



Sistemas Informatizados

CURSO DE VALIDACIÓN DE SISTEMAS INFORMATIZADOS
E INTEGRIDAD DE DATOS EN ESTUDIOS CLÍNICOS

Mayte Garrote Gallego

CTO, Oqotech

in @Mayte Garrote Gallego

@ Índice

01.
 Entorno
Regulatorio

02.
 Retos y Riesgos
de los EECC

03.
 Fundamentos de la
Validación

04.
 Proyecto de
Validación

@ Entorno Regulatorio

Normativas y guías aplicables.

La Buena **Práctica Clínica (BPC)** engloba una serie de normas dirigidas a garantizar los **derechos de los sujetos** que participan en un ensayo clínico, asegurar la **calidad de los datos** y evitar **errores** en la investigación clínica.

AEMPS / BPC - <https://www.aemps.gob.es/industria-farmaceutica/buena-practica-clinica/>

- **CPMP/ICH/135/95, Normas de Buena Práctica Clínica (BPC)**. Se define como una norma internacional de calidad científica y ética dirigida al diseño, registro y redacción de informes de los ensayos clínicos en los que participan seres humanos. El cumplimiento de estas normas garantiza públicamente la protección de los derechos, seguridad y bienestar de los sujetos que participan en el estudio y asegura la integridad y credibilidad de los datos obtenidos en un ensayo clínico.
- **Directiva 2005/28/CE** que establece los principios y directrices detalladas de la BPC respecto a los medicamentos en investigación de uso humano, así como los requisitos para autorizar la fabricación o importación de dichos medicamentos (transpuesta en España mediante ORDEN SCO 256/2007 de 5 de febrero y su MODIFICACIÓN mediante la ORDEN SCO/362/2008, de 4 de febrero.

EMA - https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/reflection-paper-expectations-electronic-source-data-data-transcribed-electronic-data-collection_en.pdf

- **EMA/INS/GPC/454280**, GCP Inspectors Working Group (GCP IWG), Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials.
- **CDISC**, Clinical Data Interchange Standards Consortium.

@ Entorno Regulatorio

Normativas y guías aplicables.

AEMPS – <https://www.aemps.gob.es/industria-farmaceutica/guia-de-normas-de-correcta-fabricacion/>

- Anexo 11, Sistemas informatizados.
- Anexo 15, Cualificación y Validación.
- Capítulo 4, Documentación
- ICH guideline Q9 on quality risk management

FDA – <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11>

- 21 CFR Part 11, Electronic Records; Electronic Signatures — Scope and Application

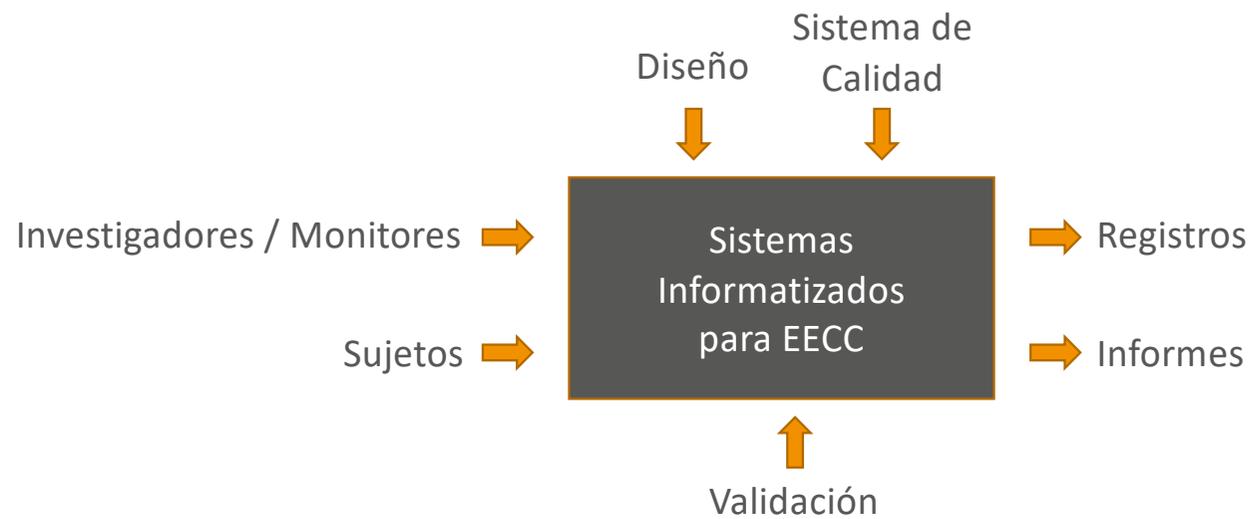
ISPE – <https://ispe.org>

- GAMP5, A Risk-Based Approach to Compliant GxP Computerized Systems.
- Good Practice Guide, A Risk-Based Approach to Testing of GxP Systems.
- Records and Data Integrity GUIDE
- Good Practice Guide. Data Integrity – Key Concepts

AENOR – <https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion>

- ISO 27001, Sistemas de gestión de la seguridad de la información.

@ Retos y Riesgos de los EECC



@ Retos y Riesgos de los EECC

REQ CAL 1	-	Requisitos de control y garantía de calidad
REQ CAL 1.1	BPC punto 2.5	Los ensayos clínicos deberán estar científicamente justificados y estar descritos en un protocolo claro y detallado.
REQ CAL 1.2	BPC punto 2.12	Los medicamentos en investigación deberán fabricarse, manejarse y almacenarse de acuerdo con las Normas de Correcta Fabricación (NCF) pertinentes y se deberán utilizar de acuerdo con el protocolo aprobado.
REQ CAL 1.3	BPC punto 2.13	Se implantarán sistemas con procedimientos que aseguren la calidad de cada aspecto del ensayo.
REQ CAL 1.4	BPC punto 5.1.1	El promotor es el responsable de poner en marcha y mantener un sistema de control y garantía de calidad con procedimientos normalizados de trabajo (PNT) escritos a fin de asegurar que los ensayos sean realizados y los datos sean generados, documentados (registrados) y comunicados de acuerdo con el protocolo, la BPC y la normativa vigente.
REQ CAL 1.5	BPC punto 5.1.2	El promotor es el responsable de llegar a un acuerdo con todas las partes implicadas que asegure el acceso directo (véase 1.2.1) a todos los centros del ensayo, a todos los datos/documentos originales y los informes necesarios para garantizar la monitorización y auditoría por parte del promotor y las inspecciones por parte de las autoridades nacionales y extranjeras.
REQ CAL 1.6	BPC punto 5.1.3	Se deberá aplicar un control de calidad en cada fase del manejo de datos para asegurar que todos ellos son fiables y que han sido procesados de forma correcta.
REQ CAL 1.7	BPC punto 5.2.1	Un promotor puede transferir alguna o todas las obligaciones y funciones relacionadas con el ensayo a una CRO, pero la última responsabilidad sobre la calidad e integridad de los datos del ensayo siempre recae en el promotor . La CRO deberá implementar la garantía y el control de calidad.

@ Retos y Riesgos de los EECC

REQ REG 1	-	Requisitos para los registros electrónicos
REQ REG 1.2	BPC punto 2.11	Se deberá proteger la confidencialidad de los registros que pudieran identificar a los sujetos respetando la privacidad y las normas de confidencialidad de acuerdo con los requisitos legislativos pertinentes.
REQ REG 1.3	BPC punto 4.6.3	El investigador/institución y/o un farmacéutico u otro individuo apropiado, que haya sido designado por el investigador/institución, deberá mantener un registro del envío del medicamento al centro del ensayo , el inventario, el uso por parte de cada sujeto y la devolución al promotor o eliminación alternativa del preparado no utilizado. Estos registros deberán incluir la fecha, cantidad, número de lote/serie, fecha de caducidad (cuando proceda) y código asignado al medicamento en investigación y a los sujetos del ensayo . Los investigadores deberán mantener registros que documenten correctamente que a los sujetos se les suministraron las dosis especificadas en el protocolo y que los datos cuadren con los medicamentos en investigación recibidos del promotor.
REQ REG 1.4	BPC punto 4.9.1	El investigador deberá garantizar la exactitud, integridad, legibilidad y puntualidad en la presentación de los datos al promotor en el plazo de tiempo convenido así como de todos los informes que se le requieran.
REQ REG 1.5	BPC punto 4.9.2	Los datos incluidos en el CRD , que se deriven de documentos fuente, deberán ser consistentes con dichos documentos o en caso contrario justificar las discrepancias .
REQ REG 1.6	BPC punto 4.9.3	Cualquier modificación o corrección de los datos del CRD deberá ser rechado, firmado con las iniciales y explicado (si es necesario) y no deberá ocultar los datos originales (es decir, se deberá mantener un "audit trail") . Esto es aplicable tanto a los cambios o las correcciones en papel como en soporte electrónico. Los promotores facilitarán a los investigadores y a los representantes designados por los investigadores, una guía sobre cómo hacer tales correcciones. Los promotores deberán tener procedimientos escritos que garanticen que los cambios o las correcciones realizados en los CRD por los representantes designados por el promotor están documentados, son necesarios y están confirmados por el investigador. El investigador deberá conservar los registros de los cambios y las correcciones.
REQ REG 1.7	BPC punto 4.9.4	El investigador/institución deberán guardar los documentos del ensayo tal como está especificado en el apartado de Documentos Esenciales para la realización de un Ensayo Clínico. El investigador/la institución deberá tomar las medidas necesarias para prevenir la destrucción accidental o prematura de estos documentos
REQ REG 1.8	BPC punto 4.9.5	Se deberán conservar los documentos esenciales hasta al menos 2 años después de la última aprobación de una solicitud de comercialización en Europa, EEUU o Japón y hasta que no quede ninguna solicitud de comercialización pendiente, o en proyecto, en dichas regiones o hasta que hayan pasado al menos 2 años desde la suspensión formal del desarrollo clínico del medicamento en investigación . Sin embargo, se deberán conservar estos documentos durante un periodo de tiempo más prolongado si así lo establecen las normas reguladoras aplicables o un acuerdo con el promotor. Es responsabilidad del promotor informar al investigador/institución a partir de qué fecha no es necesario conservar estos documentos.
REQ REG 1.9	BPC punto 4.9.7	Ante la solicitud del monitor, auditor, CEIC o autoridad sanitaria, el investigador/institución deberá ser capaz de tener disponibles todos los archivos relacionados con el ensayo.

@ Retos y Riesgos de los EECC

REQ SI 1	-	Requisitos para los sistemas informatizados
REQ SI 1.2	BPC punto 5.5.1	El promotor se deberá valer de personas debidamente calificadas para supervisar la realización global del ensayo, manejar y verificar los datos, realizar los análisis estadísticos y preparar los informes del ensayo.
REQ SI 1.3	BPC punto 5.5.3 (a)	Asegurar y documentar que el sistema de procesamiento de datos electrónicos se ajusta a los requisitos establecidos por el promotor en cuanto a la integridad, exactitud, fiabilidad y consistencia del proceso (es decir, validación)
REQ SI 1.4	BPC punto 5.5.3 (b)	Elaborar y actualizar el PNT para la utilización de estos sistemas.
REQ SI 1.5	BPC punto 5.5.3 (c)	Garantizar que el diseño de los sistemas permite la modificación de datos de tal manera que estos cambios queden documentados y que los datos originales no sean eliminados (es decir, mantener un método de seguimiento retrospectivo " audit trail ", seguimiento retrospectivo de los datos " data trail ", o seguimiento retrospectivo de los cambios " edit trail ").
REQ SI 1.6	BPC punto 5.5.3 (d)	Mantener un sistema de seguridad que impida el acceso no autorizado a los datos.
REQ SI 1.7	BPC punto 5.5.3 (e)	Elaborar y actualizar una lista de las personas que están autorizadas a hacer cambios en los datos.
REQ SI 1.8	BPC punto 5.5.3 (f)	Crear copias de seguridad de los datos.
REQ SI 1.9	BPC punto 5.5.3 (f)	Salvaguardar el enmascaramiento , si lo hay (p.e mantener el enmascaramiento de los datos durante la entrada y procesamiento de los mismos).
REQ SI 1.10	BPC punto 5.5.4	Si se modifican los datos durante su procesamiento , siempre deberá ser posible comparar los datos originales y las observaciones con los datos procesados .
REQ SI 1.11	BPC punto 5.5.5	El promotor deberá utilizar un código de identificación de los sujetos que no sea ambiguo que permita la identificación de todos los datos registrados para cada sujeto.
REQ SI 1.12	BPC punto 5.5.6	El promotor, u otros propietarios de los datos, conservarán todos los documentos esenciales específicos del promotor, que pertenezcan al ensayo.
REQ SI 1.13	BPC punto 5.5.7	El promotor conservará todos sus documentos esenciales específicos de acuerdo con la normativa pertinente de los países donde el medicamento esté aprobado y/o donde el promotor pretenda solicitar su aprobación.
REQ SI 1.14	BPC punto 5.5.8	Si el promotor interrumpe el desarrollo clínico de un medicamento en investigación (es decir, para alguna o todas las indicaciones, vías de administración o forma farmacéutica) el promotor deberá mantener todos los documentos esenciales específicos del promotor durante por lo menos 2 años después de la interrupción formal o de acuerdo con la normativa vigente de cada país.
REQ SI 1.15	BPC punto 5.5.11	Se deberán conservar los documentos esenciales específicos del promotor hasta al menos dos años después de la última aprobación de comercialización en una región ICH, y hasta que no haya solicitudes de comercialización pendientes ni en proyecto en una región ICH; o hasta que hayan pasado al menos 2 años desde la interrupción formal del desarrollo clínico del medicamento en investigación. Sin embargo, se deberán guardar estos documentos durante un periodo de tiempo mayor si así lo requieren los requisitos legales pertinentes o si lo necesita el promotor.

@ Retos y Riesgos de los EECC

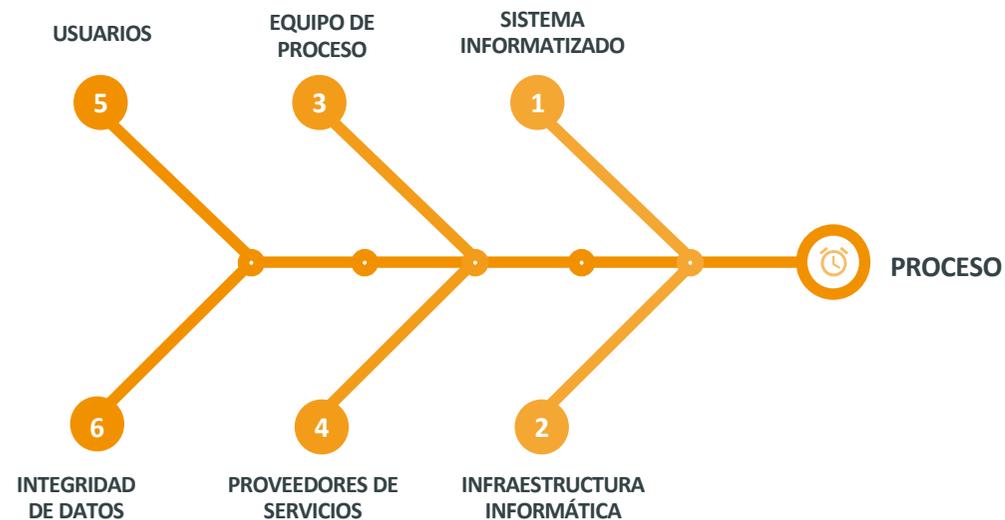
REQ MON 1	-	Requisitos del monitor
REQ MON 1.2	BPC punto 5.18.4 (f)	Garantizar que el investigador recibe el Manual del Investigador actualizado, todos los documentos y todos los suministros necesarios del ensayo para que lo realice de forma adecuada y de acuerdo con los requisitos legales pertinentes.
REQ MON 1.3	BPC punto 5.18.4 (k)	Verificar que los documentos fuente y los demás registros del ensayo son precisos, completos, actualizados y están correctamente archivados.
REQ MON 1.4	BPC punto 5.18.4 (m)	Verificar la exactitud e integridad de los datos incluidos en el CRD , con respecto a los documentos fuente y otros registros relacionados con el ensayo. El monitor específicamente verificará que: i) Los datos requeridos en el protocolo están anotados con exactitud en los CRD y concuerdan con los datos fuente. ii) Todas las dosis y/o cualquier modificación del tratamiento están bien documentadas para cada uno de los sujetos del ensayo. iii) Los acontecimientos adversos, tratamientos concomitantes y enfermedades intercurrentes se notifican de acuerdo con el protocolo en los CRD. iv) Las visitas, pruebas y exploraciones que los sujetos no hayan realizado constan claramente como tales en los CRD. v) Todas las retiradas y abandonos de los sujetos incluidos en el ensayo constan y están justificadas en los CRD.
REQ MON 1.5	BPC punto 5.18.4 (n)	Informar al investigador de cualquier error, omisión o ilegibilidad en los registros del CRD. El monitor deberá asegurarse de que se han hecho las correcciones, adiciones o supresiones apropiadas y que constan la fecha, justificación (en caso necesario) e iniciales del investigador o de un miembro del personal del ensayo debidamente autorizado para realizar cambios en el CRD en nombre del investigador. Esta autorización deberá estar documentada.

Validación Sistemas Informatizados

Principios BPC



Asegurar el **uso previsto de los sistemas informatizados** durante su ciclo de vida.



Asegurar y documentar que el sistema de procesamiento de datos electrónicos se ajusta a los requisitos establecidos por el promotor en cuanto a la **integridad, exactitud, fiabilidad y consistencia del proceso** (es decir, validación). (BCP, punto 5.5.3.a).

Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Asegurar la **integridad de los datos** proporcionados por los sistemas informatizados.



Supone la **estandarización en toda la organización**, fijando criterios comunes e independientes del soporte, formato o medio en el que los datos hayan sido registrados, procesados, archivados o retirados.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Atribuibles (Attributable)



Requisitos para administradores:

- Gestión de usuarios. La **codificación de los usuarios** generados permite identificar de forma única a la persona.
- Gestión de **permisos de seguridad**. Por puesto de trabajo, evitando el diseño de perfiles de seguridad por usuario. La definición de perfiles consiste en la asignación de accesos a funcionalidades a usuarios capacitados.
- Política de **gestión de contraseñas**. Definición de la complejidad y cambio periódico.

Requisitos para sistemas:

- En el registro de las tareas reguladas debe quedar identificada la **persona o sistema que genera el dato**.
- En el registro de las tareas reguladas debe quedar identificada la **persona o sistema que realiza la actividad que genera o modifica datos**.
- **Audit trail** de registros de datos, usuarios, perfiles de seguridad y contraseñas

Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Legibles (Legible)



Requisitos para administradores:

- Se debe usar un **código de identificación único por sujeto**, que no sea ambiguo para permitir la identificación de todos los datos registrados para cada sujeto.

Requisitos para sistemas:

- En el **registro** de las tareas reguladas debe quedar registro de los **datos y metadatos necesarios**.
- Se encontrarán **disponibles tanto los datos originales como las modificaciones posteriores**.
- En el registro de **audit trail** de las tareas reguladas debe quedar registro de los datos y metadatos necesarios: fecha/hora, usuario, entidad afectada, valor nuevo, valor antiguo y motivo de cambio (para modificaciones y bajas).

Metadatos: describen los atributos del dato, proporcionando contexto y significado y sin los cuales el dato pierde valor y no podemos asegurar su integridad.

Audit trail: registro electrónico seguro que permite la reconstrucción de eventos relacionados con la creación, modificación o eliminación de registros electrónicos. Afecta a la configuración del sistema, a la propia gestión del proceso y a los registros generados.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Simultáneo (Contemporaneous)



- Registrado y visualizado en el momento en el que se realiza la actividad.
- Uso de fecha y hora administrada por la organización, en caso de que la fecha y hora se introduzca de manera manual. El registro de la fecha y hora del registro del dato se debe realizar siempre, independientemente de cuándo se obtuvo el dato.

Requisitos para desarrolladores y proveedores de servicios:

- En caso de que el proceso se componga de varias etapas, debe quedar registrado en cada una de las etapas el resultado parcial y los datos originales. En caso de error, no habrá pérdida de datos.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Original (Original)



El registro original puede ser descrito como la primera captura de información, ya sea grabada en papel o electrónicamente. Que preserva su contenido o significado y naturaleza.

- **Registrado** en el momento en el que se realiza la actividad directamente en los medios autorizados. Sin el uso de soportes intermedios no autorizados.
- Debe quedar **registro de la primera lectura, medición o resultado calculado**.
- En caso de que el usuario cometa un **error** en el registro del dato, el dato original y el modificado deben conservarse.
- Los usuarios no deben tener a su disposición **copias no autorizadas** de los formularios. Todos los **formularios deben disponer de un identificador único**.
- En caso de un registro electrónico debe habilitarse la opción de **modificación** a usuarios autorizados, quedando registro del valor original y nuevo, así como el motivo del cambio, conforme se ha comentado en los requisitos del Audit Trail.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Exactos (Accurate)



- **Datos precisos** que permitan la reconstrucción total de las actividades que han dado lugar a la generación de los mismos. La precisión del registro debe ser conforme a los datos obtenidos y a la precisión requerida para el proceso a gestionar.
- Conforme a los **hechos y protocolos establecidos**.
- **Formación** para usuarios para el registro de datos y uso de sistemas informatizados.
- **Mantenimiento y calibración de equipos** realizada conforme al procedimiento aprobados en el rango de medición apropiado.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Completos (Complete)



- Se considera datos completos a todos los datos y metadatos relevantes, incluida cualquier **repetición o modificación**.
- Cuando se **generen múltiples resultados**, el usuario debe asegurarse de que todos los resultados se registren correctamente.
- El usuario en el registro en papel o en el uso de sistemas informatizados debe seguir un procedimiento claramente definido para **invalidar un registro**. En ningún caso el registro original se destruirá, es más se debe preservar como parte del dato completo.
- Los datos únicamente se pueden eliminar pasado el **tiempo de archivo** y siguiendo el procedimiento establecido.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Consistentes (Consistent)

- De forma previa a la revisión de la conformidad de los datos críticos, de acuerdo a las especificaciones técnicas, se debe evaluar la confiabilidad de los datos. Esto puede implicar revisión del Audit Trail y metadatos, verificar secuencias operativas o verificar datos originales.



@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Perdurables (Enduring)



Los datos deben registrarse de forma permanente y mantenerse durante el periodo de retención declarado. Los procedimientos deben confirmar que los datos archivados, incluidos metadatos relevantes, estén disponibles y sean legibles por humanos.

- En caso de registros electrónicos, debe generarse una política de copias de seguridad que identifique las fuentes de datos, el lugar de origen del registro, el tipo de copias de seguridad y el destino de copias (evitando el almacenamiento de datos GxP en los equipos o PCs donde se originó el dato). Así como determinar la periodicidad de la verificación de la correcta restauración de los datos.

@ Validación Sistemas Informatizados

Fundamentos de Integridad de Datos. Cumplimiento de la regla ALCOA+.



Disponibles (Available)

- Se debe asegurar que los datos GxP que se encuentren en periodo de archivo estén disponibles para el **personal autorizado** de la organización y las **autoridades competentes**.
- Debe comprobarse la **accesibilidad** y la **legibilidad** de los datos si se realizan cambios relevantes en el sistema (hardware o software), entonces la capacidad de recuperar los datos debe garantizarse y comprobarse.

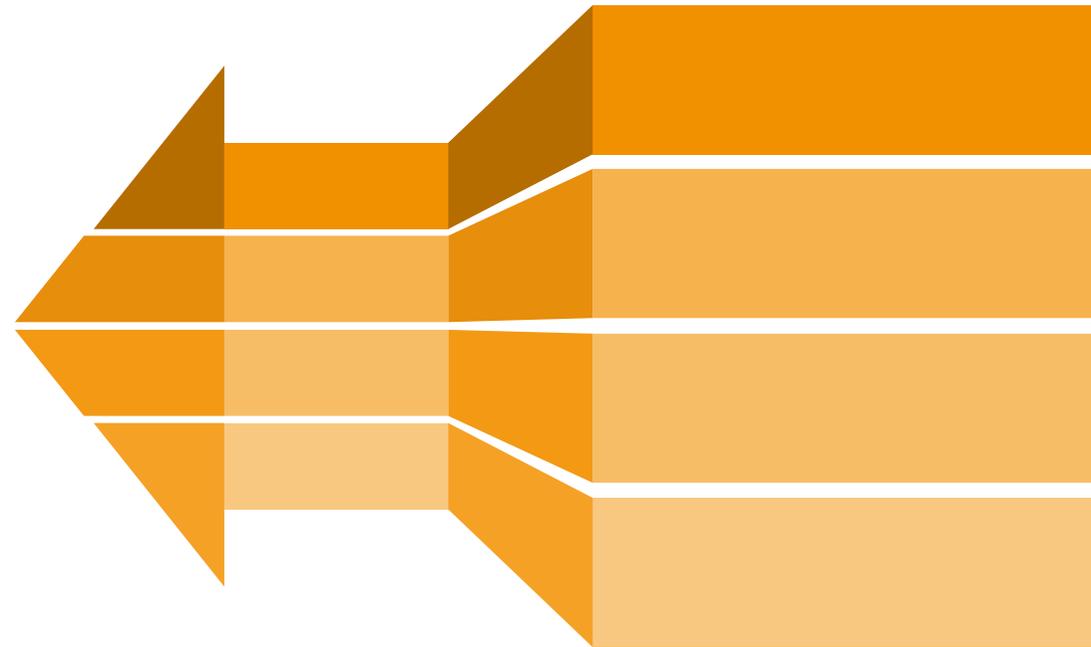


@ Proyecto de Validación

GAMP5

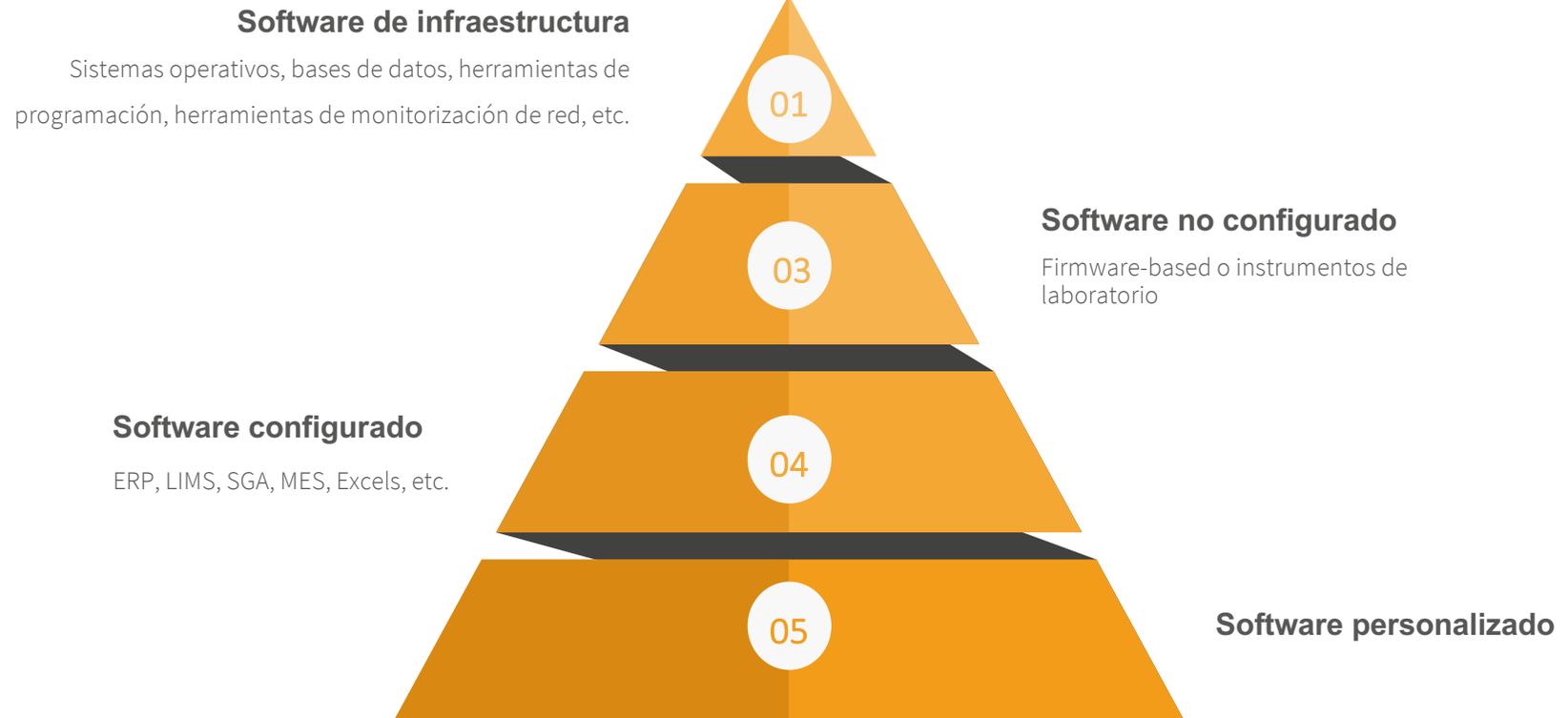
A Risk-Based Approach to Compliant GxP Computerized Systems. Publicada en 2008 por ISPE.

- Definición de ciclo de vida del sistema informatizado.
- Definición de categorías de software.
- Definición de un proyecto según las categorías de software.
- Detalle roles de equipo de validación.
- Detalle gestión con proveedor de servicios: de desarrollo e IT.



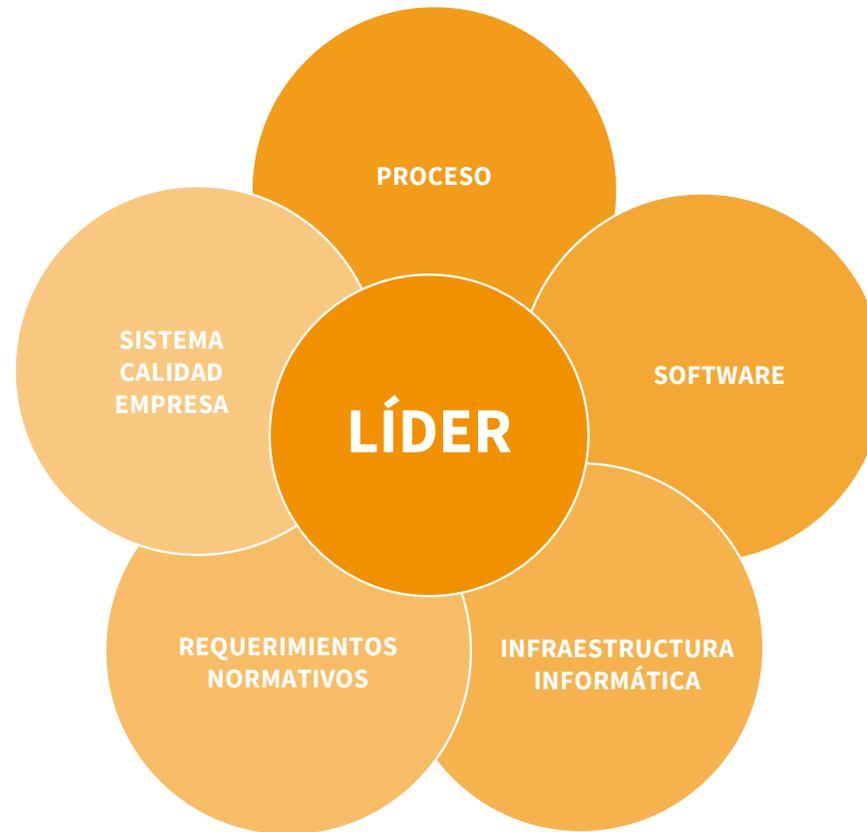
Proyecto de Validación

Categorías de software



@ Proyecto de Validación

Equipo de validación



DIRECCIÓN

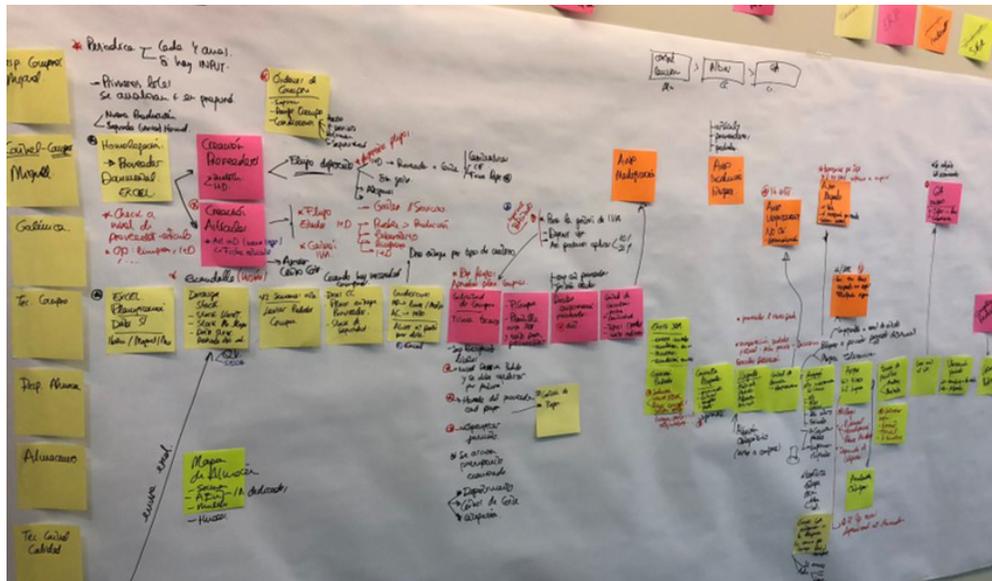
@ Proyecto de Validación

Ciclo de vida del Sistema Informatizados



Proyecto de Validación

Análisis de **Procesos** y Gestión de Datos



- Identificar procesos e información crítica
- Actividades internas y subcontractadas
- Información interna y externa
- Identificar sistemas informatizados presentes y su alcance en el proceso (pueden ser sistemas de gestión, eCRDs, Excels, ...)

Proyecto de Validación

Análisis de Sistemas Informatizados



Registro de Sistemas Informatizados:

- En uso
- Retirados en proceso de archivo
- En proceso de selección

Análisis por sistema informatizado:

- Alcance: operaciones, seguridad e integridad de datos
- Categoría GAMP5
- Proveedor de servicios: acuerdos y responsabilidades
- Infraestructura informática dedicada
- Situación Validación



Proyecto de Validación

Plan Maestro de Validación



1. ¿Objetivo?

Define el procedimiento a seguir para la administración de todos los **sistemas informatizados**.



2. ¿Alcance?

Afecta a todos los sistemas informatizados de la organización, aplicando durante todo su **ciclo de vida**.



3. ¿Legislación?

Determina la **normativa aplicable** y las **guías** a seguir como buenas prácticas.



4. ¿Organización?

Equipo de validación multidisciplinar que aporte experiencia y conocimiento en las diferentes áreas necesarias para la validación.



5. ¿Sistemas informatizados?

Inventario de los sistemas informatizados presentes, retirados y en periodo de análisis / implantación. Estableciendo la descripción mínima a detallar.



6. ¿Criticidad?

Las decisiones sobre la extensión de la validación y de los controles de la integridad de datos tendrán como base una evaluación de riesgos del sistema informatizado. Definición del **criterio de evaluación y puntuación del análisis de riesgos**.



7. ¿Criterios de aceptación validación?

Definición de **requisitos** a cumplir por los **sistemas informatizados críticos**.



8. ¿Metodología?

Definición de las **tareas** a ejecutar, el **personal** participante y sus **responsabilidades, objetivos** y los **criterios de aceptación** para dar por **liberado** cada etapa, los sistemas analizados y cumplido el plan.

Proyecto de Validación

Plan Maestro de Validación



9. ¿Mantenimiento?

Definición de los **procedimientos** de gestión continuada de sistemas informatizados que quedarán implantados en la organización.



10. ¿Auditorías?

Integrar en el plan de **auditorías internas**, a **proveedores de servicio y de integridad de datos** el seguimiento y control de los sistemas informatizados.



11. ¿Planificación?

Definición, revisión y seguimiento del **programa de validaciones**.



12. ¿Revalidaciones?

Gestión continuada de **control de cambios**. En caso de que el cambio tenga un impacto alto se podrá optar por este concepto.



13. ¿Retirada?

Diseño y retirada de sistemas informatizados, así como el **seguimiento** y mantenimiento del sistema y sus datos a lo largo de su tiempo de archivo.



14. ¿Migración?

Diseño y migración de datos entre sistemas informatizados, así como su **verificación**.

Proyecto de Validación

Ejecución de la Validación



Requisitos sistemas informatizados y sus proveedores de servicio.



- Definen, de forma clara y precisa, lo que la compañía regulada requiere del sistema. **Uso previsto.**
- Deben ir **asociados al proceso de negocio** (si aplica).
- Son **independientes de la solución informatizada** a implantar / utilizar.
- Pueden ser utilizados en el **proceso de selección** de soluciones informatizadas y sus proveedores de servicios.
- **Fundamentales** en la validación de sistemas informatizados.
- Propiedades: **específicos, medibles, realizables, realistas y testeables.**
- Tipología: **tecnológicos, informáticos, funcionales, regulatorios, integridad de datos, de servicio y estratégicos.**

@ Proyecto de Validación

Ejecución de la Validación



Requisitos sistemas informatizados y sus proveedores de servicio.



Licenciamiento

Obligación de información y asesoramiento, plazos, precios, responsabilidades, propiedad desarrollos y confidencialidad.

Servicio implantación, formación, soporte y mantenimiento

Alcance, roles y responsabilidades, descripción del servicio, documentación soporte, sistema de calidad y renovaciones.

Proyecto de Validación

Ejecución de la Validación



Análisis de selección de sistemas informatizados asociados a actividades de estudios clínicos SURS-SIEC

Requisitos sistemas informatizados y sus proveedores de servicio.



OQOTECH		SISTEMA INFORMATIZADO A EVALUAR: eCRD				
		OBJETO DE LA EVALUACIÓN: SELECCIÓN DE SISTEMAS INFORMATIZADOS DE GESTIÓN DE DATOS ASOCIADOS A ACTIVIDADES DE ESTUDIOS CLÍNICOS				
		DOCUMENTACIÓN ASOCIADA: PLAN MAESTRO DE VALIDACIÓN DE SISTEMAS INFORMATIZADOS				
CLAVE	DOC. RELACIONADA	ASUNTO	PROV1	PROV2	PROV3	PROV4
REQ CAL 1	-	Requisitos de control y garantía de calidad				
REQ CAL 1.1	BPC punto 2.5	Los ensayos clínicos deberán estar científicamente justificados y estar descritos en un protocolo claro y detallado.	NA	NA	NA	NA
REQ CAL 1.2	BPC punto 2.12	Los medicamentos en investigación deberán fabricarse, manejarse y almacenarse de acuerdo con las Normas de Correcta Fabricación (NCF) pertinentes y se deberán utilizar de acuerdo con el protocolo aprobado.	NA	NA	NA	NA
REQ CAL 1.3	BPC punto 2.13	Se implantarán sistemas con procedimientos que aseguren la calidad de cada aspecto del ensayo.	-	5	5	8
REQ CAL 1.4	BPC punto 5.1.1	El promotor es el responsable de poner en marcha y mantener un sistema de control y garantía de calidad con procedimientos normalizados de trabajo (PNT) escritos a fin de asegurar que los ensayos sean realizados y los datos sean generados, documentados (registrados) y comunicados de acuerdo con el protocolo, la BPC y la normativa vigente.	-	5	6	8
REQ CAL 1.5	BPC punto 5.1.2	El promotor es el responsable de llegar a un acuerdo con todas las partes implicadas que asegure el acceso directo (véase 1.2.1) a todos los centros del ensayo, a todos los datos/documentos originales y los informes necesarios para garantizar la monitorización y auditoría por parte del promotor y las inspecciones por parte de las autoridades nacionales y extranjeras.	-	8	9	9
REQ CAL 1.6	BPC punto 5.1.3	Se deberá aplicar un control de calidad en cada fase del manejo de datos para asegurar que todos ellos son fiables y que han sido procesados de forma correcta.	-	5	9	9
REQ CAL 1.7	BPC punto 5.2.1	Un promotor puede transferir alguna o todas las obligaciones y funciones relacionadas con el ensayo a una CRO, pero la última responsabilidad sobre la calidad e integridad de los datos del ensayo siempre recae en el promotor. La CRO deberá implementar la garantía y el control de calidad.	NA	NA	NA	NA
REQ REG 1	-	Requisitos para los registros electrónicos				
REQ REG 1.2	BPC punto 2.11	Se deberá proteger la confidencialidad de los registros que pudieran identificar a los sujetos respetando la privacidad y las normas de confidencialidad de acuerdo con los requisitos legislativos pertinentes.	-	9	9	9
REQ REG 1.3	BPC punto 4.6.3	El investigador/institución y/o un farmacéutico u otro individuo apropiado, que haya sido designado por el investigador/institución, deberá mantener un registro del envío del medicamento al centro del ensayo, el inventario, el uso por parte de cada sujeto y la devolución al promotor o eliminación alternativa del preparado no utilizado. Estos registros deberán incluir la fecha, cantidad, número de lote/serie, fecha de caducidad (cuando proceda) y código asignado al medicamento en investigación y a los sujetos del ensayo. Los investigadores deberán mantener registros que documenten correctamente que a los sujetos se les suministraron las dosis especificadas en el protocolo y que los datos cuadren con los medicamentos en investigación recibidos del promotor.	NA	NA	NA	NA
REQ REG 1.4	BPC punto 4.9.1	El investigador deberá garantizar la exactitud, integridad, legibilidad y puntualidad en la presentación de los datos al promotor en el plazo de tiempo convenido así como de todos los informes que se le requieran.	-	5	5	5
REQ REG 1.5	BPC punto 4.9.2	Los datos incluidos en el CRD, que se deriven de documentos fuente, deberán ser consistentes con dichos documentos o en caso contrario justificar las discrepancias.	-	5	8	8
REQ REG 1.6	BPC punto 4.9.3	Cualquier modificación o corrección de los datos del CRD deberá ser fechado, firmado con las iniciales y explicado (si es necesario) y no deberá ocultar los datos originales (es decir, se deberá mantener un "audit trail"). Esto es aplicable tanto a los cambios o las correcciones en papel como en soporte electrónico. Los promotores facilitarán a los investigadores y a los representantes designados por los investigadores, una guía sobre cómo hacer tales correcciones. Los promotores deberán tener procedimientos escritos que garanticen que los cambios o las correcciones realizados en los CRD por los representantes designados por el promotor están documentados, son necesarios y están confirmados por el investigador. El investigador deberá conservar los registros de los cambios y las correcciones.	-	6	9	8
REQ REG 1.7	BPC punto 4.9.4	El investigador/institución deberán guardar los documentos del ensayo tal como está especificado en el apartado de Documentos Esenciales para la realización de un Ensayo Clínico. El investigador/la institución deberá tomar las medidas necesarias para prevenir la destrucción accidental o prematura de estos documentos.	-	9	5	9
REQ REG 1.8	BPC punto 4.9.5	Se deberán conservar los documentos esenciales hasta al menos 2 años después de la última aprobación de una solicitud de comercialización en Europa, EEUU o Japón y hasta que no quede ninguna solicitud de comercialización pendiente, o en proyecto, en dichas regiones o hasta que hayan pasado al menos 2 años desde la suspensión formal del desarrollo clínico del medicamento en investigación. Sin embargo, se deberán conservar estos documentos durante un periodo de tiempo más prolongado si así lo establecen las normas regulatorias aplicables o un acuerdo con el promotor. Es responsabilidad del promotor informar al investigador/institución a partir de qué fecha no es necesario conservar estos documentos.	NA	NA	NA	NA
REQ REG 1.9	BPC punto 4.9.7	Ante la solicitud del monitor, auditor, CEC o autoridad sanitaria, el investigador/institución deberá ser capaz de tener disponibles todos los archivos relacionados con el ensayo.	NA	NA	NA	NA
				157	197	219

Proyecto de Validación

Ejecución de la Validación



Instalación y definición de la operación del sistema informatizado.



Objetivo

Verificación de **características, instalación y configuración** del entorno informatizado final (**entorno final productivo y entorno de test**).

- **Descripción** de la infraestructura informática. Determinando los servidores, software empleado, clientes y equipos conectados que componen el sistema informatizado.
- **Mínima definición aceptable** de los componentes de la infraestructura.
- Evaluación de **riesgos de los componentes** de la infraestructura informática para establecer su criticidad.
- **Criterios de aceptación** de la instalación y configuración de los componentes críticos y no críticos.
 - Verificar la existencia de requerimientos hardware y software necesarios para su correcto funcionamiento.
 - Verificar la existencia de requerimientos de comunicación con la red de la empresa, visibilidad con otros sistemas informatizados, servidores de almacenamiento de copias de seguridad o equipos de proceso.
 - Verificar la existencia de una estrategia de instalación y configuración inicial a través de las guías técnicas. Debe quedar determinado los puntos críticos a monitorizar en el proceso de instalación.
 - Verificación de la estructura hardware y software del entorno productivo final respecto a los requerimientos anteriormente descritos (únicamente para componentes críticos).

Proyecto de Validación

Ejecución de la Validación



Instalación y definición de la operación del sistema informatizado.

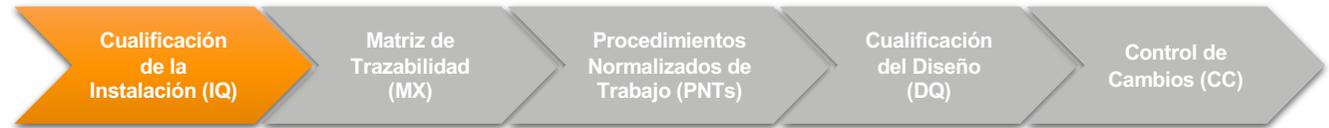
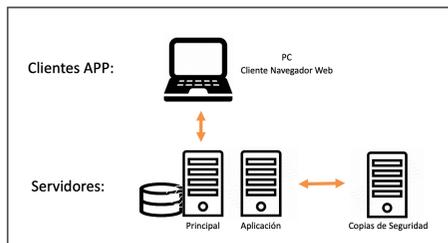


Diagrama Infraestructura Informática



Identificar Componentes: base de datos, aplicación, clientes, servidor, servidor de almacenamiento de copias de seguridad..

- Especificaciones técnicas
- Manual de instalación y configuración
- Instaladores y licencias

Identificar Servidores

- Características mínimas exigibles

Análisis de Riesgos Componentes

- Participación en el proceso
- Gravedad
- Integridad de datos

Protocolo IQ

- Metodología
- Criterios de Aceptación

Test IQ

- Verificaciones, aportando evidencias

Informe IQ

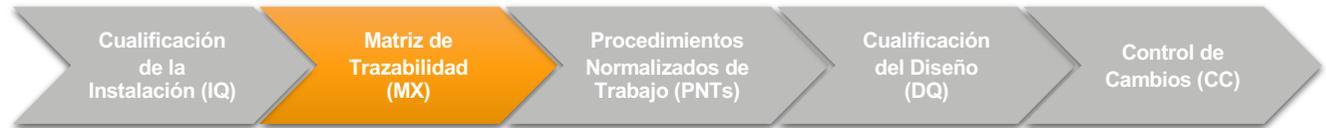
- Tiempo y personas
- Resultados
- Desviaciones y No Conformidades

Proyecto de Validación

Ejecución de la Validación



Instalación y definición de la operación del sistema informatizado.



Centralización de la documentación generada en el proyecto.

- Permite recoger y relacionar toda la información generada
- Permite seguir el avance del proyecto

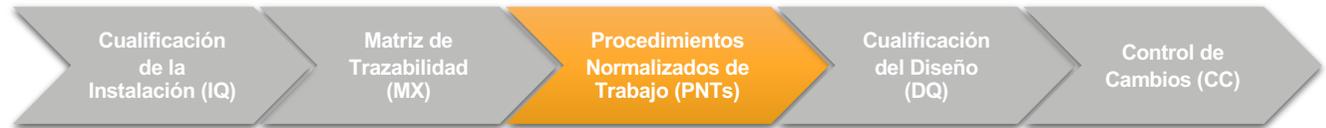
Área de proceso	Proceso	URS	PNT	DQ	CC	AR	OQ	PERF. SEG.	FORM.	PQ	AR-F
Seguridad	Gestión de Usuarios	[cod.]	[cod.]	[cod.]	[cod.]						
	Gestión de Contraseñas	[cod.]	[cod.]	[cod.]	[cod.]						
	Perfiles de Seguridad	[cod.]	[cod.]	[cod.]	[cod.]						
	Audit Trail	[cod.]	[cod.]	[cod.]	[cod.]						
	Firmas Electrónicas	[cod.]	[cod.]	[cod.]	[cod.]						
	...	[cod.]	[cod.]	[cod.]	[cod.]						

Proyecto de Validación

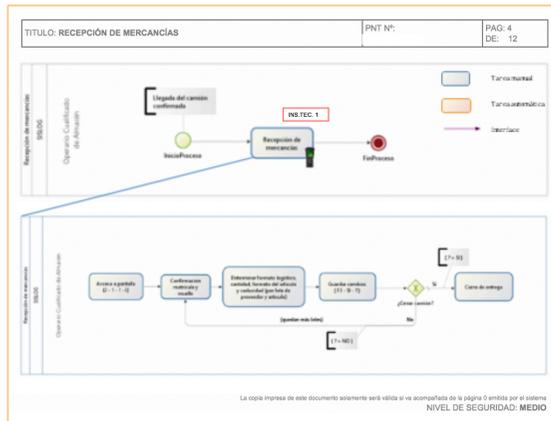
Ejecución de la Validación



Instalación y definición de la operación del sistema informatizado.



- Debe reflejar la **configuración** requerida del sistema, el **uso previsto** por parte de los usuarios finales, el **registro** final de la acción realizada (comprende el registro completo de la tarea y su audit trail) y las **tareas lanzadas**.
- Determina **proceso estándar e incidencias controladas**.
- Identifica **casos especiales**.



TÍTULO: RECEPCIÓN DE MERCANCIAS	PNT N°:	PAG: 6 DE: 12
---------------------------------	---------	------------------

MENU RECEPCIÓN DE PEDIDOS

1. LLEGADA DE CAMION
2. CONTROL CAMION
3. RECEPCIÓN PEDIDO
4. CONSULTA PEDIDO
5. RECHAZO ENTREGA

Selección: 3 recepción pedido

MATRIC: 6193 RE
MUELLE: 101
PEDIDO:
PALETA:

IDENTIFIQUE ARTICULO

Por defecto aparece en la pantalla de recepción de pedidos el último pedido dado de alta en el sistema. El almacenero deberá comprobar la matrícula y muelle de descarga. En caso de que los datos mostrados en pantalla no sean correctos se deberán rectificar de forma manual.
ENTER para comenzar la recepción.

A continuación, se muestra una pantalla con la información de las mercancías demandadas al proveedor en el pedido de compra asignado a la recepción.

En la primera línea se muestra la matrícula y pedido de compra. De esta forma si se ha confirmado la llegada de un albarán con más de un pedido será posible confirmarlo en la misma recepción.

En caso de que se haya confirmado más de una mercancía en la llegada, se deberá cambiar de mercancía pulsando F2.

En el caso de que se detecte que no se ha confirmado la llegada de una mercancía, será posible reabrir la llegada. Conforme al PNT KOR-SI102 en vigor.

La copia impresa de este documento solamente será válida si va acompañada de la página 0 emitida por el sistema
NIVEL DE SEGURIDAD: MEDIO

TÍTULO: RECEPCIÓN DE MERCANCIAS	PNT N°:	PAG: 11 DE: 12
---------------------------------	---------	-------------------

En las entregas que se reciba más de un lote por artículo es necesario guardar la recepción por cada lote de proveedor, ya que únicamente de esta forma podremos especificar la cantidad y caducidad de cada uno de ellos.

Exclusivamente en la recepción del último lote se deberá cerrar camión.

8. REGISTRO

- Registro de la entrega en SISLOG.
 - o Al finalizar la recepción la entrega cambia de MU a EX.
- Pedido de compra en SISLOG.
 - o Se asocian las cantidades confirmadas de la entrega y cambia su situación de cabecera y líneas a RE (si está parcialmente recepcionado) o CO (si está recepcionado completamente).
- Registro de movimiento de la recepción CR en SISLOG.
- Alta de paletas de la entrega. Asociando, artículo, lote interno, lote de proveedor, caducidad, cantidad y formato asociado, código y línea de pedido de compra, código de entrega, situación física y lógica.
- Pedido de compra en el ERP.
 - o Se asocian las cantidades confirmadas de la entrega y cambia su situación de líneas a CO (si está recepcionado completamente).
- Albarán de recepción.
 - o Se asocian las cantidades confirmadas de la entrega, agrupando por artículo y lote interno. Asociando además el lote de proveedor y caducidad.

9. TAREAS LANZADAS

A continuación, se registran acciones derivadas del proceso.

9.1. INTERFACES CON OTROS SISTEMAS INFORMATIZADOS

- Interface de regularización de stock desde SISLOG al ERP: rst.
- Al cerrar la entrega se envía desde SISLOG al ERP el albarán de recepción: cen y ten.

9.2. ETIQUETAS GENERADAS

- Por palé recepcionado se imprimirá la etiqueta identificativa de palé (según el tipo de etiqueta configurado por artículo). Se imprimirán tantas copias de la etiqueta de palé conforme especificue en el campo "Num. Ets.", también configurado en la ficha del artículo. Asimismo, en caso de que el artículo tenga habilitado el check de etiquetar cajas, se imprimirá una etiqueta por cada caja del palé.

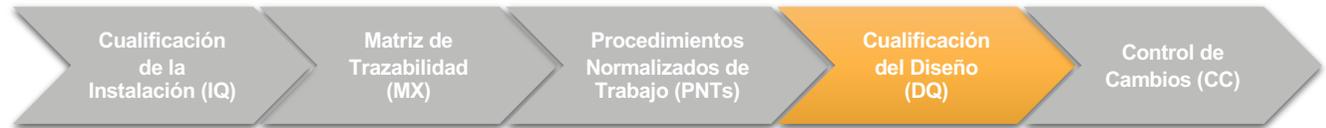
La copia impresa de este documento solamente será válida si va acompañada de la página 0 emitida por el sistema
NIVEL DE SEGURIDAD: MEDIO

Proyecto de Validación

Ejecución de la Validación



Instalación y definición de la operación del sistema informatizado.



Objetivo

Verificación del **diseño operativo, técnico y de seguridad del sistema informatizado** a implantar.

- **Evaluación del cumplimiento de requerimientos** de usuario (URS) contra el uso final detallado en los procedimientos normalizados de trabajo (PNTs)
- **Evaluación de riesgos.** Verificar, en caso de que el diseño del proceso informatizado haya sido modificado respecto al requerimiento inicial para certificar que no se pone en riesgo la gestión del proceso, la calidad del producto o la integridad de datos.

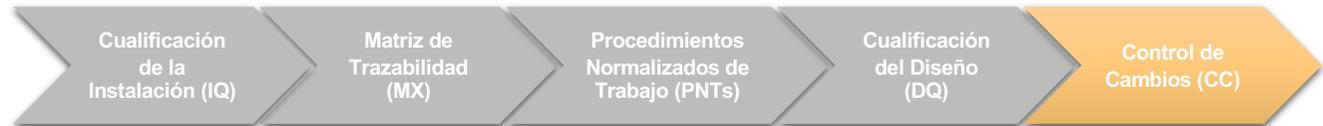
OQOTECH		SISTEMA INFORMATIZADO A EVALUAR: eCRD						
		OBJETO DE LA EVALUACIÓN: CUALIFICACIÓN DE DISEÑO (DQ) SISTEMAS INFORMATIZADOS DE GESTIÓN DE DATOS ASOCIADOS A ACTIVIDADES DE ESTUDIOS CLÍNICOS						
		DOCUMENTACIÓN ASOCIADA: PLAN MAESTRO DE VALIDACIÓN DE SISTEMAS INFORMATIZADOS						
CLAVE	DOC. RELACIONADA	ASUNTO	CLAVE DQ	IMPLANTADO	MODIFICADO	ADICIONAL	PNT	OBSERVACIONES
REQ SI 1	-	Requisitos para los sistemas informatizados	-	-	-	-	-	-
REQ SI 1.4	BPC punto 5.5.3 (b)	Elaborar y actualizar el PNT para la utilización de estos sistemas.	TDQS SI 1.4	No	No	No	[cod. PNT]	El proveedor no suministra PNTs.
REQ SI 1.5	BPC punto 5.5.3 (c)	Garantizar que el diseño de los sistemas permite la modificación de datos de tal manera que estos cambios queden documentados y que los datos originales no sean eliminados (es decir, mantener un método de seguimiento retrospectivo "audit trail", seguimiento retrospectivo de los datos "data trail", o seguimiento retrospectivo de los cambios "edit trail").	TDQS SI 1.5	Si	Si	No	[cod. PNT]	El audit trail no gestiona el motivo de modificación.
REQ SI 1.6	BPC punto 5.5.3 (d)	Mantener un sistema de seguridad que impida el acceso no autorizado a los datos.	TDQS SI 1.6	Si	No	No	[cod. PNT]	-
REQ SI 1.10	BPC punto 5.5.4	Si se modifican los datos durante su procesamiento, siempre deberá ser posible comparar los datos originales y las observaciones con los datos procesados.	TDQS SI 1.10	Si	No	No	[cod. PNT]	-
REQ SI 1.11	BPC punto 5.5.5	El promotor deberá utilizar un código de identificación de los sujetos que no sea ambiguo que permita la identificación de todos los datos registrados para cada sujeto.	TDQS SI 1.11	Si	No	No	[cod. PNT]	-
REQ SI 1.12	BPC punto 5.5.6	El promotor, u otros propietarios de los datos, conservarán todos los documentos esenciales específicos del promotor, que pertenezcan al ensayo.	TDQS SI 1.12	Si	No	Si	[cod. PNT]	El sistema dispone de un pequeño módulo de gestión documental.

Proyecto de Validación

Ejecución de la Validación



Instalación y definición de la operación del sistema informatizado.



- **Evaluación continua y documentada** del funcionamiento y modificaciones de un sistema informatizado para determinar si es necesario revalidar el sistema tras un cambio.
- **Los cambios deben solicitarse, registrarse, evaluarse, ejecutarse o rechazarse.**
- **Especificaciones técnicas** del control de cambios:
 - **Detalle técnico** del cambio:
 - Flujo de proceso, pantallas, nuevos datos, controles, nuevos cálculos, tareas a lanzar, etc.
 - **Análisis de riesgos**
 - Criticidad de la nueva funcionalidad
 - Sistema/s informatizado/s afectados. Áreas y funcionalidades afectadas (directa o indirectamente)
 - Impacto del cambio
 - Integridad de los datos históricos
 - Integraciones: con otros sistemas informatizados o equipos
 - **Documentación** afectada
 - **Verificaciones** a realizar
 - **Formación** a realizar
 - **Responsabilidades** de revisión y aprobación de cambios. Responsables de cada tarea a realizar, plazos y secuencias.
 - **Seguimiento**

Proyecto de Validación

Ejecución de la Validación



Verificación de la operación del sistema informatizado y seguridad de la información.



- Deben **registrarse y mantenerse**.
- **Mínima definición de equipos de proceso críticos**
 - Asociados a funcionalidades
 - Codificación
 - Modelo, fabricante, versión y número de serie
 - Localización
 - Equipos o piezas auxiliares
- **Información asociada**
 - **Documentación:** instalación y configuración, calibración, administración y uso, mantenimiento, cualificación, validación de método y validación del sistema.
 - **Proveedor** de servicios.
 - Control de **accesos para administración y configuración** del equipo y para su uso.
 - **Registro de datos.** Con datos y metadatos. Seguridad en la manipulación del dato.
 - **Audit trail.**

Proyecto de Validación

Ejecución de la Validación



Verificación de la operación del sistema informatizado y seguridad de la información.



Objetivo

Verificación de la operación del sistema informatizado. Asegurando de forma documentada que el sistema está configurado y funciona de acuerdo con las especificaciones descritas y previamente aprobadas.

- **Entorno de test** establecido, adecuado y documentado.
- **Análisis de riesgos.**
 - Partiendo de la matriz de trazabilidad. Análisis de áreas de proceso informatizadas y sus funcionalidades
 - Estudio de PNTs para identificar posibles fallos en el funcionamiento, seguridad o integridad de datos.
 - Por cada fallo análisis de la probabilidad, severidad y detectabilidad
 - Establecimiento de la criticidad de las funcionalidades
- **Estrategia de testeo.** (1) identifica el fallo potencial a verificar, (2) documentación asociada: URS y PNTs, (3) objetivo, (4) criterio de aceptación, (5) prerrequisitos, (6) pasos, (7) resultados esperados y evidencias, (8) acciones después del test, (9) responsable/s de la estrategia de testeo.
- **Ejecución del testeo.** Refleja: (1) resultados del test, vinculando al código de estrategia de test, (2) detalla los resultados obtenidos y las capturas generadas como evidencia, (3) determina si el resultado por cada paso es apto o no apto según el criterio establecido en la estrategia de test.

Proyecto de Validación

Ejecución de la Validación



Cualificación de la operación (OQ)

		SISTEMA INFORMATIZADO A EVALUAR: eCRD OBJETO DE LA EVALUACIÓN: CUALIFICACIÓN DE LA OPERACIÓN (OQ) CLIENTE:		
		ESTRATEGIA DE TEST		
ÁREA: REGISTROS ELECTRÓNICOS		PROCESO: Modificación de registros electrónicos		
CÓDIGO DEL TEST: OQT-REQ1.5		TÍTULO: Audit Trail		
USER REQUIREMENT CODE(S): REQ SI 1.5				
PNT ASOCIADO: [COD. PNT]				
OBJETIVO: Proporcionar evidencia documental que confirme el correcto funcionamiento del audit trail en la modificación de valores asociados a formularios.				
CRITERIOS DE ACEPTACIÓN: - Verificar que al realizar una modificación se inserta un nuevo registro en el audit trail. Este registro debe contener esta información: fecha y hora, usuario de la modificación, entidad modificada, valor antiguo, valor nuevo y motivo del cambio si es una baja o modificación.				
PRERREQUISITOS: - Existencia de un estudio en curso. - Disponer del código de usuario y contraseña de un usuario que disponga de la seguridad correspondiente para modificar datos de formularios de visita del estudio en curso. - Disponer del código de usuario y contraseña de un usuario que no disponga de la seguridad correspondiente para modificar datos de formularios de visita del estudio en curso. - Existencia de un formulario de visitarellenado y no cerrado por el médico. - Existencia de audit trail en la aplicación, activado para el estudio en curso.				
PASO DEL TEST	REFERENCIA DE PROCEDIMIENTO	ACCIÓN	DATOS A CAPTURAR	RESULTADO ESPERADO
1.1	Cód.	Autenticarse con un usuario sin acceso de escritura al estudio en curso.	Captura de pantalla en la que aparezca el código de usuario utilizado y permiso de modificación del formulario de visitas.	Usuario existentes sin permisos de edición al formulario de visitas.
1.2	Cód.	Visualizar formulario de visita relleno (no cerrado) de un estudio en curso con el usuario sin permisos de edición.	Captura de pantalla en la que aparezca el código de usuario utilizado y que no tiene la disponibilidad de modificar datos, por campo o de guardar valores modificados a través de un botón.	Uso de un usuario sin permisos de edición y no posibilidad de aplicar cambios.
1.3	Cód.	Revisión de la activación del audit trail para los formularios de visitas (todos los campos) del estudio en curso.	Captura de pantalla que muestre el formulario a utilizar y que dispone de un audit trail activado.	Audit Trail activado para el formulario a utilizar en el test.
1.4	Cód.	Autenticarse con un usuario con acceso de escritura al estudio en curso.	Captura de pantalla en la que aparezca el código de usuario utilizado y permiso de modificación del formulario de visitas.	Usuario existentes sin permisos de edición al formulario de visitas.
2.1	Cód.	Modificación del formulario de visita. Modificar todos los tipos de campo posibles: fechas, booleanos, listado de valores y numéricos.	Captura de pantalla de cada modificación mostrando el dato antes de aplicar el cambio, motivo determinado y valor final después de la modificación.	Cambio de valores y solicitud por parte del sistema del motivo del cambio.
2.2	Cód.	Consulta del audit trail generado	Captura del registro de audit trail por cambio aplicado.	Registro del audit trail. Los valores a visualizar son los siguientes: fecha y hora, usuario de la modificación, entidad modificada, valor antiguo, valor nuevo y motivo del cambio.
ACCIONES DESPUÉS DEL TEST: No aplica.				
FECHA Y FIRMA DEL GENERADOR DE LA ESTRATEGIA DE TEST:				
FECHA Y FIRMA DEL REVISOR Y APROBADOR DE LA ESTRATEGIA DE TEST:				

		SISTEMA INFORMATIZADO A EVALUAR: eCRD OBJETO DE LA EVALUACIÓN: CUALIFICACIÓN DE LA OPERACIÓN CLIENTE:		
		TESTEO		
ÁREA: REGISTROS ELECTRÓNICOS		PROCESO: Modificación de registros electrónicos		
CÓDIGO DE TEST: OQE-REQ1.5		TÍTULO: Audit Trail		
NÚMERO DE EJECUCIÓN DE TEST: 1				
FECHA INICIO: 27/03/2020		FECHA FIN: 27/03/2020		
PASO DEL TEST	DATOS A CAPTURAR (CÓDIGOS DE CAPTURAS)	RESULTADO / REGISTRO DE LA INCIDENCIA	APTO / NO APTO	
1.1	Captura 1.1	Código de usuario utilizado: 20 Código permiso: X	Apto	
1.2	Captura 1.2	Formulario de visita: 1 Caso en curso con código: C2 Usuario utilizado: 20	Apto	
1.3	Captura 1.3	Permiso de Audit Trail: Y Aplicable a todos los casos y todos los formularios.	Apto	
1.4	Captura 1.4	Código de usuario utilizado: 21 Código permiso: X	Apto	
2.1	Captura 2.1.1	Cambio campo tipo fecha: "fecha visita", de 26/03/2020 a 27/03/2020, motivo: prueba.	Apto	
2.1	Captura 2.1.2	Cambio campo tipo booleano "visita presencial", de No a Si, motivo: prueba2.	Apto	
2.1	Captura 2.1.3	Cambio campo tipo lista de valores "perfil de paciente", de adulto a anciano, motivo: prueba3.	Apto	
2.2	Captura 2.2.1	Registro cambio fecha visita. Con fecha (27/03/2020), hora (10:30), usuario (21), entidad modificada (fecha visita), valor antiguo (26/03/2020), valor nuevo (27/03/2020) y motivo (prueba).	Apto	
2.2	Captura 2.2.2	Registro cambio visita presencial. Con fecha (27/03/2020), hora (10:32), usuario (21), entidad modificada (visita presencial), valor antiguo (No), valor nuevo (Si) y motivo (prueba2).	Apto	
2.2	Captura 2.2.3	Registro cambio perfil de paciente. Con fecha (27/03/2020), hora (10:36), usuario (21), entidad modificada (perfil de paciente), valor antiguo (adulto), valor nuevo (anciano) y motivo (prueba3).	Apto	
COMENTARIOS:				
FECHA Y FIRMA EJECUTOR DEL TEST:				
FECHA Y FIRMA REVISOR Y APROBADOR DEL TEST:				

Proyecto de Validación

Ejecución de la Validación



Verificación de la operación del sistema informatizado y seguridad de la información.



- Los **perfiles de seguridad** son una agrupación de accesos/permisos al software.
 - Desde el **organigrama**, se definen **puestos de trabajo**. Éstos también pueden tener asociado accesos a los sistemas informatizados.
 - De esta forma queda definido el **ámbito de actuación de los usuarios en el sistema**.
- Los **usuarios** deben disponer de un identificador único dentro de la aplicación.
 - Deben tener **asociado un perfil de seguridad**.
 - Figura de **administrador**, diferenciada y usuario no involucrado en el proceso.
- Implantar un política de **gestión de contraseñas**: gestión de características y complejidad, así como la gestión de la renovación de la contraseña (por tiempo o incidencia por olvido o bloqueo de la cuenta de usuario).
- **Audit trail** de usuarios, contraseñas y perfiles de seguridad, que refleje el alta, baja o modificación.

Proyecto de Validación

Ejecución de la Validación



Verificación de la operación del sistema informatizado y seguridad de la información.



- **Necesidades formativas.** Por usuario, las funcionalidades asignadas a su perfil de puesto de trabajo informatizado.

- Material de **soporte** a la formación
- PNTs.
- Sesiones de formación prácticas en el entorno de test.
- Carteles informativos en los lugares de trabajo.
- Soporte técnico.
- La formación debe quedar **registrada**.
- Verificación de la **capacitación** del usuario
- **Reciclaje**

Procesos	Todos	Nivel mínimo para dar soporte	Fecha creación	LOGO	
Área Procesos	INFORMÁTICA	2	Fecha Revisión		
Niveles	Descripción				
Nivel 1	Conoce funcionalidad y su documentación asociada.				
Nivel 2	Configura y administra la aplicación.				
Nivel 3	Conoce configuración, uso y registro de funcionalidad. Puede formar y dar soporte a usuarios.				
Nivel 4	Conoce configuración, uso, registro, interfaces y tablas de funcionalidad. Puede formar, dar soporte a usuarios y validar.				
Nivel	DESCRIPCIÓN GENERAL	TAREAS ESPECIFICAS	PNT'S	DPTO FORMADOR	RESP FORMADOR
Nivel 1					
Nivel 1					
Nivel 1					
Nivel 1					
Nivel 1					
Nivel 1					
Nivel 1					
Nivel 2					
Nivel 2					
Nivel 2					

Proyecto de Validación

Ejecución de la Validación



Verificación de la operación del sistema informatizado y seguridad de la información.



- La **gestión de datos** debe ser considerado como un **proceso en sí mismo**.
- 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, utilizados o retirados.
- Aplicable a **documentación** del sistema de calidad y operaciones, **equipos** de proceso y **sistemas informatizados**.



Proyecto de Validación

Ejecución de la Validación



Verificación del proceso final y su información asociada.



Objetivo

Verificación de la integración de todos los elementos, asegurando la gestión, control y trazabilidad de los procesos.

- Alcance de la **Verificación**:
 - Fases anteriores de la **cualificación completadas** (con informe y sin desviaciones críticas): URS, IQ, DQ y OQ.
 - PNTs** de administración y uso del sistema **aprobados**.
 - Seguridades** definidas e **implantadas**
 - Formación completada**.
 - Protocolos** de **mantenimiento** del estado de control **aprobados**.
- Verifica **la integración de todos los elementos** de las áreas de proceso informatizadas, asegurando su trazabilidad.
- Estrategia de testeo**. (1) identifica el fallo potencial a verificar, (2) documentación asociada: URS y PNTs, (3) objetivo, (4) criterio de aceptación, (5) prerrequisitos, (6) pasos, (7) resultados esperados y evidencias, (8) acciones después del test, (9) responsable/s de la estrategia de testeo.
- Ejecución del testeo**. Refleja: (1) resultados del test, vinculando al código de estrategia de test, (2) detalla los resultados obtenidos y las capturas generadas como evidencia, (3) determina si el resultado por cada paso es apto o no apto según el criterio establecido en la estrategia de test.

@ Proyecto de Validación

Ejecución de la Validación



Verificación del proceso final y su información asociada.



- **Resumen** de duración, personal involucrado, actividades y resultados obtenidos.
- **Revisión del cumplimiento de los criterios de aceptación.**
 - Documentación generada y aprobada.
 - Sistemas informatizados validados sin desviaciones críticas.
 - Proveedores auditados.
 - Seguridades definidas e implantadas.
 - Usuarios formados.
 - Protocolos de mantenimiento del entorno validado definidos e implantados.
- **Conclusiones.**
- Certificado de **liberación** del sistema informatizado.

@ Proyecto de Validación

Mantenimiento de estado de control



Procedimientos para mantener el estado de control en todo el ciclo de vida del sistema informatizado.



- Seguridad física y lógica.
- Copias de seguridad y restauración de datos.
- Monitorización del rendimiento.
- Plan de contingencia y continuidad del negocio.
- Control de cambios
- Gestión de usuarios y perfiles de seguridad
- Plan de formación

@ Proyecto de Validación

Mantenimiento de estado de control



Procedimientos para mantener el estado de control en todo el ciclo de vida del sistema informatizado.



- Auditorías **internas**
- Auditorías a **proveedores** de servicio tecnológico
- Auditoría en **integridad de datos**

Proyecto de Validación

Retirada



Procedimientos para mantener el estado de control en el tiempo de archivo.



- **Protocolo**

- Diseño del **entorno final durante el tiempo de archivo**:
 - Sistema informatizado validado.
 - Procedimientos aprobados para la administración y uso del sistema.
 - Definición de permisos de acceso. Como lectura.
 - Definición de la infraestructura informática final:
 - Servidor.
 - Base de datos.
 - Acceso cliente (si aplica, si la aplicación es cliente/servidor).
 - Seguridad de acceso al servidor, base de datos y componentes.
 - Política de seguridad durante el tiempo de archivo:
 - Contenido.
 - Estrategia de copias: tipo, periodicidad y destino de copias.
 - Plan de restauración.

- **Seguimiento**

- Incluido en auditorías periódicas (internas y de integridad de datos).
- Ejecución, registro y evaluación de restauración de datos.

@ Proyecto de Validación

Retirada



Procedimientos para mantener el estado de control en el tiempo de archivo.



- **Diseño del entorno final**

- Información a transferir al nuevo sistema
 - **Documento de interface** de transferencia de datos:
 - Canal de la transferencia: por ficheros o bases de datos.
 - Detalle de la comunicación: campos, tipo de campo, precisión, etc.
 - **Protocolo de transferencia de datos.** Procesamiento de la información para adecuarla al interface.
 - Tratamiento de la información original.
 - Generación de nuevos datos (obligatorios).
 - Cálculos a realizar.

- **Ejecución de la migración**

- **Exportación** de la información y tratamiento de datos siguiendo el protocolo.
- **Verificación de la transferencia de datos.** En valor y/o significado.



¡Gracias por su atención!

Mayte Garrote Gallego

✉ mayte@oqotech.com