# Guía de Buenas Prácticas de Fabricación de Medicamentos de Uso Humano

## ANEXO 6

## SISTEMAS INFORMATIZADOS

### Principio

Este anexo aplica a todas las formas de sistemas informatizados usados como parte de las actividades reguladas por las BPF.

Un sistema informatizado es un set de componentes de software y hardware que juntos satisfacen ciertas funcionalidades. La aplicación debe validarse; la infraestructura informatizada (IT) debe calificarse.

Cuando un sistema informatizado reemplace una operación manual, no debe ser en detrimento de la calidad del producto, control del proceso o garantía de calidad. No debe haber un incremento del riesgo total del proceso.

Las actividades relacionadas deberían seguir los lineamientos internacionales de *GAMP®5: A Risk-based Approach to Compliant GxP Computarized Systems* u otras similares actualizadas con requerimientos similares o superiores.

### General

### 1. Gestión de riesgos

**1.1** La gestión de riesgos debe aplicarse durante el ciclo de vida del sistema informatizado teniendo en cuenta la seguridad del paciente, la integridad de datos y la calidad del producto. Como parte del sistema de gestión de riesgos, las decisiones sobre la extensión de la validación y de los controles de la integridad de datos deben basarse en una evaluación de riesgos del sistema informatizado justificada y documentada.

### 2. Personal

**2.1** Debe existir una cooperación estrecha entre todo el personal relevante entre los que se encuentra el propietario del proceso (*process owner*), el propietario del sistema (*system owner*), las Personas Cualificadas e informática (IT). Todo el personal debe disponer de la cualificación apropiada, el nivel de acceso y tener definidas sus responsabilidades para llevar a cabo las tareas asignadas.

### 3. Proveedores y proveedores de servicios

**3.1.** Cuando se emplea a terceros (como proveedores, proveedores de servicios) por ejemplo para suministrar, instalar, configurar, integrar, validar, mantener (ej. vía acceso remoto), modificar o conservar un sistema informatizado o un servicio relacionado o para el procesado de datos, tienen que existir acuerdos formales entre el fabricante y tercero, y en estos acuerdos deben incluirse declaraciones claras sobre las responsabilidades del tercero. Los departamentos de informática (IT) deben considerarse análogamente.

**3.2.** La competencia y la fiabilidad del proveedor son factores claves a la hora de seleccionar un producto o proveedor de servicios. La necesidad de realizar una auditoría debe basarse en una evaluación de riesgos.

**3.3.** La documentación entregada con los productos comerciales (*commercial off-the-shelf*) debe revisarse por usuarios regulados para comprobar que los requerimientos de usuario se satisfacen.

**3.4.** El sistema de calidad y la información de auditorías relativas a los proveedores o desarrolladores del software y de los sistemas implantados deben estar disponibles a petición de los inspectores.

**Fase de proyecto**

**4. Validación**

**4.1.** La documentación de validación y los informes deben cubrir los pasos relevantes del ciclo de vida del sistema. Los fabricantes deben ser capaces de justificar sus estándares, protocolos, criterios de aceptación, procedimientos y registros basados en su evaluación de riesgos.

**4.2.** La documentación de validación debe incluir los registros de controles de cambio (si aplican) y los informes de cualquier desviación observada durante el proceso de validación.

**4.3.** Debe disponerse de una lista actualizada (inventario) de todos los sistemas relevantes y su funcionalidad en relación con las BPF. Para los sistemas críticos debe disponerse de una descripción actualizada detallando las disposiciones físicas y lógicas, los flujos de datos y las interfaces con otros sistemas o procesos, cualquier pre-requisito del hardware y del software, y las medidas de seguridad.

**4.4.** Las especificaciones de requerimientos de usuario deben describir las funciones requeridas del sistema informatizado y deben basarse en una evaluación de riesgos documentada y en su impacto en BPF. Los requerimientos de usuario deben trazarse a lo largo del ciclo de vida del sistema.

**4.5**. El usuario regulado debe tomar todas las precauciones que sean razonables para asegurar que el sistema se ha desarrollado de acuerdo con un sistema de apropiado de garantía de calidad. El proveedor debe evaluarse adecuadamente.

**4.6.** Para la validación de sistemas informatizados hechos a medida o personalizados debe existir un proceso que asegure la evaluación formal y la comunicación de las medidas de calidad y funcionales de todos los estados del ciclo de vida del sistema.

**4.7.** Debe demostrarse con evidencias que los métodos y los escenarios de test son adecuados. Particularmente, los límites de parámetros del sistema (para el proceso), límites de datos y el manejo de errores, deben considerarse. Las herramientas automáticas y los entornos de test deben tener evaluaciones documentadas de su idoneidad.

**4.8.** Si los datos se transfieren a otro formato de datos o sistema, la validación debe incluir comprobaciones de que los datos no se alteran en valor y/o en significado durante el proceso de migración.

**4.9** Si el sistema se adquiere como sistema cerrado (Paquetes de Software Estándar) ya validado por el proveedor, el usuario regulado debe realizar todos los desafíos relacionados con su

requerimiento de usuario y la validación en operación para demostrar que todas actividades manejadas por el sistema se realizan de forma segura, inviolable, confiable y traceable. Los desafíos deben ser realizados deben incluir las alarmas, desafíos de pasa y no pasa con usuarios autorizados y no autorizados para realizar una operación crítica GxP relevante

**Fase de operación**

**5. Datos**

Los sistemas informatizados que intercambian datos electrónicamente con otros sistemas deben incluir comprobaciones intrínsecas adecuadas de la entrada y el procesado correcto y seguro de datos, de cara a minimizar riesgos.

**6. Comprobaciones de exactitud**

Para la entrada manual de datos críticos, debe existir una comprobación adicional de la exactitud de los datos. Esta comprobación puede realizarse por un segundo operario o por medios electrónicos validados. La gestión de riesgos debe incluir la criticidad y las consecuencias potenciales de una entrada errónea o incorrecta de datos en el sistema.

**7. Archivo de datos**

**7.1.** Los datos deben asegurarse frente a daños tanto por medios físicos como electrónicos. Para el almacenaje de datos debe comprobarse la accesibilidad, la legibilidad y la exactitud. El acceso a los datos debe asegurarse durante el periodo de conservación de datos.

**7.2**. Debe realizarse regularmente copias de seguridad de todos los datos relevantes. La integridad y la exactitud de las copias de seguridad de datos y la capacidad de re-establecer los datos debe comprobarse durante la validación y controlarse periódicamente

**8. Impresiones**

**8.1.** Tiene que ser posible obtener copias impresas claras de los datos electrónicos almacenados.

**8.2.** Para los registros en los que se basa la liberación de lotes debe ser posible la generación de impresiones que pongan de manifiesto que un dato se ha cambiado respecto de la entrada original.

**9. Registro de auditoría *("Audit trail")***

Debe considerarse, en base a la gestión de riesgos, incorporar en el sistema la creación de un registro de todos los cambios y eliminaciones relevantes relacionados con BPF (un registro de auditoría generado por el sistema). Debe documentarse el motivo del cambio o de la eliminación de datos relevantes relacionados con BxP (buenas prácticas de almacenamiento, distribución, fabricación, control de calidad). El registro de auditoría tiene que estar disponible y en general, ser convertible en un formato inteligible así como revisarse regularmente.

**10. Gestión de cambios y configuración**

Cualquier cambio a un sistema informatizado incluyendo las configuraciones de sistema sólo debe realizarse de manera controlada de acuerdo con un procedimiento definido.

**11. Evaluación periódica**

Los sistemas informatizados deben evaluarse periódicamente para confirmar que se mantienen en un estado válido y que cumplen con las BPF. Estas evaluaciones deben incluir, cuando proceda, el alcance actual de funcionalidades, registros de desviaciones, incidentes, problemas, historial de actualizaciones, rendimiento del sistema, fiabilidad, seguridad e informes del estado de validación.

**12. Seguridad**

**12.1.** Deben incorporarse controles físicos y/o lógicos para restringir el acceso a los sistemas informatizados a personas autorizadas. Entre los métodos idóneos de prevención de accesos no autorizados se incluyen el uso de llaves, tarjetas de paso, códigos personales con contraseñas, métodos biométricos, acceso restringido a los equipos informáticos y a las áreas de almacenaje de datos.

**12.2.** La extensión de los controles de seguridad depende de la criticidad del sistema informatizado.

**12.3.** La creación, cambio y la cancelación de una autorización de acceso debe registrarse.

**12.4.** Los sistemas de gestión de datos y de documentos deben diseñarse para registrar la identidad de los operarios que entran, cambian, confirman o eliminan datos, incluyendo fecha y hora.

**13. Gestión de incidencias**

Todos los incidentes deben comunicarse y evaluarse, no solamente los fallos de sistema y los errores de datos. La causa raíz de un incidente crítico debe identificarse y constituir la base de las acciones correctivas y preventivas.

**14. Firma electrónica**

Los registros electrónicos pueden firmarse electrónicamente. Respecto de las firmas electrónicas se espera que:

a. tengan el mismo impacto que las firmas manuscritas en el ámbito de la compañía,

b. estén permanentemente ligadas al respectivo registro,

c. incluyan la hora y el día en el que se realizaron.

**15. Liberación de lotes**

Cuando se utiliza un sistema informatizado para registrar la certificación y liberación de lotes, el sistema sólo debe permitir a las Personas Cualificadas certificar la liberación de lotes y debe identificar claramente y registrar la persona que ha liberado o certificado los lotes. Esto debe realizarse usando una firma electrónica.

**16. Continuidad del negocio**

Deben tomarse medidas para asegurar la continuidad de los sistemas informatizados que soportan procesos críticos, en el caso de un colapso de los mismos (ej. tener un sistema alternativo o manual). El tiempo necesario para poner en uso los sistemas alternativos debe basarse en el riesgo y

ser apropiado para el sistema particular y para el proceso de negocio que soporta. Estas disposiciones deben documentarse y comprobarse adecuadamente.

**17. Archivo**

Los datos pueden archivarse. Debe comprobarse la accesibilidad, la legibilidad y la integridad de estos datos. Si se realizan cambios relevantes en el sistema (ej. en los equipos informáticos o programas), entonces la capacidad de recuperar los datos debe garantizarse y comprobarse.

**Glosario**

**Aplicación:** software instalado en una plataforma/hardware definido que proporciona una funcionalidad específica.

**Ciclo de vida:** todas las fases de la vida de un sistema desde los requerimientos iniciales hasta su retirada, incluyendo diseño, especificaciones, programación, testeo, instalación, operación y mantenimiento.

**Infraestructura informática (IT):** el hardware y el software tales como el software de red y el sistema operativo, los cuales hacen posible que función de la aplicación.

**Propietario del proceso (*process owner*):** la persona responsable del proceso de negocio.

**Propietario del sistema (*system owner*):** la persona responsable de la disponibilidad y el mantenimiento de un sistema informatizado y de la seguridad de los datos contenidos en el mismo.

**Sistema hecho a medida/personalizado (*Bespoke/customized computerised system*):** un sistema informatizado diseñado individualmente para encajar con un proceso de negocio específico.

**Software comercial (*commercial of the shelf software*):** software disponible comercialmente, cuya idoneidad para el uso está demostrada por un amplio espectro de usuarios.

**Terceros (*third party*):** grupos no directamente gestionados por el titular de la autorización de fabricación y/o importación.

**Usuario regulado:** Entidad, regulada por Buenas Prácticas, responsable de la operación de los sistemas informatizados y aplicaciones, archivos y datos contenidos en ellas. Se entiende pues como la entidad que ha adquirido un producto informático comercial y que debe asegurar el cumplimiento de BxP en su funcionamiento, uso al que se destina, archivo de la información así como en los datos contenidos en el mismo.