Validación de sistemas informatizados en laboratorios de control farmacéuticos

M. Garrote Gallego
CTO de Oqotech S.L.

La validación de sistemas informatizados tiene como principal objetivo aportar las evidencias documentales que aseguren que el sistema informatizado funciona de acuerdo a su uso previsto, previamente determinado y aprobado por la organización. A lo largo del presente artículo revisaremos aspectos clave a la hora de definir el personal involucrado en el proyecto, enfoque de la validación y actividades a realizar.

Palabras clave: Cumplimiento GxP, Anexo11 GMP, GAMP5, 21 CFR Part11, GDP, Cualificación

Main objective of computerized systems validation is to provide documented evidence to ensure that system operates according to its intended use previously established and approved by the organization. In this article, we will review key aspects like defining the personnel involved in the project, validation approach and activities to be performed.

Keywords: Compliance GxP, Annex11 GMP, GAMP5, 21 CFR Part11, GDP, Qualification

INTRODUCCIÓN

En la actualidad, la mayoría de los equipos que se utilizan en laboratorios de control de medicamentos se apoyan en soluciones informatizadas integradas en el propio dispositivo o conectadas a los mismos para la obtención de resultados o el procesamiento de los datos generados.

Si el sistema informatizado interviene en actividades reguladas por las GxP deben ser validados. Pero, ¿debemos poner el foco en el sistema informatizado o en el proceso que debe gestionar? Es vital huir del concepto tradicional de cualificación de equipos y sistemas informatizados de forma separada o poco integrada. Se deben identificar los componentes que van a aportar la operación, seguridad, ingeniería o tecnología que en conjunto van a gestionar el proceso y verificar que todos ellos, de forma integrada, operan según el uso previsto.

La metodología que se expone a continuación nace de la experiencia y proyectos desarrollados en Oqotech.

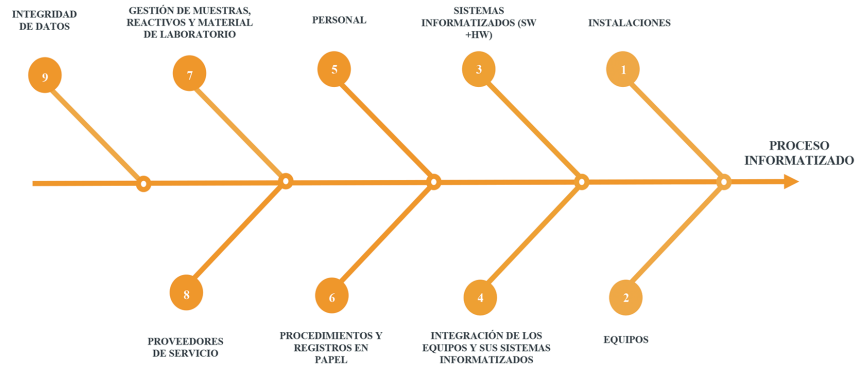
RIESGOS ASOCIADOS A LOS PROCESOS INFORMATIZADOS

Para elaborar la metodología a desarrollar en el proyecto de validación, inicialmente se debe realizar el

ejercicio de identificar los factores que pueden afectar a su correcto funcionamiento.

En la Figura 1 se muestra un análisis de riesgos, en forma de espina de pez, que identifica los factores principales a controlar en el proyecto de validación.

FIGURA 1. Espina de pez que analiza los riesgos asociados a los procesos informatizados en laboratorios de control farmacéuticos



ESTRATEGIA DE LA VALIDACIÓN DE SISTEMAS INFORMATIZADOS

La validación de sistemas informatizados es parte del sistema de calidad de la organización y permite seguir las fases de selección, implantación, uso y retirada de los sistemas informatizados. Debe quedar reflejada, en un plan maestro de validación, la estrategia global a seguir por parte de todos los equipos y sistemas informatizados de la organización.

Con el fin de establecer controles y aplicar verificaciones a todos los posibles tipos de riesgos del proceso informatizado, debe formarse un equipo de validación que cuente con especialistas que aporten experiencia y conocimiento en las diferentes áreas de la empresa. Los roles que deben quedar representados en el equipo de validación son: los especialistas de los procesos a informatizar, responsables del sistema de calidad, responsables de los sistemas informatizados y de la infraestructura informática.

La estrategia de validación debe ser aplicable a todos los equipos y sistemas informatizados presentes en la organización, con la dificultad de que todos los sistemas informatizados no tienen la misma complejidad, naturaleza o madurez dentro de la organización o en el sector. La validación, por tanto, debe tener un enfoque basado en el riesgo para establecer la estrategia y extensión de la validación aplicable a cada sistema informatizado.

Cabe destacar la siguiente clasificación de sistemas informatizados según GAMP5:

- **Categoría 1, software de infraestructura**: hace referencia a software de bajo nivel como son los lenguajes de programación, sistemas operativos o bases de datos.
- **Categoría 3, software no configurado**: hace referencia a sistemas que no requieren configuración para ejecutar el proceso para los que fueron diseñados. Un ejemplo podría ser una impresora de etiquetas, balanzas no integradas con ningún software o pH metros.
- **Categoría 4, software configurado**: hace referencia a sistemas más o menos complejos que, a través de su configuración, pueden adaptarse al proceso a ejecutar en la organización. Un ejemplo de categoría puede ser un HPLC o espectrofotómetros.
- **Categoría 5, software hecho a medida**: hace referencia a software hecho a medida para la organización de forma parcial o total.

Aplicado a sistemas informatizados utilizados en laboratorios de control se podría realizar la siguiente clasificación según su complejidad:

- **Sistemas simples**: sistemas no configurados (categoría 3 GAMP5) que generan valores basados en su *firmware*.
- **Sistemas de complejidad media**: compuestos por uno o varios componentes configurables (categoría 4 GAMP5), los cuales generan valores basados en su *firmware* y su software con una mínima configuración.
- **Sistemas complejos**: compuestos por múltiples componentes configurables o hechos a medida que operan en red.

Conforme se incrementa la categoría GAMP5 o la complejidad de los sistemas, la extensión de la validación aumenta.

El proyecto de validación se divide principalmente en cuatro etapas:

- Definición de los equipos y sistemas informatizados presentes en la organización.
- Proyecto de validación para los equipos y sistemas críticos.
- Mantenimiento del estado de control.
- Retirada y migración de sistemas.

DEFINICIÓN COMPLETA DE SISTEMA INFORMATIZADO

La organización debe disponer en todo momento de información actualizada de los equipos y sistemas informatizados que tiene en uso o en proceso de archivo (retirados, pero con información almacenada que debe mantener su integridad de datos un tiempo determinado). De esta forma, se podrá justificar que mantiene bajo control todos los procesos informatizados.

Para definir el sistema informatizado se contemplan dos tipos de detalle. El primero consistiría en una descripción completa del equipo,

centralizada en un inventario de sistemas, y el segundo en la definición de su mapa de procesos.

INVENTARIO DE EQUIPOS Y SISTEMAS INFORMATIZADOS

Todos los equipos existentes deben quedar identificados y detallados en un inventario global de la organización. Deben quedar reflejados los componentes industriales, hardware o software, información del sistema, proveedor de servicios, operación prevista y personal de la organización responsable de su instalación, uso, administración y mantenimiento. Esta información debe estar actualizada de manera permanente.

DIAGRAMA DEL EQUIPO Y SU SISTEMA INFORMATIZADO

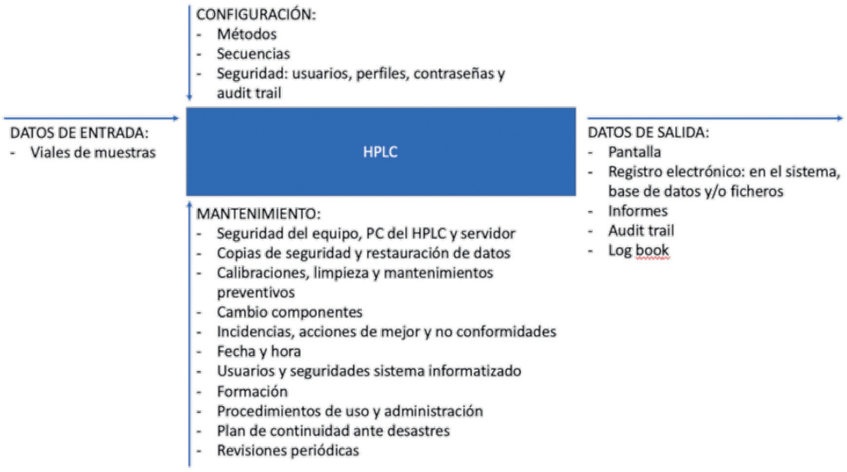
Asimismo, debe quedar plasmado el uso previsto del equipo y su sistema informatizado. Para realizar el diagrama se debe tener en cuenta el equipo y sistema como una caja negra, teniendo que determinar qué datos de entrada son requeridos para el proceso (pueden ser muestras, ficheros de otros sistemas informatizados, una señal de un equipo industrial, etc.), la configuración que se debe aplicar (pueden ser parámetros simples o secuencias que dispongan de condiciones específicas), el mantenimiento para asegurar la operación a lo largo del tiempo del equipo y sistema, y los datos de salida o resultados esperados.

En la Figura 2 se muestra un ejemplo de diagrama de un HPLC con un sistema informatizado asociado. El diagrama se debe acompañar de protocolos o documentación que amplíe la información de los puntos nombrados en el gráfico, por ejemplo, manuales de uso, administración, informes de calibración, etc.

PROYECTO DE VALIDACIÓN

A continuación, se presentan las principales tareas del proyecto de validación.

FIGURA 2. Definición del flujo de información, proceso y gestión del equipo y sistema informatizado



PLAN DE VALIDACIÓN POR SISTEMA INFORMATIZADO

El plan de validación tiene como principal objetivo definir y plasmar el procedimiento a seguir por todos los equipos y sistemas informatizados. Debe dejar definido los equipos y sistemas informatizados afectados, los procesos que serán analizados, los pasos a seguir en el proyecto acorde con la situación del equipo (diferenciando si el proceso de validación se realiza desde el inicio, adquiriendo el sistema informatizado, o si en el momento de la validación el equipo y sistema ya se encuentra en marcha), el personal de la organización participante y sus responsabilidades, objetivos y los criterios de aceptación para dar por liberado los sistemas analizados y cumplido el plan.

REQUERIMIENTOS DE USUARIO (URS)

Este informe define, de forma clara y precisa, lo que la compañía requiere del sistema informatizado, el denominado uso previsto. Se espera que los requerimientos de usuario sean específicos, medibles, realizables, realistas y testeables.

Deben ir asociados al proceso de negocio a gestionar y pueden ser utilizados para el proceso de selección del equipo y el sistema informatizado asociado.

ACUERDOS CON PROVEEDORES DE SERVICIO

La organización será responsable de todos los servicios subcontratados a un tercero. Por tanto, con el fin de asegurar la calidad del servicio por parte del proveedor, será necesario la firma de acuerdos.

La extensión del acuerdo dependerá de la criticidad de cada sistema informatizado y estrategia de colaboración con el proveedor. Siendo los puntos recomendados a concretar: descripción del servicio, roles y responsabilidades, sistemas de calidad, auditorías periódicas, documentación soporte, obligación de información y asesoramiento, plazos de ejecución, mantenimiento, propiedad de desarrollos y confidencialidad.

CUALIFICACIÓN DE LA INSTALACIÓN (IQ)

El objetivo final de la cualificación de la instalación es la verificación de las características, instalación y configuración del entorno final del equipo y del sistema informatizado.

Las principales tareas a realizar en esta etapa de proyecto son la definición del sistema (componentes industriales, hardware, software, estructura de comunicación y cableado), la ejecución de un análisis de riesgos para establecer la criticidad de cada componente, verificar la exis-

tencia de documentación tal como manuales de instalación y configuración, uso y administración del sistema o especificaciones técnicas, y, por último, la verificación, para componentes críticos, de la infraestructura informática e industrial respecto a los requisitos técnicos.

MATRIZ DE TRAZABILIDAD (MX)

Tomando como referencia los requerimientos de usuario aprobados, se generará una matriz que permitirá vincular toda la documentación asociada al proyecto de validación por requisito.

De esta forma, por cada equipo podremos asociar el código de requerimiento de usuario que informa su uso previsto, sus procedimientos de administración y uso, así como las cualificaciones requeridas por su categoría GAMP5.

PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNTS)

Deben quedar reflejadas, en los procedimientos normalizados de trabajo, las actividades de administración y uso por parte de los usuarios finales y gestores de la información generada o procesada.

Los procedimientos deben detallar la configuración requerida, su uso previsto y el registro que debe quedar del proceso.

CUALIFICACIÓN DEL DISEÑO (DQ)

Realizado el listado de requerimientos de usuario, instalado el equipo y sistema informatizado y documentado el proceso, es necesario verificar el cumplimiento de los requerimientos críticos para el proceso. Se debe aplicar un análisis de riesgos en caso de que se detecte alguna desviación o cambio del entorno informatizado final respecto a los requisitos iniciales. De esta forma se evaluará el impacto del cambio y se determinará si se debe aplicar alguna medida correctora.

El objetivo final de esta etapa es la verificación del diseño operativo, técnico y de seguridad del equipo y sistema informatizado implantado.

> Todo cambio que se produzca en el sistema informatizado debe pasar por un proceso de análisis, aprobación, implementación, documentación y seguimiento

CONTROL DE CAMBIOS

Todo cambio que se produzca en el sistema informatizado, tanto de componentes industriales, software o hardware, debe pasar por un proceso de análisis, aprobación, implementación, documentación y seguimiento.

Aspectos críticos a tener en cuenta en la valoración del impacto de un cambio son los siguientes: funcionalidades y documentación afectadas, verificaciones o formaciones a realizar y la afectación en la integridad de datos históricos.

CUALIFICACIÓN DE LA OPERACIÓN (OQ)

Establecidas las funcionalidades del equipo y sistema informatizado, es necesario evaluar su criticidad en el proceso desde un enfoque funcional, de seguridad, integridad de datos y cumplimiento de la normativa aplicable.

Tomando como referencia los procedimientos normalizados de trabajo se identifican los posibles fallos. A través del análisis de riesgos se establece la criticidad en caso de que el fallo sucediese. Las funcionalidades críticas seguirán un proceso de cualificación de la operación.

Se debe establecer un procedimiento de testeo estableciendo el personal involucrado y las tareas a llevar a cabo. Debe quedar evidente el objetivo del *test*: verificar el correcto funcionamiento de una operación determinada, analizando unos casos concretos, en un entorno determinado, con unos usuarios y simulando una situación específica. Asimismo, se determinarán los criterios de aceptación por paso del *test* y las evidencias a capturar en el proceso de testeo.

Al ejecutar el *test* debe quedar documentada la evidencia del resultado y, finalmente, adjuntar todos los resultados en un informe final de la cualificación de la operación.

GESTIÓN DE USUARIOS Y PERFILES DE SEGURIDAD

Se debe cumplir con la premisa, en la medida de lo posible, de que cada usuario del sistema disponga de su propio código de usuario y contraseña privada para autentificarse en los sistemas informatizados implantados en la empresa.

Cabe destacar la figura del administrador del sistema. El administrador debe disponer de una cuenta diferente a la cuenta de usuario de uso del sistema, preferiblemente deben asignarse como administradores a personas que no estén involucradas en el proceso y los cambios que apliquen como administrador deben ser documentados y aprobados.

De igual modo, debe quedar claramente concretado el acceso y tipo de permisos (visualización o modificación) por usuario y funcionalidad.

Se debe implantar un procedimiento que determine la metodología para la solicitud de altas de usuario, modificación de sus permisos e inactivación del usuario. Debe quedar registro de todas estas acciones, determinando el usuario que realiza la acción, el usuario afectado, la fecha y hora, el cambio realizado y el motivo de la acción en caso de modificación o baja.

PLAN DE FORMACIÓN

Establecidas las tareas a ejecutar por los diferentes miembros de la orga-

nización, se ponen de manifiesto las necesidades formativas de los usuarios en las funcionalidades que tienen asociadas.

Cabe destacar que es necesario reflejar en un acta la formación impartida, los usuarios asistentes, la fecha y tiempo de duración de la formación, y la documentación utilizada.

SEGURIDAD DE LA INFORMACIÓN

La gestión de los datos debe ser considerada como un proceso en sí mismo, no como algo subsidiario a cada proceso operativo.

Debe enfocarse a todo el ciclo de vida del dato, desde su generación pasando por su selección, representación, almacenaje, recuperación, distribución y uso; independientemente del formato o medio en el que hayan sido registrados, procesados, archivados o retirados.

Los sistemas informatizados que gestionan procesos considerados como críticos deben cumplir la regla ALCOA+.

CUALIFICACIÓN DEL PROCESO (PQ)

Una vez realizada la OQ, es necesario verificar de forma agrupada la gestión de un proceso para asegurar que el conjunto usuario, equipo, sistema y procedimientos permite la correcta ejecución y registro del proceso. Verificando asimismo la idoneidad de procedimientos (de uso, administración y mantenimiento), así como la finalización de las fases anteriores de la validación sin desviaciones críticas.

INFORME DE ACEPTACIÓN Y LIBERACIÓN

Elaboración de un informe final de aceptación del sistema determinando el personal involucrado, metodología seguida, resultados obtenidos, procedimientos de mantenimiento del estado de control y el dictamen final.

MANTENIMIENTO DEL ESTADO DE CONTROL

Con el fin de mantener el entorno validado de forma permanente, es necesario determinar los procedimientos que quedarán implantados en la organización. Dichos procedimientos deben reflejar las actividades, responsables y tiempos de ejecución.

Cabe destacar los siguientes procedimientos de gestión: control de cambios, gestión de usuarios y seguridades, plan de formación, procedimiento de seguridad física y lógica, política de copias de seguridad y restauración de datos y plan de contingencia.

Asimismo, en esta etapa del proyecto se establece la metodología a llevar a cabo en el proceso de revisión periódica de la validación. Se establecen los procedimientos de auditoría interna de la validación, proveedores de servicio e integridad de datos que permitan mantener el estado de control a lo largo del tiempo.

RETIRADA

La retirada de un sistema informatizado se debe realizar de forma planificada. Debe quedar descrito el entorno informático final, los procedimientos de uso, características técnicas del servidor, plan de copias de seguridad y la definición de permisos de seguridad para, a partir de la retirada del sistema, asegurar que únicamente es posible consultar información en el sistema.

Deben quedar incluidos los sistemas retirados en las auditorías internas periódicas durante su tiempo de archivo y en todos los procedimientos de mantenimiento del entorno de control.

CONCLUSIONES

- Es de vital importancia que el objetivo de la validación sea asegurar el proceso a gestionar de manera informatizada. Y ser conscientes de que este proceso es el conjunto de la operación de varios componentes industriales, hardware y software.

- Debemos tener en cuenta la integridad de los datos en todo su ciclo de vida.

- La validación se debe realizar por un equipo de validación en el que estén presentes especialistas en el proceso a gestionar, en la normativa a cumplir y en los sistemas informatizados a gestionar.

BIBLIOGRAFÍA

[1] ISPE, "GAMP5, "A Risk-Based Approach to Compliant GxP Computerized Systems". 2008.

[2] ISPE, GAMP Good Practice Guide, "A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems". 2012.

[3] ISPE, GAMP Good Practice Guide, "A Risk-Based Approach to Testing of GxP Systems". 2012.

[4] ISPE, GAMP Good Practice Guide, "Records & Data Integrity". 2017.

[5] AEMPS, "Guía de Normas de Correcta Fabricación de la Unión Europea, Medicamentos de uso humano y uso veterinario. Anexo 11 (sistemas informatizados)". 2011.

[6] AEMPS, "Guía de Normas de Correcta Fabricación de la Unión Europea, Medicamentos de uso humano y uso veterinario. Capítulo 1, (Sistema de Calidad Farmacéutico)". 2011.

[7] AEMPS, "Guía de Normas de Correcta Fabricación de la Unión Europea, Medicamentos de uso humano y uso veterinario. Anexo 15 (cualificación y validación)". 2015.

[8] AEMPS, "Guía de Normas de Correcta Fabricación de la Unión Europea, Medicamentos de uso humano y uso veterinario. Capítulo 4 (documentación)". 2011.

[9] ISO, "UNE-EN ISO 17025:2017, Requisitos generales para la competencia de los laboratorios de ensayo y de calibración". 2017.

[10] AEMPS, "Garantía de calidad y buenas prácticas de laboratorio". 2001.

[11] AEMPS, "Guía para la preparación de informes de inspección de buenas prácticas de laboratorio". 2001.

[12] FDA, "21 CFR Part 11". 2003.

[13] EMA/CHMP/ICH, "ICH guideline Q9 on quality risk management". 2015.

[14] ISO, "ISO 27001, Sistemas de gestión de la seguridad de la información.". 2014.

[15] PIC/S, "Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments.". 2016.

[16] FDA, "Data Integrity and Compliance with cGMP. Guidance for Industry". 2016.

[17] MHRA, "GxP Data Integrity Guidance and Definitions". 2018.

[18] ISO, "UNE-EN ISO 9001:2015 Sistemas de gestión de calidad. Requisitos.". 2015.

[19] WHO, "Annex 5, Guidance on Good Data and Record Management Practices". 2016.