OQOTECH
PROCESS VALIDATION SYSTEM

DATA INTEGRITY

Jornada de Sistemas Informáticos en la Industria farmacéutica

Mayte Garrote
6 de julio de 2017

Data Integrity - Integridad de datos

- Definición
- Anexo 11
- Guías ID
- Conceptos
- Requerimientos
- Estrategia
- Validación IS – ID
- Auditoría ID

Requerimiento de que los datos sean completos, consistentes y precisos

- La gestión de datos debe ser considerado 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, utilizados o retirados.

Requerimiento ya presente en Anexo 11 de las NCF

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**.

OQOTECH
PROCESS VALIDATION SYSTEM

MARCO REGULATORIO

Todas sugieren la implantación de **políticas y medidas** para mantener y asegurar la exactitud y consistencia de datos en todo su ciclo de vida.

Lo que supone una **estandarización en toda la organización**, fijando criterios comunes e independientes del soporte físico de los datos y su origen.

Generación y Registro

- Datos registrados en papel.
- Datos generados en papel de manera automática.
- Datos registrados en formato electrónico, tanto capturados electrónicamente como registrados por un operador.

- Diferentes tipos de riesgos.
- Adaptar la estrategia de control a su naturaleza y tecnología empleada.

Metadatos

- Información contextual necesaria para entender los datos.
- Describen los atributos del dato, proporcionando contexto y significado y sin los cuales el dato pierde valor y no podemos asegurar su integridad.
- Por ejemplo: fecha y hora, código de usuario, código de equipo, audit trail, etc.

- Las relaciones entre los datos y sus metadatos deben **preservarse de forma segura y trazable.**

Audit trail

- Registro electrónico seguro que permite la reconstrucción de eventos relacionados con la creación, modificación o eliminación de registros electrónicos.
- Recoge la información la siguiente información clave: cuándo, qué, quién y a veces por qué.
- Afecta a la configuración del sistema, a la propia gestión del proceso y a los registros generados.

- Determinar **procesos críticos y mantenimiento de datos maestros** que deben disponer de audit trail. Según AR.
- Las **copias de seguridad** deben contener toda la información del proceso: datos y audit trail.
- Los audit trail **deben revisarse** como una parte más del proceso a verificar.

Regla ALCOA*

A	*Attributable* **Atribuibles**	*Debe ser posible **identificar la persona** que realizó la tarea registrada.* *Demuestra el control de la acción por personal identificado, autorizado y capacitado.* *También aplica a los cambios realizados en los registros: correcciones, eliminaciones, cambios, etc.*
L	*Legible* **Legibles**	*Los datos y metadatos deben ser almacenados, evitando su deterioro o pérdida, durante todo el tiempo reglamentario de conservación.* *Deben estar **fácilmente disponibles y entendibles para el personal autorizado**.*
C	*Contemporaneous* **Simultáneos**	*El registro de los datos debe producirse en el **menor tiempo posible** desde su generación y sin el uso de soportes temporales intermedios.*
O	*Original / true copy* **Originales o copia verificada**	*El registro original puede ser descrito como la **primera captura de información**, ya sea grabada en papel o electrónicamente.*
A	*Accurate* **Exactos**	*Datos **precisos** que permitan la reconstrucción total de las actividades que han dado lugar a la generación de los mismos.*

OQOTECH PROCESS VALIDATION SYSTEM

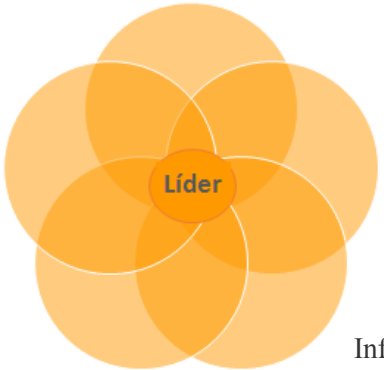
Regla ALCOA*

Complete **Completos**	***Toda la información crítica*** *para la reconstrucción* ***de un proceso*** *debe quedar registrada, incluyendo datos y metadatos relevantes.* *Todos los datos, incluyendo cualquier repetición o reproceso se tiene que conservar.*
Consistent **Consistentes**	***Todos las tareas del proceso*** *tienen que constar.*
Enduring **Perdurables**	*Los datos deben permanecer* ***intactos y accesibles*** *como un registro permanente / duradero a lo largo de su tiempo de archivo.*
Available **Disponibles**	*Los registros deben estar* ***disponibles*** *para revisión en cualquier momento durante el* ***período de retención requerido****, accesible en un formato legible a todo el personal aplicable responsable de su revisión, ya sea para decisiones de liberación de rutina, investigaciones, tendencias, informes anuales, auditorías o inspecciones*

Grupo de trabajo multidisciplinar. **PERSONAS**

Proceso

Sistema Calidad Empresa



Software

Requerimientos regulatorios

Infraestructura informática

Dirección

Estrategia para aplicar los requerimientos

Marcar pasos, responsables y objetivos. **PLAN**

Validación de Sistemas Informatizados

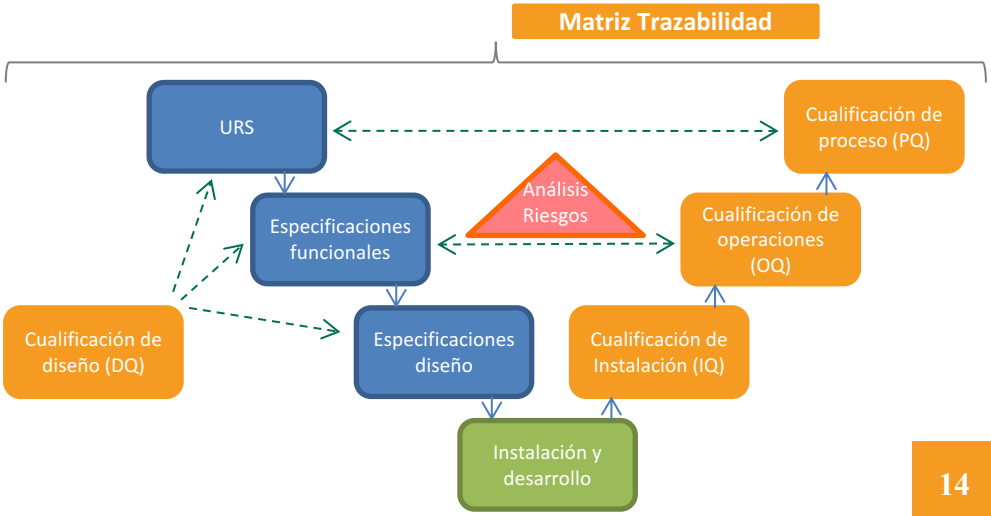
Incorporando la integridad de datos en todas las fases de la validación

Implantación Política de Integridad de Datos

Realizar auditorías, controlar desviaciones, indicadores y formación.

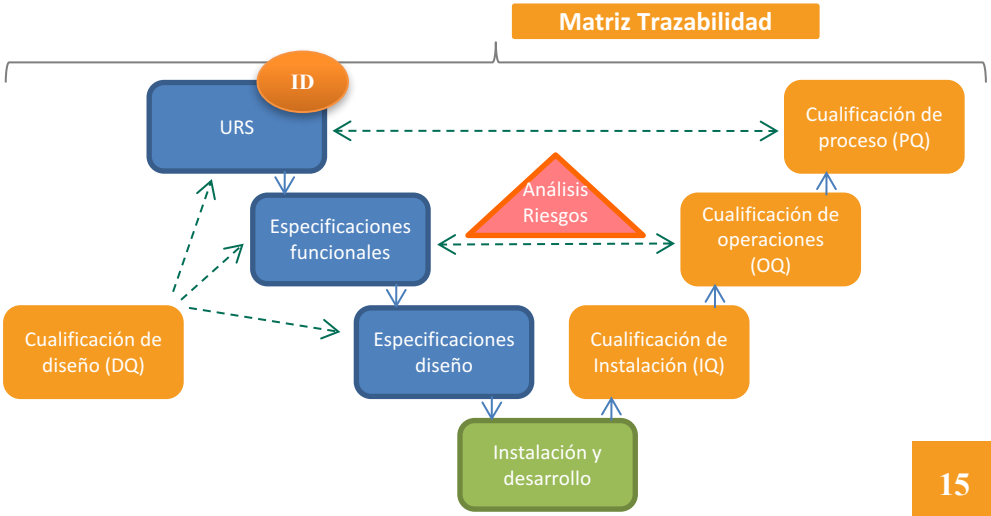
Validación basada en el **análisis de riesgos**

Incorporar al análisis de cada etapa la afectación a la integridad de datos.



Introducir un área de requerimiento para la integridad de datos y Anexo 11 NCF

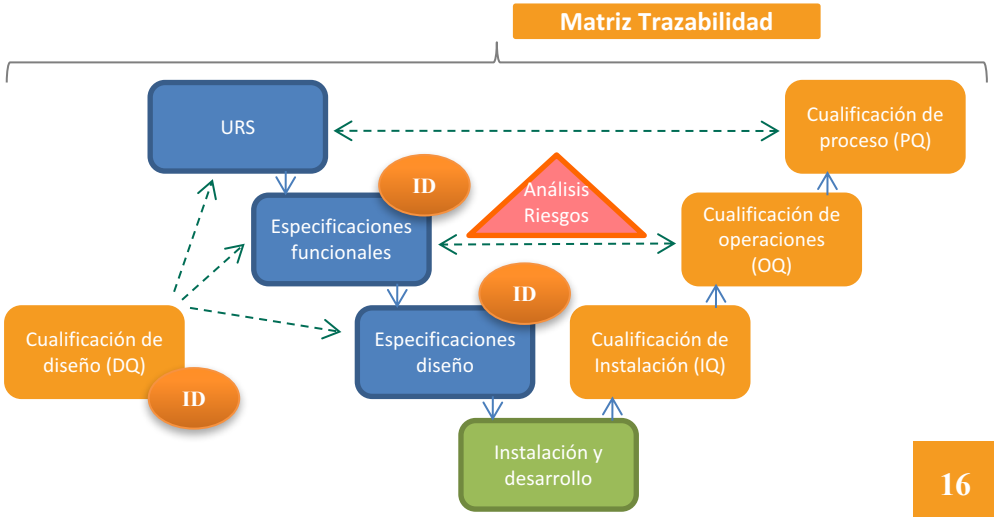
Requerimiento integridad de datos: regla ALCOA.



OQOTECH
PROCESS VALIDATION SYSTEM

Seguridad de la información

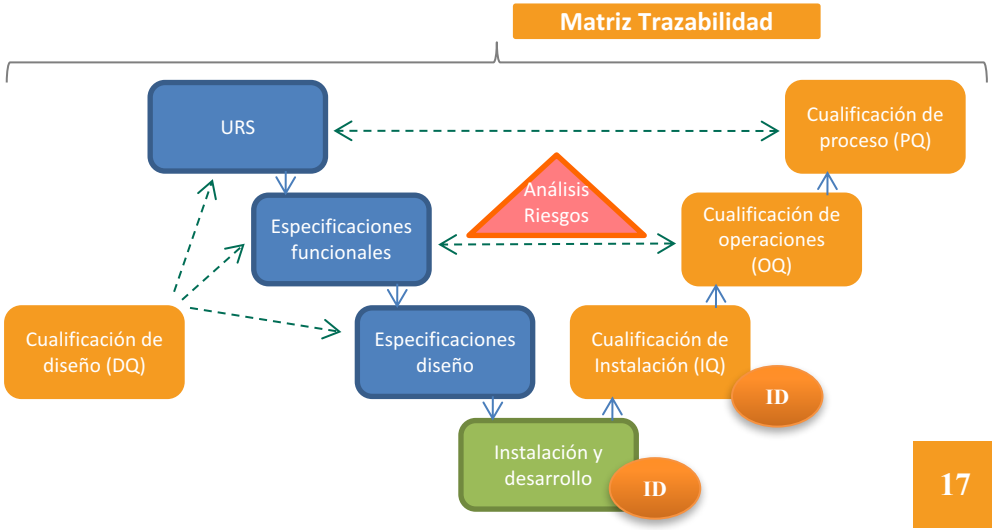
- Usuarios del sistema informatizado identificados.
- Control de contraseñas.
- Perfiles de seguridad.
- Audit trail.
- Flujos de procesos.
- Seguridad registros.
- Establecer procedimientos alternativos en la gestión de ID, no cubiertos por el sistema.



OQOTECH PROCESS VALIDATION SYSTEM

Seguridad de la información

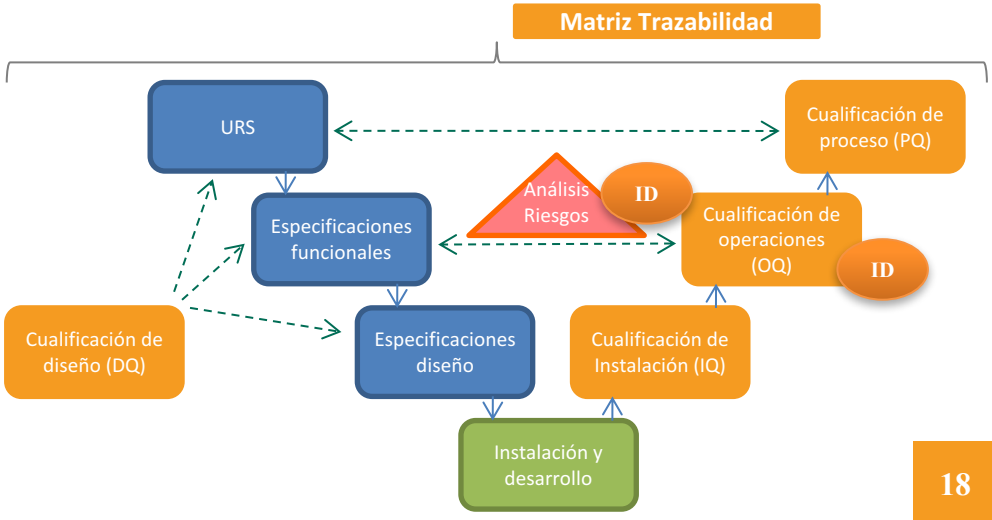
- Seguridad física y lógica.
- Seguridades usuarios sistemas operativos.
- Acceso a rutas y datos del sistema.
- Comunicación servidor del sistema informatizado con servidores de almacenamiento de copias de seguridad.
- Copias de seguridad.
- Plan de contingencia.
- Monitorización del rendimiento.



OQOTECH
PROCESS VALIDATION SYSTEM

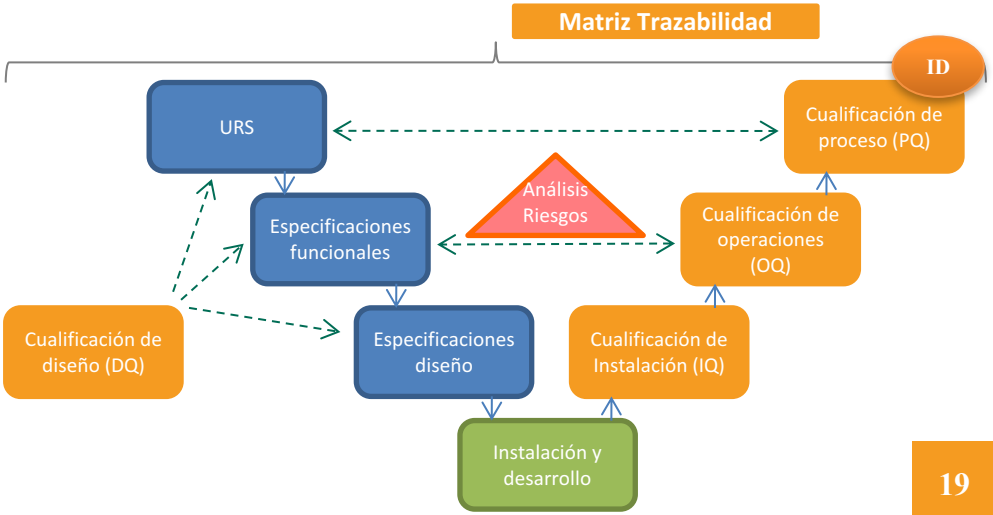
Gestión de la información

- Flujos de información.
- Gestión de datos maestros.
- Gestión del proceso.
- Gestión de registros.
- Controles en proceso.
- Audit trail.



Gestión de la información

- Procedimientos y formación.
- Ciclo de vida del dato.



Es necesario implantar una **política de auditoría** de cumplimiento de los requerimientos citados anteriormente, así como aplicar las medidas correctoras necesarias y realizar formación a todo el personal involucrado.

ITEM	SECCIÓN / REQUISITO	CUMPLE / NO CUMPLE	JUSTIFICACIÓN / COMENTARIOS
	1- A - ATRIBUIBLES Debe ser posible identificar la persona que realizó la tarea registrada. Demuestra el control de la acción por personal identificado, autorizado y capacitado. También aplica a los cambios realizados en los registros: correcciones, eliminaciones, cambios, etc.		
1.1	¿Se dispone de perfiles de seguridad que deperminen accesos y permisos otorgados a los usuarios?		
1.2	¿Cada usuario del sistema informatizado dispone de un código único que le identifica inequivocamente?		
1.3	¿Se dispone de algún procedimiento automático o manual para la asignación de contraseñas, control de características de las contraseñas y que fuerce el cambio de contraseña periodicamente?		
1.4	¿Se dispone de firmas electrónicas? ¿Se encuentran permanentemente ligadas al respectivo registro, disponen de un significado y han quedado registrada en fecha y hora ?		
1.5	¿Se dispone de audit trail para la configuración y registros críticos? ¿En el registro de auditoría de datos se muestra fecha, hora, usuario, valor antiguo, valor nuevo y motivo del cambio?		
	2- L - LEGIBLES Los datos y metadatos deben ser almacenados, evitando su deterioro o pérdida, durante todo el tiemo reglamentario de conservación. Deben estar fácilmente disponibles para el personal autorizado.		
2.1	¿Se controla el acceso a apartados de los sistemas informatizados y rutas de la infraestructura a través d ela definición de permisos?		
2.2	¿Existe un control para evitar la modificación de datos?		
2.3	¿Se dispone de un plan de copias de seguridad? ¿Se realizan simulacros de restauración de copias para verificar su validez y el protocolo?		

ATRIBUIBLES

Debe ser posible **identificar la persona** que realizó la tarea registrada.

Demuestra el control de la acción por personal identificado, autorizado y capacitado.

También aplica a los cambios realizados en los registros: correcciones, eliminaciones, cambios, etc.

- Código de usuario únicos e individuales.
- Perfiles de seguridad.
- Gestión de contraseñas: asignación, control tipos de contraseñas, cambios periódicos.
- Firmas electrónicas
- Audit trail.

LEGIBLES

Los datos y metadatos deben ser almacenados, evitando su deterioro o pérdida, durante todo el tiempo reglamentario de conservación.

Deben estar **fácilmente disponibles y entendibles para el personal autorizado**.

- Acceso limitado.
- Sin posibilidad de modificar datos almacenados.
- Copias de seguridad y restauración de datos.

SIMULTÁNEOS

El registro de los datos debe producirse en el **menor tiempo posible** desde su generación y sin el uso de soportes temporales intermedios.

- La fecha y la hora no se deben poder modificar.
- Registro on-line, en el punto de uso.
- Conexión con equipos de proceso.

ORIGINALES O COPIA VERIFICADA

El registro original puede ser descrito como la **primera captura de información**, ya sea grabada en papel o electrónicamente.

Concepto Copia Verificada: copia exacta y verificada de un registro original.

Se pueden considerar válidas.

- Tiene que ser el primer registro, el primer dato registrado.
- Para las operaciones críticas, no se deben combinar en una sola transacción del sistema con otras operaciones y registrar al final de una serie de actuaciones.
- Con el fin de asegurar la restauración de los datos. Es necesario realizar copias de datos originales antes de realizar cambios.

EXACTOS

Datos **precisos** que permitan la reconstrucción total de las actividades que han dado lugar a la generación de los mismos.

- Calibración de los equipos integrados con el sistema para la obtención de un dato correcto y preciso.
- Verificación del proceso de obtención de datos, procesamiento y registro para integraciones de sistemas por interfaces o comunicación con equipos.
- Gestión de desviaciones.
- Capacitación del personal.

COMPLETOS

Toda la información crítica para la reconstrucción **de un proceso** debe quedar registrada, incluyendo datos y metadatos relevantes.

Todos los datos, incluyendo cualquier repetición o reproceso se tiene que conservar.

- Control del registro completo de datos por proceso para que sea trazable.
- Deben registrarse todas las acciones, incluidas repeticiones o reprocesos.

CONSISTENTES

Todos las tareas del proceso tienen que constar.

- La secuencia seguida ha de corresponder en el tiempo.
- Los datos vinculados al registro deben ser correctos y coherentes.

PERDURABLES

Los datos deben permanecer **intactos y accesibles** como un registro permanente / duradero a lo largo de su tiempo de archivo.

- No se deben usar elementos de almacenamiento de datos temporales.

DISPONIBLES

Los registros deben estar **disponibles** para revisión en cualquier momento durante el **período de retención requerido**, accesible en un formato legible a todo el personal aplicable responsable de su revisión, ya sea para decisiones de liberación de rutina, investigaciones, tendencias, informes anuales, auditorías o inspecciones.

- Tiempo de archivo de datos: declarado, implantado y supervisado.
- Teniendo en cuenta que se deben conservar el periodo reglamentario, asegurando la estabilidad del soporte.
- Debe registrarse por dato el sistema informatizado que lo genera y el que lo mantiene almacenado a lo largo del tiempo de archivo.

¡Gracias por su atención!

OQOTECH SL
902 995 129
info@oqotech.com

Centro de Desarrollo
Calle Capellà Belloch, 11
03801 Alcoy – Alicante

Delegación Valencia
Plaza Conde de Carlet, 3
46003 Valencia

Delegación Madrid
Calle Príncipe de Vergara, 55
28006 Madrid