sistemas de alto riesgo se debería configurar un proceso de desconexión automática o bloqueo del sistema en caso de inactividad.
10. El sistema debería utilizar una fuente de tiempo (fecha / hora) segura, de forma que no pueda ser alterada por los usuarios.
11. Dependiendo de la criticidad del sistema de almacenamiento de datos, es conveniente impedir el acceso físico a los mismos por parte de personal no autorizado. A continuación, se indican a modo de ejemplo algunas medidas de seguridad física que se podrían contemplar:
    - El acceso al espacio o la sala donde se encuentra ubicado el equipo.
    - El acceso a los componentes críticos del equipo o su configuración.
    - Cuando proceda, protección contra incendios, inundaciones o ambientes pesados que puedan comprometer su rendimiento.
    - Condiciones medioambientales de operación.
    - Etc.....
12. Los sistemas de copias de seguridad o de archivo que se utilizan para almacenar datos de manera externa al sistema, se deberían mantener separadas de éste, con las medidas de seguridad apropiadas en función de la relevancia de los datos. Todos los datos relevantes, y sus metadatos asociados, deben ser protegidos mediante copias de seguridad adecuadas, establecidas con un alcance y una frecuencia acorde a la relevancia y criticidad de los datos.
13. Es aconsejable que los procesos de copia de seguridad y restauración se comprueben periódicamente en cuanto a su correcto funcionamiento.
14. Cuando las hojas de cálculo son utilizadas como almacén de información, deben establecerse medidas que garanticen la integridad de los datos almacenados. Es recomendable utilizarlas únicamente para la realización de cálculos a partir de plantillas validadas y almacenadas en lugar seguro. Cuando se empleen hojas de cálculo se debería extremar las medidas de seguridad (p.ej. mediante acceso restringido).
15. Es recomendable para control de la generación y modificación de los datos el uso de la herramienta Audit Trail, registro electrónico seguro, generado de manera automática, que identifica quién y cuándo (fecha/hora) se ha generado o modificado el dato, de forma que permita la reconstrucción de la secuencia de eventos relacionados con la creación, modificación o borrado de registros electrónicos.

16. En caso de que las limitaciones técnicas del sistema no permitan establecer las medidas de seguridad descritas en este apartado, podrían establecerse otras de carácter manual documentadas que permitan alcanzar un nivel de seguridad similar, tales como registros manuales de acciones realizadas, registro de accesos, equivalente manual al Audit Trail, restricción al acceso a funciones críticas para la seguridad, etc.

ANEXO I: INTEGRIDAD DE DATOS: UNE-EN ISO/IEC 17025

Se detallan a continuación la aplicación de esas buenas prácticas a los apartados específicos de la norma UNE-EN ISO/IEC 17025, en los que los datos, documentos o registros a los que se hace referencia requieren una garantía de su integridad, en los términos que se establecen en el apartado 2.1 de esta guía.

Los aspectos desarrollados a continuación son aplicables de igual forma a las actividades de ensayo, calibración y muestreo que puede realizar un laboratorio.

NOTA: En este documento se utiliza el término "debe" cuando se refiere a un requisito incluido en la norma UNE-EN ISO/IEC 17025.

1. Organización y personal

UNE-EN ISO/IEC 17025: apartados 5.5, 5.7, 6.2.5.

1. Responsabilidades: En el caso de disponer de sistemas informáticos que intervengan en los resultados o actividades realizadas, el laboratorio debería definir las responsabilidades sobre la gestión de estos sistemas y de los datos en formato electrónico.

2. Control de cambios: Los sistemas informáticos deben mantenerse en un estado de control adecuado para asegurar la integridad de los datos que gestionan.

   Para mantener este estado de control, es aconsejable disponer de un procedimiento de control de cambios, con responsabilidades claramente definidas, que evalúe el impacto de los cambios antes de que estos se implanten y establezca las medidas necesarias para mantener el sistema y la integridad de los datos en el mismo estado de control.

3. Formación: la documentación relacionada y los registros de formación y cualificación están a menudo en soporte electrónico. En este caso, éstos deberían ser de acceso limitado a los responsables y estar protegidos.

2. Instalaciones y equipos

UNE-EN ISO/IEC 17025: apartados 6.3.3, 6.4.1, 6.4.2, 6.4.4, 6.4.13

1. Condiciones ambientales: Algunos de los sistemas más habituales empleados por los laboratorios cuando es necesario monitorizar y controlar las condiciones ambientales, son:
   - Sistemas de monitorización ambiental (sistemas SCADA) que registran y almacenan datos ambientales y tienen capacidad de emitir gráficos e informes. En estos sistemas es importante garantizar la seguridad de los datos primarios: ubicación, acceso, copias de seguridad.

- Dispositivos móviles que registran las condiciones ambientales (p.ej. Data loggers), cuyos datos son descargados en un PC, siendo revisados posteriormente por personal del laboratorio. En este caso es importante limitar el riesgo de manipulación de los datos, para lo cual debería establecerse un sistema controlado, con responsabilidades claras, del proceso de descarga y archivo de datos.

2. Equipos: Se debería disponer de un listado o inventario de los sistemas informáticos y equipos de generación de datos para poder determinar fácilmente si cada uno dispone de los elementos de control, seguridad y procedimientos de uso necesarios.

   Cuando el laboratorio utiliza equipamiento que está fuera de su control permanente, también debe asegurar la integridad de los datos que son generados por esos equipos.

   Los equipos, instrumentos o sistemas informáticos que generan datos deben disponer de registros de su verificación o validación (véase también clausula 3.4), así como de las incidencias que se puedan producir. Cualquier cambio relevante en un equipo informático debe validarse o verificarse para asegurar que no tiene impacto en los elementos de control y seguridad que garantizan la integridad de los datos manejados por el equipo.

3. Procesos del laboratorio

UNE-EN ISO/IEC 17025: apartados 7.2, 7.3, 7.4, 7.5, 7.7 y 7.8

1. Métodos:

   Los sistemas informáticos de los que se obtienen resultados calculados a partir de datos primarios (p.ej. hojas de cálculo), deben estar validados y protegidos frente a cambios no autorizados. La validación debe incluir pruebas documentales que demuestren que:

   - Mediante los cálculos que realiza se obtienen resultados equivalentes a los obtenidos mediante un método independiente.
   - Las fórmulas que incluye están protegidas, no son accesibles sin contraseña y sólo son accesibles las entradas de los datos primarios.

   Si se utiliza software de cálculo, entendiendo como tal un sistema de cómputo numérico que ofrece un lenguaje de programación propio, debe estar caracterizado (versión, módulos instalados, requisitos de sistema operativo y de hardware) para el uso previsto por parte del laboratorio y sujeto a control de cambios.

2. Identificación de ítems de ensayo o de calibración: El proceso de etiquetado es esencial para garantizar la trazabilidad y evitar errores. En el caso de que la emisión de etiquetas se genere por sistemas informáticos, estos deberían estar controlados, protegidos y ser únicamente accesibles al personal autorizado.
3. Registros técnicos: El cumplimiento de las buenas prácticas recogidas en el apartado 2 de este documento para los datos y metadatos permiten asegurar que los registros técnicos de cada una de las actividades son fiables e íntegros. Los datos dinámicos (los que permiten reproducir el resultado de la medición, a partir del dato primario) deben también conservarse.

Además, en caso de que estos registros sean electrónicos, es aconsejable que el sistema asocie automáticamente usuario y fecha-hora de cada registro.

Las modificaciones sobre los registros técnicos deben ser trazables a versiones anteriores u observaciones originales. Para ello es recomendable conservar tanto los registros originales como modificaciones. En el caso que éstos sean electrónicos, es aconsejable que el sistema informático disponga de sistemas de control para garantizar esta trazabilidad (p.ej. la herramienta Audit Trail).

4. Aseguramiento de la validez de los resultados: debe garantizarse que los datos generados en las actividades para asegurar la validez de los resultados son recuperables para su tratamiento y verificación posterior.
5. Informe de resultados: La integridad de los datos contenidos en un informe de resultados debe garantizarse mediante revisión frente a los originales o, en caso de que el informe proceda de un sistema informático, validar la coherencia y exactitud de los datos contenidos en el informe y los datos electrónicos originales del sistema.

   En aquellos casos en los laboratorios transmiten de forma electrónica los resultados, se deberán adoptar medidas de seguridad proporcionales a los riesgos asociados a la criticidad de la información que va a reportar, y tener en cuenta, en su caso, las recomendaciones o exigencias de sus clientes. Los cambios, correcciones o nuevas emisiones de un informe de resultados, deben quedar trazados mediante controles adecuados de las versiones del sistema de gestión documental o por alguna funcionalidad disponible en el sistema informático (p.ej. Audit Trail).

4. Control de los datos y sistemas de gestión

UNE-EN ISO/IEC 17025: apartado 7.11

1. Control de los datos y gestión de la información: Los sistemas de gestión de la información del laboratorio utilizados para recopilar, procesar, registrar, informar, almacenar o recuperar datos deben validarse en cuanto a su funcionalidad por parte del laboratorio antes de su introducción. Siempre que haya cualquier cambio, incluida la configuración del software del laboratorio o modificaciones al software comercial listo para su uso, se debe autorizar, documentar y validar antes de su implementación.

   Todo sistema validado debe estar bajo control de cambios. De otra manera no es posible garantizar el estado continuado de validación.

   El software comercial de uso general en el campo de aplicación para el cual fue diseñado se puede considerar que está suficientemente validado. Esto es únicamente aplicable al software comercial que no es personalizado. En caso contrario debe validarse.

2. Validación de los sistemas: Todo sistema del laboratorio que interviene en la adquisición, almacenamiento, procesado o cálculo de datos se debe validar. La diversidad de sistemas y modos de utilizar un mismo sistema hacen difícil establecer una metodología de validación común a todos los casos, aun así, todo proceso de validación debería disponer de:

   a) Preparación, contemplando:

      - Requisitos de usuario documentados que definan cual es el propósito del sistema y qué funciones debe realizar.
      - Documentación adecuada (especificaciones, manuales, etc. en caso de sistemas no desarrollados por el laboratorio) y procedimientos que garanticen que el sistema se utilizará y mantendrá de la manera prevista para garantizar/preservar la integridad de los datos.
      - Un protocolo o plan de validación que establezca las comprobaciones y pruebas a realizar: de instalación, de integridad de la información, de accesos, funcionales, etc. describiendo, paso a paso, cómo se hacen las pruebas y qué se pretende con cada una, y que contemple resultados esperados o criterios de aceptación de las pruebas.

   b) Comprobación del sistema, que debería incluir, en función del tipo de sistema a validar:

      - En caso de sistemas no desarrollados por el laboratorio, comprobaciones en cuanto a la instalación del sistema, de modo que se demuestre que se lleva a cabo según las recomendaciones del suministrador y se configura conforme a los requisitos de usuario.
      - Comprobación del uso, de modo que se garantice la integridad de los datos.
      - Pruebas para demostrar que funciona según se espera, mediante test o similar, que deberían incluir las funciones que se van a utilizar, tales como una entrada de datos, un cálculo (que se podrá comparar mediante su realización por un método independiente), la comparación de los datos impresos en un informe con los que se ven en pantalla, casos que pudieran poner en riesgo el funcionamiento del sistema por su criticidad (por ejemplo, valores extremos en cálculos), etc.
      - Pruebas de seguridad que demuestren que sólo los usuarios autorizados acceden al sistema mediante combinaciones de usuario y contraseña, así como a las funciones y datos que son de su responsabilidad y están autorizados.
      - Si hay interfaces entre sistemas y transferencia de datos, pruebas que demuestren el correcto funcionamiento de estas.

   c) Obtención de los resultados, con una declaración de si se cumplen los resultados esperados o los criterios de aceptación establecidos.

   El laboratorio deberá mantener registros de la validación que permitan demostrar que el sistema es apto para el uso previsto.

Los cambios realizados sobre un sistema validado y en uso deben documentarse, validarse y autorizarse antes de su introducción. Esta nueva validación debería extenderse también a otras funcionalidades que pudieran haberse visto afectadas por dicho cambio

Cuando el sistema es gestionado o mantenido por un proveedor externo, el laboratorio es responsable de asegurar y demostrar que también éste cumple con los requisitos aplicables de la norma.

ANEXO II: INTEGRIDAD DE DATOS UNE-EN ISO 15189

Se detalla a continuación la aplicación de esas buenas prácticas a los apartados específicos de la norma UNE-EN ISO 15189, en los que los datos, documentos o registros a los que se hace referencia requieren una garantía de su integridad, en los términos que se establecen en el apartado 2.1 de esta guía.

NOTA: En este documento se utiliza el término "debe" cuando se refiere a un requisito incluido en la norma UNE-EN ISO 15189.

UNE-EN ISO 15189: apartado 4.1.1.4. Director del laboratorio

Entre las funciones y responsabilidades del director del laboratorio (o persona en quién delegue) están las relacionadas con los sistemas de información y el aseguramiento de la integridad de los datos. Entre otros aspectos debería asegurar la adecuada implantación de los procesos de integración de los sistemas de información del laboratorio (SIL) con los sistemas de información externos como por ejemplo la historia clínica electrónica (HCE), y establecer medidas para controlar que la información de entrada y salida es completa y trazable.

UNE-EN ISO 15189: apartado 4.5. Análisis efectuados por laboratorios subcontratistas

En el caso de que los sistemas de información del laboratorio y del subcontratista estén conectados, sería necesario realizar una verificación que asegure la transcripción fidedigna de los datos. Esta verificación se debería llevar a cabo, al menos en las siguientes situaciones:

- ✓ al implantar la conexión
- ✓ ante modificaciones o cambios de versión de los sistemas
- ✓ ante cualquier cambio o incorporación de nuevas pruebas subcontratadas
- ✓ periódicamente, aunque no se hayan producido cambios

UNE-EN ISO 15189: apartado 4.6. Servicios externos y suministros

Tanto la selección, aprobación como el seguimiento de desempeño de los proveedores debería incluir aquellos que provean sistemas para la gestión de la información.

UNE-EN ISO 15189: apartado 4.7. Servicio de asesoramiento

El laboratorio debería proporcionar asesoramiento sobre las posibles limitaciones de uso y los factores a tener en cuenta en la explotación de los datos una vez transmitidos a la historia clínica electrónica, a la historia clínica de salud u otros sistemas explotables mediante inteligencia artificial. Los metadatos asociados a los datos de laboratorio deberían considerarse para usos posteriores de la información ya sea para un paciente concreto o para estudios poblacionales o de investigación.

UNE-EN ISO 15189: apartado 4.13. Control de los registros

2. El cumplimiento de las buenas prácticas recogidas en el apartado 2 de este documento para los datos y metadatos debería asegurar que los registros técnicos de cada una de las actividades son fiables e íntegros. Los datos dinámicos (los que permiten reproducir el resultado de la medición, a partir del dato primario) deberían también conservarse.

UNE-EN ISO 15189: apartado 4.14.5. Auditoría interna

Las auditorías internas deberían cubrir los sistemas de información, incluida la realización de copias de seguridad, la integración con sistemas externos y la trazabilidad desde la solicitud hasta el informe emitido, comprobando que en todo momento se puede conocer quién y cuándo ha intervenido en la generación, modificación y transmisión de los datos y registros electrónicos.

UNE-EN ISO 15189: apartado 4.14.6. Gestión del riesgo

Se deberían analizar los riesgos inherentes a la transmisión y modificación de datos entre los diferentes sistemas (ej.: HCE, petición electrónica, sistemas de inteligencia artificial para detección de patrones de riesgo, etc.), así como los riesgos asociados cuando los datos no se transmiten automáticamente al SIL (ej.: analizadores no conectados, técnicas manuales), tomando medidas para minimizarlos y controlarlos.

UNE-EN ISO 15189: apartado 4.15. Revisión por la dirección

Los elementos de entrada de la revisión por la dirección deberían incluir expresamente los sistemas de gestión de información: cambios acontecidos, revisión periódica y adecuación a la sistemática actual de trabajo, integración con sistemas externos, incidencias, medidas de control, etc.

UNE-EN ISO 15189: apartado 5.1. Personal

1. Debería definirse un responsable para la gestión de los sistemas de información y para la integración del SIL con los sistemas de información externos.
2. Se deberían tomar medidas para que la información sensible del personal (ej.: registros de formación y experiencia) sean de acceso limitado al personal autorizado.
3. La formación del personal debería incluir aspectos relacionados con los sistemas de información, integración entre los diferentes sistemas, confidencialidad de la información o integridad de los datos.

UNE-EN ISO 15189: apartado 5.3. Equipo de laboratorio

1. Es recomendable disponer de un listado actualizado de todos los equipos y sistemas de información que intervienen en el ciclo de vida del dato.
2. Cuando el laboratorio utiliza equipamiento que está fuera de su control permanente, también debe asegurar la integridad de los datos que son generados por esos equipos.
3. Se debería asegurar que la fecha de los equipos (día y hora) está sincronizada con un sistema general.
4. En el caso de equipos conectados al SIL a través de un middleware, se debería asegurar la trazabilidad de la información.
5. Los sistemas informáticos de los que se obtienen resultados calculados a partir de datos primarios (p.ej. hojas de cálculo), deben estar validados y protegidos frente a cambios no autorizados. La validación debería incluir pruebas documentales que demuestren que:
   - mediante los cálculos que realiza se obtienen resultados equivalentes a los obtenidos mediante un método independiente.
   - las fórmulas que incluye están protegidas, no son accesibles sin contraseña y sólo son accesibles las entradas de los datos primarios.

UNE-EN ISO 15189: apartado 5.4. Procesos preanalíticos

1. En caso de petición electrónica se debería garantizar la trazabilidad de los datos y su integración con el SIL.@
2. En el caso de dispositivos POCT, en ausencia de una solicitud formal, debería identificarse la muestra con un identificador único del paciente para que se pueda incorporar la petición al SIL.
3. Cuando se utilicen plataformas on-line (web) de información a pacientes y usuarios, debería existir un responsable o un sistema que garantice la actualización de dicha información.

UNE-EN ISO 15189: apartado 5.8. Notificación de los resultados

Con la finalidad de garantizar la interoperabilidad entre sistemas de información, se debería considerar el uso de sistemas de codificación de pruebas de laboratorio, como LOINC, GNC, SNOMED, IUPAC, etc.

UNE-EN ISO 15189: apartados 5.10.2 y 5.10.3. Gestión de la información del laboratorio

1. Acceso restringido

Al definir los permisos de acceso a los distintos sistemas de información existentes en el laboratorio, se debería tener en cuenta el puesto de trabajo y las funciones y responsabilidades para las que esté autorizada cada persona del laboratorio. Esto incluiría:

- acceso a los datos e información de los pacientes
- introducción de datos de pacientes
- modificación de datos de pacientes
- introducción de resultados
- modificación de resultados
- comunicación de los resultados de los análisis y emisión de informes de laboratorio
- configuración de los sistemas de información

Debería estar documentada la sistemática y responsabilidades para conceder los permisos de acceso a los sistemas de información.

2. Instrucciones de uso

Se debería disponer de procedimientos documentados para el uso de los sistemas de gestión de la información. Pueden utilizarse las propias instrucciones de los proveedores de estos sistemas, siendo completadas por el laboratorio con la información necesaria.

Además, deberían estar documentadas las relaciones existentes entre los diferentes sistemas, incluidos los middleware, HCE, sistemas externos, etc.

3. Medidas frente al acceso no autorizado

Los sistemas de gestión de la información deben estar protegidos contra el acceso no autorizado y contra la manipulación indebida. Lo habitual es utilizar un sistema de autenticación con usuario y contraseña única y confidencial para cada usuario, y en caso de inactividad bloquear la cuenta del usuario. Pueden existir situaciones excepcionales, en el uso de equipos analíticos, en las que estos sistemas no sean de aplicación o se utilice un usuario genérico. Estas situaciones deberían estar justificadas por la ausencia de riesgo y por llevar a cabo otras medidas alternativas de control.

4. Validación y verificación

4.1. La verificación/validación de los sistemas de gestión de la información debería realizarse siempre ante la implantación, modificación o actualización de:

4.2. Sistemas de información del laboratorio (SIL)

4.3. Sistemas de información externos al laboratorio con los que está conectado el SIL, como pueden ser: historia clínica electrónica, sitios web, solicitud electrónica, sistemas informáticos de laboratorios subcontratistas, etc.

4.4. Otros sistemas conectados al SIL. Ej.: middleware, software de los analizadores.

La profundidad de las actividades de verificación en caso de actualizaciones o modificaciones serán acordes a los cambios realizados y a la información aportada por el proveedor.

4.5. Aspectos a tener en cuenta en la verificación:

- que los datos, resultados, unidades y comentarios se transmiten de forma correcta.
- considerar diferentes variables como factores de dilución, creación de pruebas reflejas, fórmulas, algoritmos matemáticos, conversión de resultados numéricos en no numéricos (ej.: positivo/negativo, indetectable), delta check, diferentes equipos o sites que confluyen en un informe único, equipamiento POCT, pruebas internas que se utilizan para la validación de resultados como son los índices séricos, informes evolutivos, gráficos, detección de patrones de riesgo, etc.

5. Integración y conectividad entre sistemas

Además de en el proceso de verificación, debería realizarse una comprobación del correcto funcionamiento de los sistemas de gestión de la información y su integración entre ellos y con los sistemas externos al laboratorio:

- cuando se implementa un análisis o comentario automatizado nuevo.
- periódicamente, independientemente de que no se haya producido ningún cambio en ellos.

6. Planes de contingencia

Debería disponerse de planes de contingencia documentados para mantener los servicios en caso de un fallo o interrupción de los sistemas de información (tanto si se trata de interrupciones programadas como imprevistas) que afecten a la capacidad del laboratorio para proporcionar sus servicios.

Estos planes de contingencia deberían asegurar que se mantiene la confidencialidad e integridad de los datos ante cualquier incidente en los sistemas de información.

7. Copias de seguridad e integridad de datos

El laboratorio es responsable de asegurar la integridad de los datos e información contenida en los sistemas de información. Para ello debería estar documentada la sistemática de copias de seguridad incluyendo las responsabilidades, y comprobar periódicamente su cumplimiento.

Debería incluir no solo los datos incluidos en el SIL sino también en otros sistemas de información, como los relacionados con los analizadores, más aún en el caso de no estar conectados con el SIL.

8. Subcontratación a proveedores externos

En caso de que los sistemas de gestión de la información sean gestionados por un proveedor externo, incluida la realización de copias de seguridad, el laboratorio es responsable de asegurar y demostrar que también éste cumple con los requisitos aplicables de la norma.

Legislación

• Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

• Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

ANEXO III: INTEGRIDAD DE DATOS: UNE-EN ISO/IEC 17020

Se detallan a continuación la aplicación de esas buenas prácticas a los apartados específicos de la norma UNE-EN ISO/IEC 17020, en los que los datos, documentos o registros a los que se hace referencia requieren una garantía de su integridad, en los términos que se establecen en el apartado 2.1 de esta guía.

Los aspectos desarrollados a continuación son aplicables de igual forma a las actividades de inspección que realizan las entidades.

NOTA: En este documento se utiliza el término "debe" cuando se refiere a un requisito incluido en la norma UNE-EN ISO/IEC 17020.

1. Organización y personal

UNE-EN ISO/IEC 17020:2012: apartados 5.2.3 y 6.1

Responsabilidades

En caso de que se disponga de sistemas informáticos que intervengan en los resultados o actividades de inspección, la entidad debería definir y documentar las responsabilidades del personal sobre la gestión de estos sistemas. Las responsabilidades establecidas deberían ir dirigidas, en todo caso, a garantizar la integridad de los datos.

Formación

En aquellos casos en los que los registros de formación, supervisión, etc. y documentación relacionada se encuentren en soporte electrónico, la entidad debería establecer mecanismos de seguridad que limitaran el acceso a esta información del personal. Por ejemplo: dar acceso a la información sólo a los responsables.

El organismo de inspección debería asegurar que el personal usuario de los sistemas informáticos empleados cuenta con la formación necesaria pasa su uso de forma apropiada y segura.

2. Instalaciones y equipos

UNE-EN ISO/IEC 17020: apartados 6.2.1, 6.2.2, 6.2.3, 6.2.5 y 6.2.11 c.

Equipos

Se debería disponer de un listado o inventario de los sistemas informáticos y equipos de generación de datos disponibles para poder determinar fácilmente si cada uno dispone de los elementos de control, seguridad y procedimiento de mantenimiento y uso necesarios.

Cuando la Entidad utiliza equipamiento que no es de su propiedad, también debe asegurar la integridad de datos que son generados por estos equipos.

Los equipos, instrumentos, sistemas automáticos o automatizados que generan datos deben disponer de registros de su verificación o validación y mantenimiento, así como las incidencias que se puedan producir. Cualquier cambio relevante en un equipo informático (hardware o software) debe validarse o verificarse para asegurar que no tiene impacto en los elementos de control y seguridad que garantizan la integridad de los datos manejados por el equipo.

Condiciones ambientales

Algunos de los sistemas más habituales empleados por las Entidades cuando es necesario monitorizar y controlar las condiciones ambientales, son:

- Sistemas de monitorización ambiental (SCADA) que registran y almacenan los datos ambientales y tienen capacidad de emitir gráficos e informes. En estos sistemas es importante garantizar la seguridad de los datos primarios: ubicación, acceso, copias de seguridad.

- Dispositivos móviles que registran las condiciones ambientales (p.ej. Data Loggers), cuyos datos son descargados en un PC, siendo revisados posteriormente por personal de la Entidad. En este caso es importante limitar el riesgo de manipulación de los datos, para lo cual debería establecerse un sistema controlado, con responsabilidades claras, del proceso de descarga y archivo de datos.

3. Procesos de la entidad de inspección

UNE-EN ISO/IEC 17020: apartados 7.1, 7.2, 7.3, 7.4 y 8.4

1. Tratamiento de los ítems de inspección y muestras:

La identificación de los ítems y muestras a inspeccionar es esencial para garantizar la trazabilidad y evitar errores. En el caso de que la entidad de inspección genere su propio sistema de identificación por sistemas informáticos, estos deberían estar controlados, protegidos y ser únicamente accesibles al personal autorizado.

2. Registros de inspección:

El cumplimiento de las buenas prácticas recogidas en el apartado 2 de este documento para los datos y metadatos permiten asegurar que los registros técnicos de cada una de las actividades son fiables e íntegros. Los datos dinámicos (los que permiten reproducir el resultado de la medición, a partir del dato primario) deben también conservarse.

Además, en caso de que estos registros sean electrónicos, el sistema debe permitir trazar automáticamente el usuario que lo generó/modificó y fecha-hora de cada registro.

Las modificaciones sobre los registros de inspección deben ser trazables a versiones anteriores u observaciones originales y para ello se han de conservar tanto los registros originales como las modificaciones. En el caso de que éstos sean electrónicos, el sistema informático debe disponer de sistemas de control para garantizar esta trazabilidad (p.ej. la herramienta Audit Trail).

5. Informes y certificados de inspección:

La integridad de los datos contenidos en un informe de resultados debe garantizarse mediante revisión frente a los originales o, en caso de que el informe proceda de un sistema informático, validar la coherencia y exactitud de los datos contenidos en el informe y los datos electrónicos originales del sistema.

En aquellos casos en los que las entidades de inspección transmiten de forma electrónica los resultados, se deben adoptar medidas de seguridad proporcionales a los riesgos asociados a la criticidad de la información que va a reportar, y tener en cuenta, en su caso, las recomendaciones o exigencias de sus clientes.

La firma o aprobación por personal autorizado debería hacerse mediante una firma electrónica legalmente válida.

Los cambios, correcciones o nuevas emisiones de un informe de resultados, deben quedar trazados mediante controles adecuados de las versiones del sistema de gestión documental o por alguna funcionalidad disponible en el sistema informático (p.ej. Audit Trail).

4. Control de los datos y sistemas de gestión de la información

UNE-EN ISO/IEC 17020: apartados 6.2.13 y 7.1.8

- Sistema de gestión de la información (en adelante "sistema"):

  El software comercial de uso general en el campo de aplicación para el cual fue diseñado se puede considerar que está suficientemente validado. Esto es únicamente aplicable al software comercial que no es personalizado. En caso contrario debe validarse.

  Los "sistemas" que incluyen fórmulas deben estar protegidas ante modificaciones indebidas.

- Validación del "sistema": Todo proceso de validación debería disponer de:

  1) Preparación, contemplando:
     - Requisitos de usuario documentados que definan cual es el propósito del "sistema" y qué funciones debe realizar.
     - Documentación adecuada (especificaciones, manuales, etc. en caso de softwares no desarrollados por la entidad) y procedimientos que garanticen que el "sistema" se utilizará y mantendrá de la manera prevista para garantizar/preservar la integridad de los datos.
     - Un protocolo o plan de validación que establezca las comprobaciones y pruebas a realizar: de instalación, de integridad de la información, de accesos, funcionales, etc. describiendo, paso a paso, cómo se hacen las pruebas y qué se pretende con cada una, y que contemple resultados esperados o criterios de aceptación de las pruebas.

2) Comprobación del "sistema", que debería incluir, en función del tipo de sistema a validar:

   - En caso de "sistemas" no desarrollados por la entidad, comprobaciones en cuanto a la instalación del "sistema", de modo que se demuestre que se lleva a cabo según las recomendaciones del suministrador y se configura conforme a los requisitos de usuario.
   - Comprobación del uso, de modo que se garantice la integridad de los datos.
   - Pruebas para demostrar que funciona según se espera, que deberían incluir las funciones que se van a utilizar, tales como una entrada de datos, un cálculo (que se podrá comparar mediante su realización por un método independiente), la comparación de los datos impresos en un informe con los que se ven en pantalla, casos que pudieran poner en riesgo el funcionamiento del "sistema" por su criticidad (por ejemplo, valores extremos en cálculos), etc.
   - Pruebas de seguridad que demuestren que sólo los usuarios autorizados acceden al "sistema" mediante combinaciones de usuario y contraseña, así como a las funciones y datos que son de su responsabilidad y están autorizados.
   - Si hay interfaces entre "sistemas" y transferencia de datos, pruebas que demuestren el correcto funcionamiento de estas.

3) Obtención de los resultados, con una declaración de si se cumplen los resultados esperados o los criterios de aceptación establecidos.

   La entidad debe mantener registros de la validación que permitan demostrar que el "sistema" es apto para el uso previsto.

   Los cambios realizados sobre un "sistema validado" y en uso deben documentarse, validarse y autorizarse antes de su introducción. Esta nueva validación debería extenderse también a otras funcionalidades que pudieran haberse visto afectadas por dicho cambio

   Cuando el sistema es gestionado o mantenido por un proveedor externo, la entidad es responsable de asegurar y demostrar que también éste cumple con los requisitos aplicables de la norma.