LOS RETOS DE LA VALIDACIÓN DE SISTEMAS INFORMATIZADOS EN ENTORNOS ATMP: DEL CUMPLIMIENTO DOCUMENTAL A UN ENFOQUE BASADO EN RIESGO

La fabricación de medicamentos de terapia avanzada (ATMP, Advanced Therapy Medicinal Products) representa uno de los ámbitos más complejos de la industria farmacéutica. Con la complejidad de los procesos se añade la alta regulación del entorno donde los sistemas informatizados no quedan atrás, y deben sumarse al carro de las Normas de Correcta Fabricación.

LIMS, sistemas de monitorización ambiental, software asociado a equipos de qPCR o citometría de flujo, aplicaciones de gestión documental, ERP, sistemas de trazabilidad o incluso hojas de cálculo pueden generar, procesar o almacenar información directamente relacionada con la calidad del medicamento.

En este contexto surge una pregunta fundamental: **¿hasta dónde debe llegar la validación de estos sistemas?**

La respuesta pasa por abandonar un modelo centrado exclusivamente en generar documentación y adoptar una estrategia proporcional al riesgo que cada sistema representa para el paciente, el producto y la integridad de los datos.

Un marco regulatorio con diferentes piezas

En Europa, las Normas de Correcta Fabricación específicas de los medicamentos de terapia avanzada se encuentran recogidas en la Parte IV de EudraLex Volumen 4. A su vez, el Anexo 11 establece los principios aplicables a los sistemas informatizados utilizados en actividades GMP.

GAMP 5 (*Good Automated Manufacturing Practice*), actualmente en su segunda edición, proporciona un marco metodológico para llevar estos principios a la práctica, apoyándose en el ciclo de vida del sistema, el conocimiento del proceso, el pensamiento crítico y la gestión de riesgos. Su enfoque se articula alrededor de tres elementos fundamentales: **seguridad del paciente, calidad del producto e integridad de los datos**.

Parte IV, Anexo 11, GAMP 5 y 21 CFR Part 11 no son, referencias equivalentes, pero conjuntamente permiten construir una estrategia sólida de aseguramiento de los sistemas informatizados.

Primer reto: identificar qué debe validarse

Uno de los primeros errores consiste en hablar exclusivamente de "validación de software". Un sistema informatizado incluye no sólo la aplicación, sino también su configuración, infraestructura, usuarios, procedimientos, datos, interfaces y entorno operativo.

Además, no todos los sistemas presentan el mismo impacto GxP.

Una aplicación utilizada únicamente para tareas administrativas no presenta el mismo riesgo que un software de qPCR empleado para obtener un resultado de control de calidad o que una hoja Excel que calcula automáticamente un resultado utilizado para determinar la conformidad de un lote.

Por ello, el punto de partida debería ser disponer de un inventario de sistemas y realizar una evaluación inicial de su impacto GxP.

La pregunta clave podría ser: **"¿Qué podría ocurrir si este sistema no funcionase correctamente?"**

Segundo reto: definir el uso previsto

Una validación comienza antes de ejecutar una IQ, OQ o PQ. La validación comienza con los requisitos de usuario (URS), el análisis de riesgos del sistema donde se delimiten las funcionalidades críticas.

Por ejemplo, indicar que "el sistema dispone de gestión de usuarios" aporta poca información. Resulta más útil establecer que el acceso debe estar restringido a usuarios autorizados, que deben existir perfiles diferenciados según las responsabilidades y que determinadas funciones críticas deben quedar limitadas a personal autorizado.

Las URS constituyen así el punto de partida para determinar posteriormente los riesgos, controles y pruebas necesarias.

Tercer reto: validar en función del riesgo

Uno de los principios esenciales de GAMP 5 es que **no todas las funcionalidades requieren la misma intensidad o profundidad de verificación.**

Esta aproximación permite concentrar los recursos de validación sobre las funciones cuyo fallo puede afectar realmente al paciente, a la calidad del producto o a la integridad de los datos.

Diez preguntas antes de validar un sistema informatizado en un entorno ATMP

Antes de comenzar a redactar protocolos y ejecutar pruebas, resulta útil responder a diez preguntas:

1. ¿Qué proceso GxP soporta el sistema?

Fabricación, control de calidad, monitorización ambiental, almacenamiento, liberación, trazabilidad, gestión documental, etc.

2. ¿Qué datos GxP genera, procesa, modifica, transfiere o almacena?

Debe conocerse el ciclo de vida completo del dato.

3. ¿Qué decisiones dependen de esos datos?

Especialmente cuando intervienen en la aceptación o rechazo de materiales, resultados analíticos o lotes.



4. ¿Qué podría ocurrir si el sistema proporciona un resultado incorrecto?

Esta pregunta conecta directamente la funcionalidad con el riesgo.

5. ¿Quién puede acceder y qué puede hacer cada usuario?

Usuarios individuales, perfiles, privilegios administrativos y segregación de funciones deben formar parte de la evaluación.

6. ¿Los datos pueden modificarse o eliminarse?

Y, si pueden modificarse: ¿queda registrado quién lo hizo, cuándo y qué cambió?

7. ¿Existe audit trail y es revisable?

Disponer de audit trail no es suficiente. Debe establecerse qué se revisa, quién lo hace y cuándo.

8. ¿Cómo se protegen y recuperan los datos?

No basta con realizar backups: debe poder demostrarse que los datos pueden restaurarse correctamente.

9. ¿Qué depende del proveedor y qué depende de la organización?

Mantenimiento, actualizaciones, administración, incidencias y responsabilidades deben estar claramente definidos.

10. ¿Cómo se mantendrá el sistema en estado validado?

Cambios, actualizaciones, incidencias y revisiones periódicas forman parte de la validación durante el ciclo de vida.

Responder adecuadamente a estas preguntas permite definir gran parte de la estrategia de validación antes incluso de redactar el primer protocolo.

Cuarto reto: garantizar la integridad de los datos

La integridad de datos constituye uno de los aspectos más críticos en los sistemas informatizados utilizados en entornos ATMP.

Garantizar los principios ALCOA+ implica evaluar, entre otros aspectos, usuarios individuales, perfiles de acceso, capacidad de modificar o eliminar información, audit trail,

sincronización temporal, conservación de metadatos y recuperación de la información.

Un ejemplo sencillo es la utilización de cuentas compartidas. Si varios analistas acceden al software de un equipo mediante un único usuario denominado "Laboratorio", puede resultar imposible determinar posteriormente quién realizó una modificación.

La cuestión no es únicamente si el resultado final es correcto, sino si puede demostrarse **quién generó el dato, cuándo lo hizo y qué ocurrió con él desde su generación hasta su utilización final.**

Lo mismo sucede con el audit trail. Su mera existencia no constituye un control suficiente. La organización debe determinar qué eventos son relevantes, quién debe revisarlos y con qué frecuencia, aplicando nuevamente un enfoque basado en riesgo.

Quinto reto: proveedores y equipos de laboratorio

Los entornos ATMP presentan una elevada dependencia de software incorporado a equipos analíticos y productivos. Es frecuente que el proveedor entregue documentación de cualificación o indique que el software se encuentra "validado", incluso con la documentación del equipo que lo porta.

Sin embargo, el proveedor puede aportar evidencias sobre el desarrollo y funcionamiento de su producto, pero no puede validar completamente **el uso concreto que cada organización hará de él.**

Un mismo software de qPCR puede utilizarse para una determinación cualitativa o para obtener resultados cuantitativos que condicionen la liberación de un lote. El software es el mismo; el riesgo GxP no.

Este principio también aplica a externalizar infraestructura, almacenamiento o mantenimiento no implica externalizar la responsabilidad GMP. Deben definirse las responsabilidades relacionadas con actualizaciones, backups, recuperación de información, incidencias, seguridad, disponibilidad y conservación de los datos.

Sexto reto: mantener el estado validado

Probablemente uno de los errores más frecuentes sea considerar que la validación termina con la aprobación del informe final de PQ.

Durante la vida del sistema aparecerán nuevos usuarios, incidencias, cambios de configuración, actualizaciones, nuevas versiones y modificaciones de infraestructura. Cada cambio deberá evaluarse para determinar su impacto sobre el estado validado.

No toda actualización requiere repetir la validación completa, pero todo cambio relevante debe ser evaluado.

De la documentación al aseguramiento del sistema

Durante años, la validación de sistemas informatizados se ha asociado casi automáticamente a IQ, OQ y PQ. Estas actividades continúan siendo útiles, pero no deberían convertirse en un fin en sí mismas.

Una prueba tiene valor cuando proporciona evidencia sobre un requisito o riesgo identificado.

Ejecutar numerosas pruebas de funciones de bajo impacto mientras no se verifica adecuadamente un algoritmo crítico, la restauración de un backup o los privilegios administrativos puede generar mucha documentación, pero poca garantía adicional.

En entornos ATMP, donde pueden coexistir tecnologías innovadoras, procesos altamente especializados y recursos limitados, este enfoque resulta especialmente relevante.

El objetivo no debe ser validar menos, sino **validar mejor.**

Esto implica identificar los sistemas con impacto GxP, definir su uso previsto, conocer los datos críticos, evaluar los riesgos y concentrar la verificación sobre aquellas funciones cuyo fallo pueda afectar al paciente, al producto o a la fiabilidad de los datos.

En definitiva, el éxito de una validación no debería medirse por el número de páginas de un protocolo ni por el número de evidencias obtenidas durante una OQ, sino mediante una pregunta mucho más sencilla:

¿Tenemos evidencia suficiente para confiar en que el sistema hará correctamente aquello que necesitamos que haga, podremos detectar cuándo algo no ha ocurrido como debía y podremos demostrarlo durante todo su ciclo de vida?

Ese es, en última instancia, el verdadero objetivo de la validación de sistemas informatizados.

Bibliografía

- 1.European Commission. EudraLex Volume 4. Part IV: Guidelines on Good Manufacturing Practice specific to Advanced Therapy Medicinal Products.
- 2. European Commission. EudraLex Volume 4. Annex 11: Computerised Systems.
- 3.ISPE. GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems. Second Edition. 2022.
- 4.U.S. Food and Drug Administration. 21 CFR Part 11 – Electronic Records; Electronic Signatures.
- 5.U.S. Food and Drug Administration. Part 11, Electronic Records; Electronic Signatures – Scope and Application.