



Integridad de datos y Buenas Prácticas de Documentación



Temario:

1. Marco Regulatorio

1.1 MHRA, FDA, PICS y WHO

2. ¿Cuándo aplica la integridad de datos ?

3. ALCOA ++ para integridad de datos

3.1 tipo de datos: Dato crudo, metadato, Audit trail

4. Garantizando la integridad de datos

4.1 Capacitación, calificación de personal

4.2 Detectando riesgos y GAPS

4.3 Compromiso y liderazgo

4.4 Estructura y gobernanza

5. Lista de Verificación Para Integridad de Datos

6. Análisis de riesgos de integridad de datos para el laboratorio analítico

7. Tendencias de integridad de datos

8. Buenas Prácticas de documentación

8.1 El porqué de las BPD y definiciones principales

8.2 Marco regulatorio de BPD

8.3 Sistema de documentación. Elaboración y control de la documentación

8.4 Registros de datos de calidad

8.5 Resguardo de la documentación



Marco Regulatorio



Las agencias regulatorias emiten los lineamientos mínimos a cumplir para demostrar la Integridad de Datos.

Publicando reportes, guías, normas.

- ❖ MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018
- ❖ Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments – PIC/S; PI041-1(draft 2); August 2016
- ❖ Data Integrity and Compliance With CGMP Guidance for Industry FDA, 2016
- ❖ CFR 21 Parte 210, 211
- ❖ ICH Quality Risk Management Q9
- ❖ Reporte OMS 48, 50



Guías de referencia



Definiciones GMP
DI y orientación
para la industria
farmacéutica
Marzo de 2015



Integridad de
datos y
cumplimiento de la
guía GXP para la
industria
farmacéutica
CFR 21 Part 11
Guía ALCOA ++



**Directriz sobre
integridad de datos**

1. ALCOA ++
2. Audit Trail
3. Respaldo de
datos
4. Gobernanza
5. Firmas
electrónicas
6. Riesgos de ID



Guía práctica
basada en riesgos
para la gestión de
DI



Buenas prácticas
para la gestión e
Integridad de
datos en entornos
regulados
GMP/GDP



GUIAS REGULATORIAS PARA INTEGRIDAD DE DATOS

FDA ALCOA

1. ATRIBUIBLE
2. LEGIBLE
3. CONTEMPORANEO
4. ORIGINAL
5. ACCURATE (EXACTO)

CFR 21 Parte 11

1. ASEGURAR LA VALIDACIÓN DE LOS SISTEMAS
2. ASEGURAR LA PROTECCIÓN DE LOS REGISTROS
3. ASEGURAR LA MARCA DE TIEMPO DEL AUDIT TRAIL
4. ASEGURAR EL USO AUTORIZADO DE CONTRASEÑAS
5. ASEGURAR EL ACCESO LIMITADO A LOS SISTEMAS
6. ASEGURAR EL ACCESO LIMITADO A LOS DOCUMENTOS
7. ASEGURAR LA CAPACITACION A EMPLEADOS

MHRA Integridad de Datos

1. COMPORTAMIENTO ETICO DE TODOS LOS PROFESIONALES
2. CREAR CONTRASEÑAS SEGURAS
3. GARANTIZAR EL ACCESO AUTORIZADO A LOS SISTEMAS

GUIAS REGULATORIAS PARA INTEGRIDAD DE DATOS



Las guías mantienen estructura en tres grandes rubros

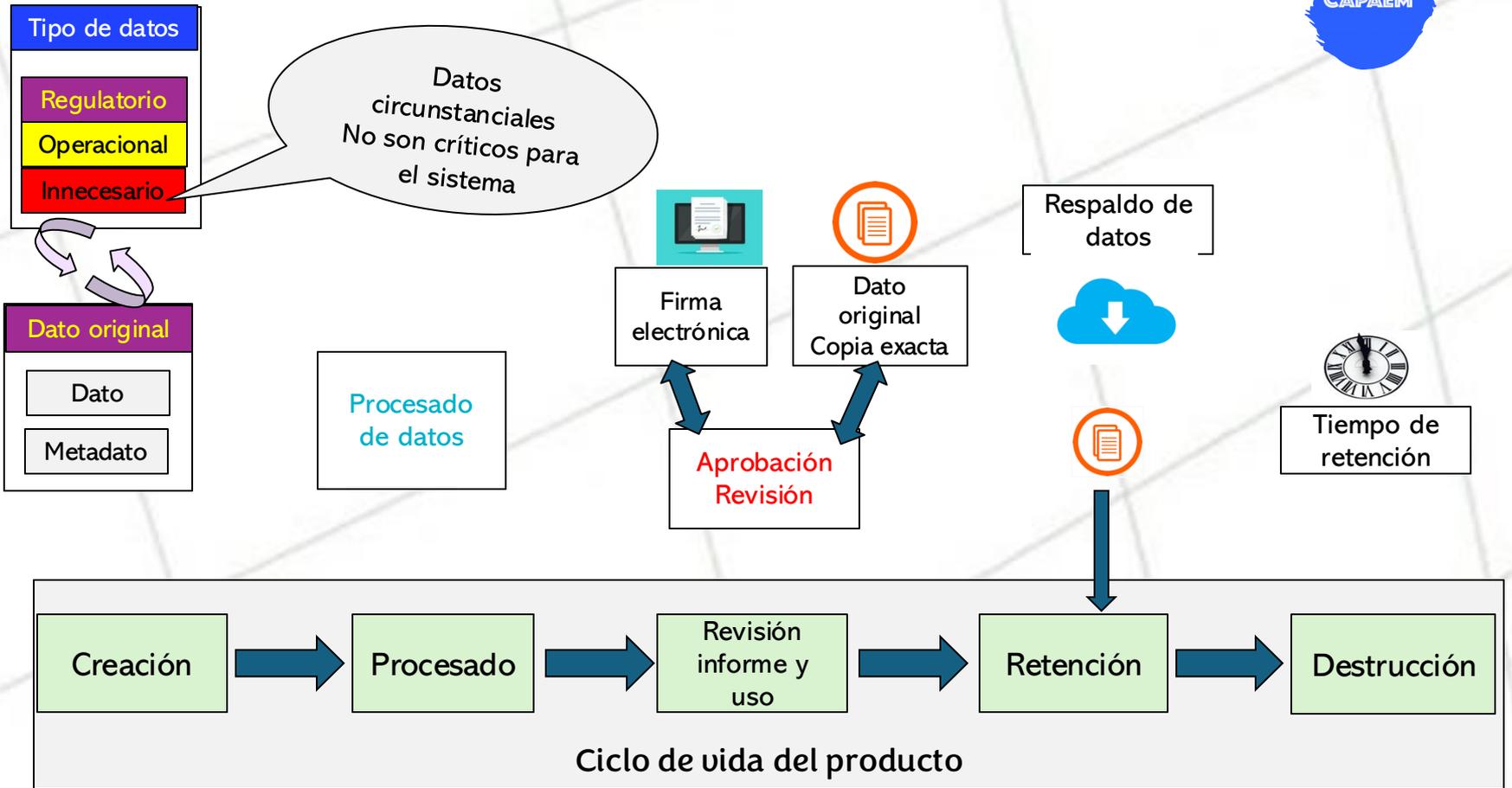
1a. Parte. Incluye las disposiciones generales, definiciones generales y **tipos de registros**.

2a. Parte. Sección de registros electrónicos, necesidad de **firmas en los registros, los sistemas computarizados** deben garantizar la exactitud, fiabilidad y coherencia de los datos introducidos y procesados. Restricciones de acceso a través de identificación y contraseñas.

3a. Parte. Énfasis en las firmas electrónicas y el control, cómo los cambios periódicos de contraseñas.



¿ Cuándo Aplica la Integridad de Datos ?



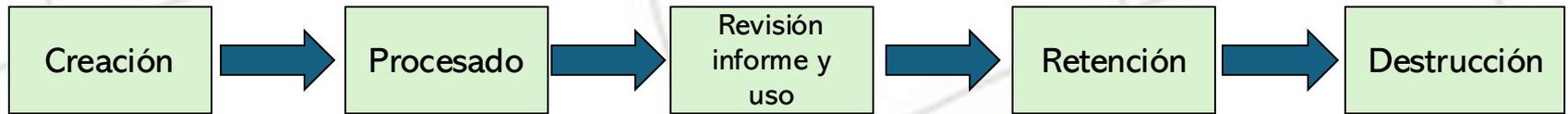
Audit trail

Se debe tener control de los datos + los metadatos ligados al proceso durante todo el ciclo de vida del producto

¿ Cuándo ?



Integridad de datos durante todo el ciclo de vida



- ❖ ¿ Cómo y dónde se crean los datos? (papel vs electrónico o híbrido)
- ❖ ¿ Qué metadatos están asociados a los datos ?
- ❖ ¿ Es posible modificar o eliminar los datos originales ?
- ❖ ¿ Cómo se transfieren los datos (flujo de datos) a otros lugares ?

- ❖ ¿ Cómo se procesa los datos?
 - Métodos a probados y codificados
- ❖ ¿ Cómo se registra el proceso de datos?
 - Registrar el proceso de transferencia de datos
- ❖ ¿ Influye el procesado en la presentación del informe de resultados?
 - Posible impacto por ejemplo: Estadística

- ❖ ¿ Qué datos estoy revisado, datos originales, copia certificada, datos no controlados?
 - ❖ ¿ El revisor tiene acceso a todos los datos?
 - Incluyendo los no válidos y pruebas de control
 - ❖ ¿ Cuándo se toma la decisión de pasa no pasa?
 - Asegurarse de que los datos están almacenados de manera fija y no pueda haber manipulación de datos (intencionales y no intencionales)

- ❖ ¿Dónde están almacenados los datos?
- ❖ ¿Cómo están protegidos de accesos no autorizados?
 - ❖ ¿ Se realiza back-up?
 - ❖ ¿ Se almacenan los datos según su periodo de retención ?
 - ❖ ¿Se verifica el back-up periódicamente ?

- ❖ ¿Ha expirado el periodo de retención de los datos?
 - ❖ ¿Es todavía válido el tiempo de retención inicialmente definido?
 - ❖ Cómo se autoriza la eliminación/destrucción de los datos?
 - ❖ ¿ Cómo se ejecuta y verifica la eliminación/destrucción de datos?



¿ Qué busca
la autoridad,
Qué se espera
del usuario ?

Se debe poder
responder a las
siguientes
preguntas:

¿ Quién ha realizado la acción ?
¿ Cuándo se realizó la acción ?
¿ Quién ha modificado el
registro?
¿ Porque se ha modificado el
registro ?
Enlace con el dato original

¿ En qué tipo de registros es aplicable la integridad de datos ?



- ¿ En registros en papel en formatos ?
- ¿ En los registros electrónicos ?

Respuesta: Ambos

Son mandatorios para registros manuales en formatos y electrónicos

Integridad de datos y BPD

CAPAEM

Tipos de datos regulatorio/operacional

Registro Original

Es el registro original el cual es capturado por primera vez ya sea electrónico o manual

Registro completo realizado al momento de hacer la actividad en formatos, fotografías, impresiones o medios electrónicos, **debe cumplir con las BPD**

Fuente de datos

Esta terminología se utiliza con fines de investigación clínica. Los datos de origen son los mismos que los datos sin procesar (propósito de investigación de laboratorio). Los datos de origen incluyen registros originales de observación e investigación clínica. Revisión de datos fuente por parte del patrocinador y la FDA para determinar la seguridad, calidad e integridad (ALCOA++).

Metadatos

Datos que indican atributos de otros datos y dan referencia y significado de esos otros datos, **descritos como datos asociados a datos**. Los datos generados automáticamente por la fuente de datos original también se consideran metadatos.

Audit Trail

Forma de metadatos que contiene información sobre la creación, alteración o eliminación de un registro en un entorno GXP. Este es el medio que incluye quién, qué, cuándo y por qué cronológicamente se realizó la acción. El sistema computarizado responsable de la generación de datos sin procesar siempre se vincula con una liga de auditoría para identificar la modificación en los datos al retener tanto los datos modificados como los datos originales.

Integridad de datos y BPD

¿ En qué tipo de datos aplica la integridad de datos ?

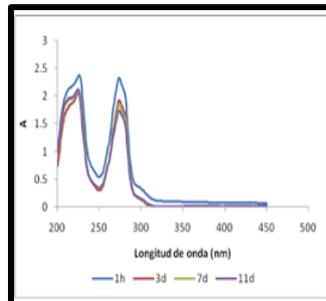


Registro Original manual



Registro original
llevado a cabo de manera **manual** en un formato

Registro original electrónico

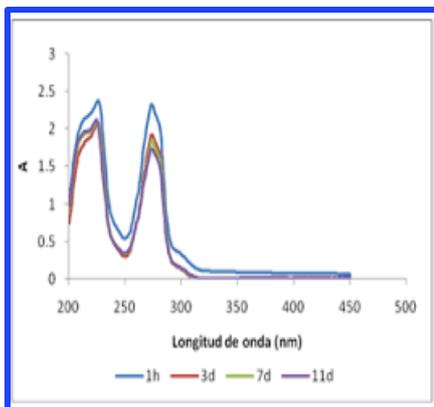


Registro Original
Espectrograma UV
Registro original encriptado por el **sistema** junto con datos asociados de identificación de muestras, analista, fechas, etc. (**Metadatos**).

Metadatos en sistema de HPLC

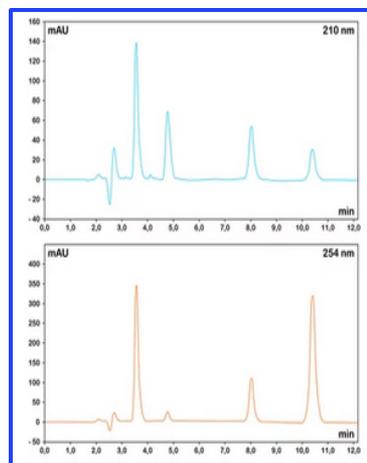


Registro Original
Espectrograma UV
+ Datos de
identificación de
muestra



Datos originados por la fuente de manera automática también se consideran **Metadatos**

Datos que se pueden
modificar. **PNO**
integración
cromatográfica



Cálculo de área bajo
la curva

Metadato
Audit trial

Refleja Cambios
realizados

¿Quién?

¿Cómo?

¿Cuándo?

Niveles de acceso
por usuario

Fecha y hora

Equipos heredados
que no contemplan
Audit Trial, se deben
considerar acciones
de mitigación **AR**



Audit Trial

Cambios rastreados, cambios que registra el módulo

Cambiar	Descripción
Objeto creado	Se crea el objeto auditado.
Valor inicial asignado	Se asigna un valor inicial al objeto auditado antes del primer guardado.
Objeto cambiado	Se cambia la propiedad del objeto auditado.
Objeto eliminado	El objeto auditado se elimina.
Agregado a la colección	El objeto auditado se agrega a una colección.
Eliminado de la colección	El objeto auditado se elimina de una colección.
Objeto de colección cambiado	Se cambia un objeto del objeto auditado.
Objeto agregado <u>modificado</u>	Se cambia un objeto agregado con el objeto auditado.
Datos personalizados	Los datos personalizados se agregan al registro de auditoría.



Metadatos de Indexación

Validación de un método de análisis por cromatografía líquida de alta resolución para determinar quercetina en *Allium shoenoprasum* Regel & Tiling (cebollín)

PROYECTO	ELEMENTOS DE METADATOS BD	METADATOS PARA EL DOCUMENTO
1.	Título	Título del documento Validación de un método de análisis por cromatografía líquida de alta resolución para determinar quercetina en <i>Allium shoenoprasum</i> Regel & Tiling (cebollín)
2.	Creador/a	Nombre de autor/a, institución, país Pesantes Domínguez; Cuba
2.	Creador/a	Nombre de autor/a, institución, país Katherine Pesantes, Cuba
2.	Creador/a	Nombre de autor/a, institución, país
2.	Creador/a	Nombre de autor/a, institución, país
3.	Materia	Disciplina(s)
3.	Materia	Palabra/s clave <i>Allium schoenoprasum</i> L (cebollino); validación de métodos análisis; HPLC
4.	Descripción	Resumen Introducción: las especies del género <i>Allium</i> como la cebolla, el ajo, el puerro y el cebollino son reconocidos

Audit Trial
Cambios rastreados, cambios que registra el módulo

Acción	Descripción
Dato creado	Se crea el objeto auditado.
Valor inicial asignado	Se asigna un valor inicial al dato auditado antes del primer guardado.
Dato cambiado	Se cambia la propiedad del objeto auditado.
Objeto eliminado	El objeto auditado se elimina.
Agregado a la colección	El objeto auditado se agrega a una colección.
Eliminado de la colección	El objeto auditado se elimina de una colección.
Objeto de colección cambiado	Se cambia un objeto del objeto auditado.
Objeto agregado <u>modificado</u>	Se cambia un objeto agregado con el objeto auditado.
Datos personalizados	Los datos personalizados se agregan al registro de auditoría.



ATRIBUTO	REQUERIMIENTO
A tribuible	Debe ser posible identificar a la persona que realizó el registro de datos. El originador se identifica de manera única (usuario o Sistema). Metadatos Asociados al dato.
L egible	Todo registro debe ser legible y permanente. Accesible durante todo el ciclo de vida. Dato original y modificaciones visibles.
C ontemporáneo	La evidencia de la acción, evento o decisión debe ser registrada en el momento en que se realiza la actividad
O riginal	El registro original puede ser descrito como la primera captura de información. Copia exacta del original
A ccurance (Preciso)	Los datos son correctos, veraces, válidos y fiables

ALCOA +



ATRIBUTO	REQUERIMIENTO
C ompleto (Complete)	Se debe tener toda la información requerida para recrear y entender un evento. Incluyendo cualquier repetición o reanálisis se encuentra registrada.
C onsistente (Consistent)	Todos los registros se encuentran fechados o cuentan con registro de hora en la secuencia esperada.
D uradero (Enduring)	Los registros deben existir en forma adecuada durante el tiempo de retención del registro, en forma intacta y accesible. Por ejemplo: en bitácoras de laboratorio o registros electrónicos
D isponible (Available)	Los registros deben estar disponibles para ser auditados durante todo su ciclo de vida.

El principio añadido - *Traceable* (Trazable) **ALCOA ++**

La información debe ser trazable durante todo su ciclo de vida, y los cambios que se realicen deben ser registrados como parte de los metadatos (por ejemplo, Audit Trail).



El generador del dato se identifica de manera única (usuario o sistema)
Asociado al dato

La información debe ser trazable durante todo su ciclo de vida, y los cambios que se realicen deben ser registrados como parte de los metadatos

Los registros deben estar disponibles para ser auditados durante todo su ciclo de vida.

Legible y permanente
Accesible durante todo el ciclo de vida
Dato original y modificaciones legibles

Los registros deben existir en forma adecuada durante el tiempo de retención del registro, en forma intacta y accesible. Por ejemplo: en bitácoras de laboratorio o registros electrónicos



Observado y registrado en el momento que se realiza la actividad

El dato original es el primero registrado/copia exacta del original

Los registros deben estar disponibles para ser auditados durante todo su ciclo de vida.

Se debe tener toda la información requerida para recrear y entender un evento. Incluyendo cualquier repetición o reanálisis se encuentra registrada.

Los datos son correctos, veraces, válidos y fiables

➤ Todos los datos y metadatos, incluyendo las repeticiones o reanálisis



Atribuible

El originador del registro se identifica de manera única

Problema de integridad de datos:

- Datos originales no firmados
- Compartir usuario/password de un sistema electrónico
- No poder identificar el equipo con el que se ha registrado un dato (aplicable a correcciones)

¿ Por qué es importante	Riesgo	Mitigación
<p>Dato trazable a la persona que lo ha generado</p> <p>Los usuarios deben estar capacitados para acceder a los sistemas</p>	<p>Debe existir un vínculo único y seguro entre el originador y el dato</p> <p>Se puede requerir de un procedimiento híbrido para sistemas que no tengan firma electrónica</p> <p>Incumplimiento de 21 cfr parte 11 (Electronic records)</p>	<p>Sistemas electrónicos:</p> <p>Usuarios únicos (no compartir claves de acceso a usuarios genéricos)</p> <p>Firmar y fichar cuando se registra un dato</p> <p>Firmar y fechar los informes</p>

Legible

Todas las actividades deben poder ser reconstruidas por los revisores, en cualquier momento y durante el período de retención del dato

Problema de integridad de datos:

- Los metadatos no son legibles
- Se han modificado datos y no se ve el dato anterior
- Se cambia una versión del sistema y no se pueden recuperar datos de versiones anteriores

¿ Por qué es importante	Riesgo	Mitigación
Permite a las personas que revisan el registro comprender plenamente todas las actividades durante todo su período de revisión. Los datos ilegibles generan desconfianza.	Necesidades de asociar todos los cambios de los datos a las personas que realizan esos cambios Audit Trail incompleto Segregación de funciones entre los usuarios y los administradores del sistema	Papel: Tinta permanente Archivar la documentación en un lugar de acceso controlado Electrónico: Audit Trail con fecha y hora Validación Política de retención de datos y documentos



Contemporáneo

Los datos se deben registrar en el momento en que se generan

No se deben mantener en la memoria

Problema de integridad de datos:

- Que se pueda modificar la fecha/hora en el software
- Que se anoten los datos en una libreta y posteriormente se transcriban

¿ Por qué es importante

La retrospectión puede llevar a confusión y generar errores
Los borradores se pueden modificar

Riesgo

Puede generar errores
Desconfianza en auditores
Permite la modificación no controlada del dato

Mitigación

Capacitación: Los datos deben registrarse en el momento de realizar la operación.
Revisar el acceso de los usuarios mantener control sobre estos.
Papel: PNOs definidos
Electrónico: Registro seguro de día/hora que no pueda ser modificado por el usuario





Original

Los datos se deben ser originales y completos

Problema de integridad de datos:

- Descartar los datos originales y mantener solamente los datos procesados
- Realizar un reporte de unos datos dinámicos y considerarlo como el dato original
- Realizar una ejecución de un formato en papel y una vez escaneado descartar el papel.

¿ Por qué es importante	Riesgo	Mitigación
El dato se puede perder o ser incompleto Puede haber errores de transcripción	Revisar las decisiones basadas en el riesgo a partir de la revisión de los datos originales Realizar un examen basado en los riesgos de los datos originales y los metadatos relevantes Retención y revisión de los registros originales frente a las copias certificadas	Revisión y aprobación adecuada de los datos originales en papel Utilizar formatos estandarizados Reportar la revisión de los datos y metadatos relevantes Establecer las acciones para datos erróneos (OOS) en PNOs



Exacto

Los datos son correctos, veraces, válidos y confiables

Problema de integridad de datos:

- Realizar un análisis con equipos/reactivos/patrón que no estén en estado de validez
- Ante una desviación no realizar correctamente el análisis de causa raíz

¿ Por qué es importante	Riesgo	Mitigación
Los datos exactos proporcionan la base para una buena toma de decisiones científicas	Obtener datos incorrectos	Procedimientos, procesos, sistemas y control adecuados que componen el SGC Calibración, calificación, validación de sistemas computacionales. Investigar los resultados fuera de especificaciones (OOS)

Registros en papel



Generar registros

- ✓ Formularios con un código único de identidad
- ✓ Almacenamiento controlado
- ✓ Espacio para registro manual
- ✓ Clara definición del dato requerido

Formularios

- ✓ Control de espacios en blanco
- ✓ Copias controladas
- ✓ Conciliación

Registros en papel



Distribución controlada

- ✓ Copias controladas
- ✓ Retirar obsoletos y destrucción controlada
- ✓ Solamente tener disponible la versión vigente

Completar registros

- ✓ Registrar quién ejecuta la operación
- ✓ No dejar espacios en blanco
- ✓ Identificar fecha/hora/firma

Registros en papel



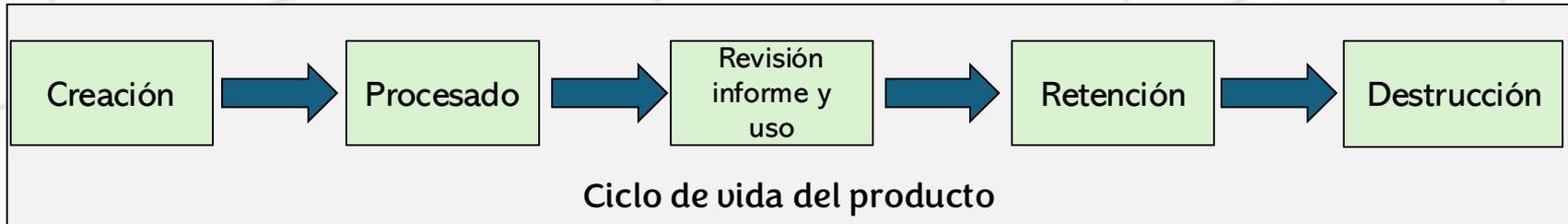
Verificación

- ✓ Revisado y aprobado
- ✓ Fecha/firma
- ✓ Revisión de datos críticos

Archivo

- ✓ Protección contra fuego, agua, plagas
- ✓ Organización para poder recuperar los documentos

Registros electrónicos: Audit trail



- ✓ El Audit Trail es un registro electrónico seguro, generado automáticamente y contiene el registro de fecha y hora, que permite la reconstrucción del curso de los eventos relacionados con la creación, modificación o la eliminación de un registro electrónico.
- ✓ Registra los cambios en el registro de los datos a nivel de sistema
 - ✓ ¿Quién?
 - ✓ ¿Cuándo?
 - ✓ ¿Qué?
 - ✓ ¿Por qué?

El objetivo es tener la trazabilidad del registro

Ejemplo: Sistema HPLC



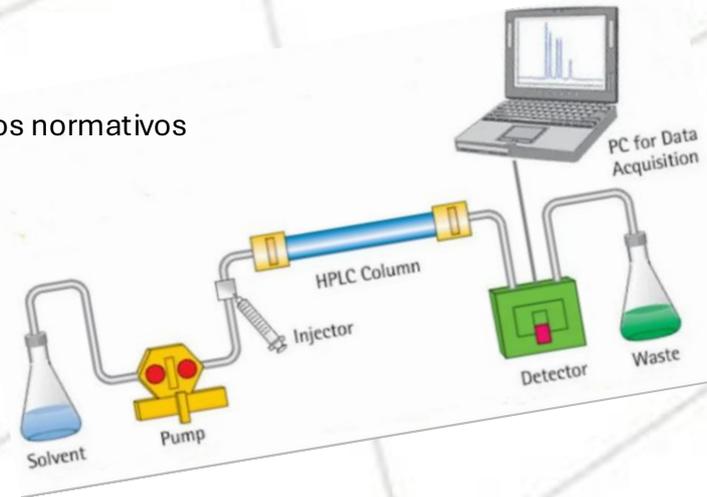
Dato:

- ✓ Usuario, fecha y hora de análisis
- ✓ Método y parámetros de integración
- ✓ Secuencia de inyección asociada
- ✓ Condiciones de reintegración, incluyendo la razón del cambio

Sistema:

- ✓ Intentos de acceso al sistema (Dato irrelevante)
- ✓ Cambio de nombre o borrado de ficheros
- ✓ Fecha de creación/modificación del registro

Datos normativos



Datos normativos

¿ Con que frecuencia se debe realizar el Audit Trail ?



- ✓ FDA recomienda que el Audit Trail de datos críticos se revisen con cada registro y antes de la aprobación final del registro (Ejemplo: Dictamen)
- ✓ Las revisiones periódicas del Audit Trail deben incluir lo siguiente:
 - El historial de cambios de los resultados de las pruebas de productos terminados, los cambios en las secuencias de ejecución de muestras, los cambios en la identificación de la muestra y los cambios en los parámetros críticos del proceso
 - La periodicidad dependerá de la complejidad del sistema y su uso previsto

PNO que describa los criterios de revisión del Audit Trail

¿ Quién debe realizar el Audit Trail ?



- ✓ El Audit Trail forma parte del dato, por lo que el personal responsable de la revisión de registros en un ambiente GMP debe revisar también el Audit Trail

Ejemplo:

Los registros de producción y control, que incluyen Audit Trail deben ser revisados y aprobados por la unidad de calidad (aplica a registros electrónicos como en papel)

Funcionamiento de sistemas, la unidad de IT
(CFR 211.192)

¿ Registros electrónicos:
Audit Trail?



Tres tipos principales de revisión de seguimiento del Audit Trail

Revisión del Audit Trail como parte de la revisión y verificación normal de datos

Revisión del Audit Trail de un conjunto de datos específicos durante una investigación por ejemplo: en CAPAS.

Revisión y verificación de la funcionalidad efectiva del Audit Trail ejemplo: Verificación de la configuración del seguimiento de auditoría como parte de la revisión periódica del sistema

1. Definir PNO y responsabilidades
2. Documentar la revisión del Audit Trail

¿ Registros electrónicos: Audit Trail?



Tres tipos principales de revisión de seguimiento del Audit Trail

% Impurezas HPLC

- El certificado forma parte del certificado de análisis y condicionarán la liberación del lote
- **Audit Trail:**
El responsable de la revisión aprobación revisa el Audit Trail antes de dar el dictamen

¿Qué revisar?

Integración manual, reintegraciones, recálculos, borrado o modificación de ficheros

Bitácora de calibración de instrumento

- Se registran las calibraciones periódicas y actuaciones que se realizan para un determinado instrumento analítico
- **Audit Trail:**
Dependiendo de la frecuencia de uso y de la criticidad de los análisis realizados con dicho instrumento (análisis de riesgos) se definirá la periodicidad de revisión de la bitácora.

Sistema de gestión de pesadas

Registro de pesadas para la medición destinada a un ensayo clínico

Audit Trail

Se debe revisar antes de la liberación del medicamento

¿Qué revisar?

Envases, pesos, pesos rechazados, autorización de usuarios, fechas de preparación de muestras

Registros electrónicos: 21 CFR P11/ANEXO 11

Sistema Cerrado

- Identificar registros no válidos o alterados
- Protección de registros ante modificaciones o borrado
- Copias legibles completas
- Retención de datos
- Flujo de pasos en el sistema

ATRIBUIBLE
LEGIBLE

Sistema abierto

- PNO para garantizar autenticidad, integridad y confidencialidad
- Encriptación de datos
- Firma controlada
- Control para la autenticidad, integridad y confidencialidad de los datos

ATRIBUIBLE
ORIGINAL

Entrada de datos con dispositivos

- Existen PNOS para su uso
- El sistema identifica y valida la información de un determinado dispositivo

EXACTO

CAPAEM

Registros electrónicos: 21 CFR P11/ANEXO 11

Acceso al sistema

- Acceso limitado a las personas autorizadas
- Sistema de comprobación de la autenticidad del acceso

ATRIBUIBLE

Identificación y contraseña

- Relación única usuario/contraseña
- Identificación de accesos no autorizados
- Revisión periódica de contraseñas
- Activar/desactivar usuarios
- Confidencialidad de accesos
- Dispositivos de control de pérdida de datos

ATRIBUIBLE

CAPAEM

Registros electrónicos: 21 CFR P11/ANEXO 11

Audit Trail

- No puede alterarse, activar/desactivar
- Usuario/fecha/hora/valor original y nuevo valor
- Verificable
- Accesible durante todo el ciclo de vida del dato

ATRIBUIBLE
LEGIBLE
CONTEMPORÁNEO
ORIGINAL

PNOs y capacitación

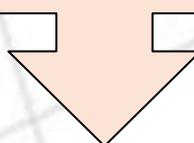
- Registro de capacitación
- PNO que defina: uso, integridad y confidencialidad de los datos
- Control de cambios de los PNOs
- Gestión de cambios

ATRIBUIBLE
LEGIBLE
ORIGINAL

CAPAEM

Registros electrónicos: 21 CFR P11/ANEXO 11

Firma electrónica



- Contener nombre, fecha/hora/razón
- Mismos controles que los registros electrónicos
- Presente en las copias del registro (papel, electrónico)
- Asociada inequívocamente al registro
- única e individual
- Doble identificación (usuario+ contraseña, usuario + biometría)

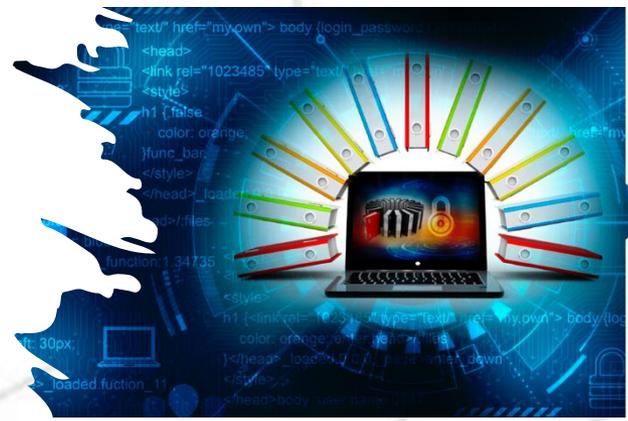
ATRIBUIBLE
LEGIBLE
CONTEMPORÁNEO
ORIGINAL



CAPAEM



Garantizando la integridad de datos





Cuatro puntos para garantizar la integridad de datos

1. Capacitación, calificación de personal, comunicación y colaboración

2. Detectando riesgos y GAPs de integridad de datos



Cuatro puntos para garantizar la integridad de datos



3. Compromiso y liderazgo



4. Estructura y gobernanza

1.0

Capacitación y calificación de personal



Capacitación:

- PNOs, Instructivos Políticas Inducción, Onboarding
- Manual de calidad, Objetivos de Calidad
- Buenas Prácticas de Documentación



2.0 Detectando riesgos y GAPS de integridad de datos

La integridad puede verse comprometida cada vez que los datos se **replican o transfieren** deben permanecer intactos e inalterados .



Sistema de auditorías
Sistema CAPA
Tendencia de datos
Gestión de riesgos
Mejora continua
Mapeo de procesos



Señales potenciales de fallas de ID/Tendencia de datos CC-AC

Los controles en proceso están bien, pero los resultados finales de las pruebas están fuera de tendencia (OOT) o fuera de especificaciones (OOS)



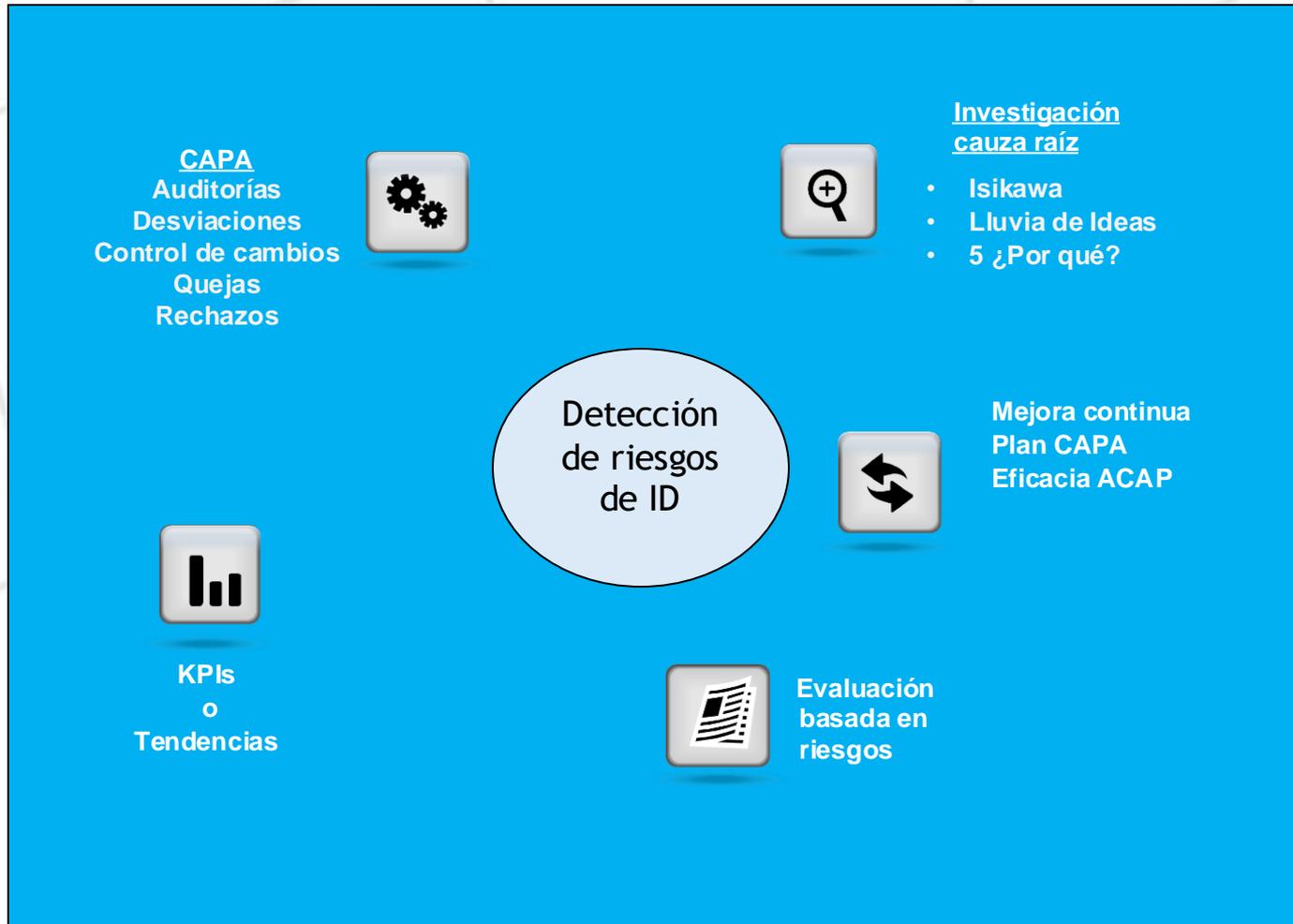
Los resultados del control de calidad son correctos, pero los indicadores de estabilidad fallan



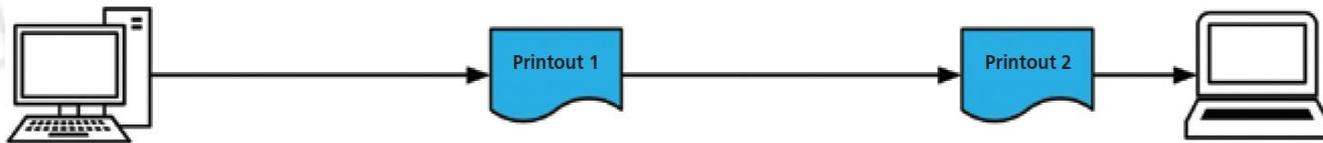
Investigaciones repetidas debido a información faltante o incorrecta en los registros de lotes



2.0 Detectando riesgos y GAPS de integridad de datos



Ejemplo de uso de mapeo de procesos para identificar Gaps y riesgos en integridad de datos en proceso de HPLC híbrido



Contraseña de usuario
Niveles de usuario
Usuario Key
Encriptación de metadatos
Identidad de muestras y referencia

Integración de picos para cálculo del área bajo la curva
PNO ?



Validación de hoja de cálculo ?



Contraseña de usuario
Niveles de usuario
Usuario Key
Firma electrónica
Validación del LIMS

La integridad puede verse comprometida de varias maneras. Cada vez que los datos se replican o transfieren deben permanecer intactos e inalterados .

Principales vulnerabilidades identificadas en proceso de HPLC

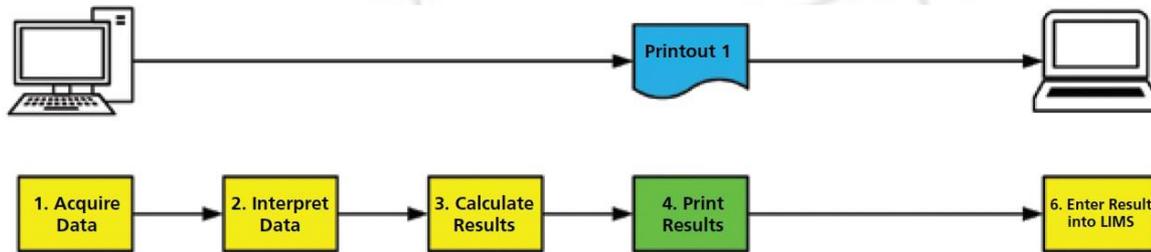


Etapa del proceso	Vulnerabilidad del registro de datos (Riesgos)
1. Adquisición de datos	<ul style="list-style-type: none"> • Sin atribución de acción: todos los usuarios comparten una cuenta • Conflicto de intereses: todos los usuarios son administradores • sistema independiente • La copia de seguridad la realizan los usuarios del laboratorio. • Entrada manual de datos de estándar y preparación de muestra, como: Identidad, número de lote, pesos de muestra y diluciones.
2. Interpretación de datos	<ul style="list-style-type: none"> • Sin atribución de acción: todos los usuarios comparten una cuenta • No hay PNO para la integración • No hay control sobre la integración manual
3. Impresión de áreas de picos	<ul style="list-style-type: none"> • El laboratorio considera el papel como datos originales • Riesgo de que los registros en papel y electrónicos sean diferentes
4. Transcripción a hoja de cálculo	<ul style="list-style-type: none"> • Errores tipograficos al transcribir datos • Hojas de cálculo no validadas
5. Impresión de hoja de calculo	<ul style="list-style-type: none"> • Falla al guardar el archivo de la hoja de cálculo • No registrar la firma que ligue el cumplimiento con CFR parte 11 • Puede re-ingresar todos los datos en nueva hoja de cálculo
6. Introducción de resultados a LIMS	<ul style="list-style-type: none"> • Errores tipográficos • Segunda persona revisora solamente revisa los registros en papel

Uso de mapeo de procesos para identificar Gaps y riesgos en integridad de datos en proceso de HPLC híbrido



Solución a mediano plazo



Contraseña de usuario
Niveles de usuario
Usuario Key
Encriptación de metadatos
Identidad de muestras y referencia

Integración de picos para cálculo del área bajo la curva
PNO ?

Impresión de resultados
Usuario introduce a LIMS



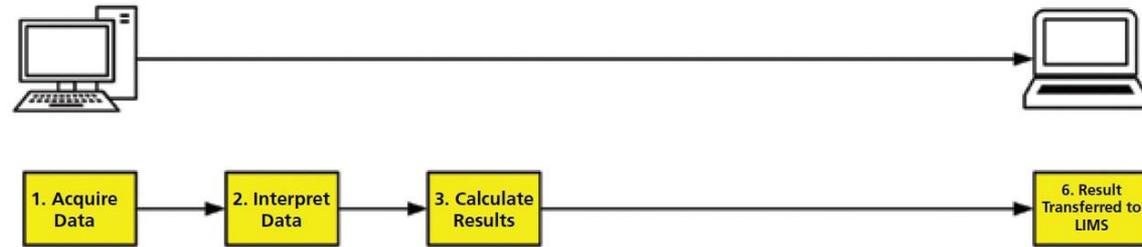
Contraseña de usuario
Niveles de usuario
Usuario Key
Firma electrónica
Validación del LIMS

La integridad puede verse comprometida de varias maneras. Cada vez que los datos se replican o transfieren deben permanecer intactos e inalterados .

Uso de mapeo de procesos para identificar Gaps y riesgos en integridad de datos en proceso de HPLC híbrido



Solución a largo plazo



Contraseña de usuario
Niveles de usuario
Usuario Key
Encriptación de metadatos
Identidad de muestras y referencia

Integración de picos y cálculos de ensayo

Transferencia de resultados a LIMS

La integridad puede verse comprometida de varias maneras. Cada vez que los datos se replican o transfieren deben permanecer intactos e inalterados .

3. Compromiso y liderazgo Alta dirección



- Planificación de la calidad
- Proporcionando recursos
- Programa de seguridad
- Reconocimiento al personal
- Evaluación de personal
- Programas de desarrollo de personal
- Define prioridades



3. Comunicación y Colaboración



Responsabilidad de la alta dirección:

Establecer políticas de comunicación

Seguimiento a métricas (Revisión por la dirección)

Feedback a partes interesadas internas

Encuestas de cultura de calidad

Proporcionar recursos

Patrocinio Ejecutivo



Factores Críticos de Éxito

En la terminología de la FDA se solicita a la alta dirección con autoridad ejecutiva que:

- Promueva la causa de integridad de datos
- Proporcione recursos
- Asigne prioridades
- Garantice que la expectativa de integridad de datos se lleve a cabo en todos los niveles de la organización

La MHRA declara en su guía que:
El sistema de gobernanza de datos debe ser parte integral del sistema de gestión de calidad de la organización



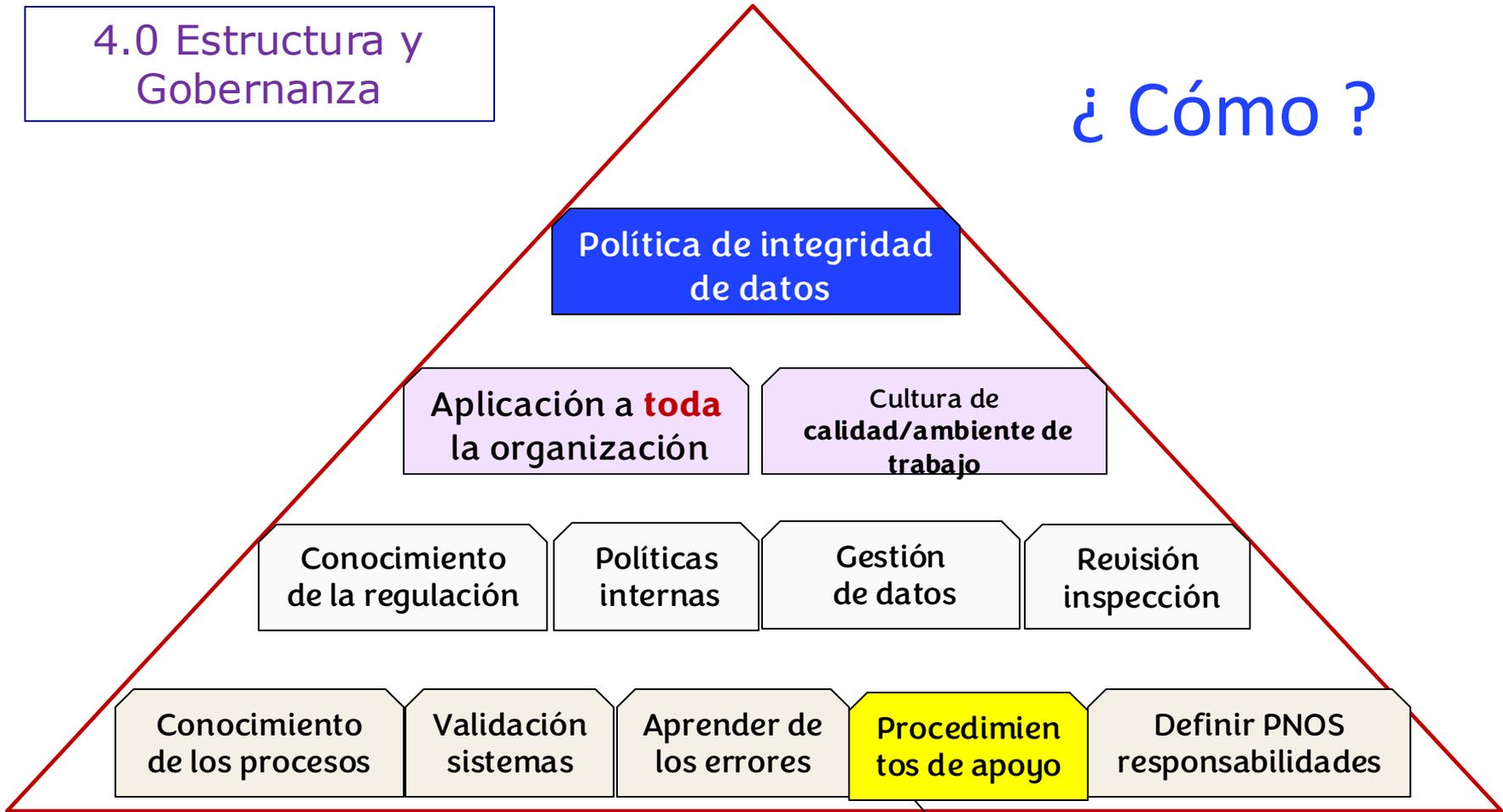
4.0 Estructura y Gobernanza

La gobernanza de datos describe los roles, los procesos y las políticas que las **organizaciones** promulgan para garantizar la exactitud, calidad y seguridad de los datos. Sus políticas dictan los métodos que las personas pueden usar para acceder a los datos y aprovecharlos.

La administración de datos es la implementación de esos procedimientos. Las personas asignadas con responsabilidades de administración de datos gestionan y supervisan los procedimientos y las herramientas usadas para gestionar, almacenar y proteger los datos.

4.0 Estructura y Gobernanza

¿Cómo?



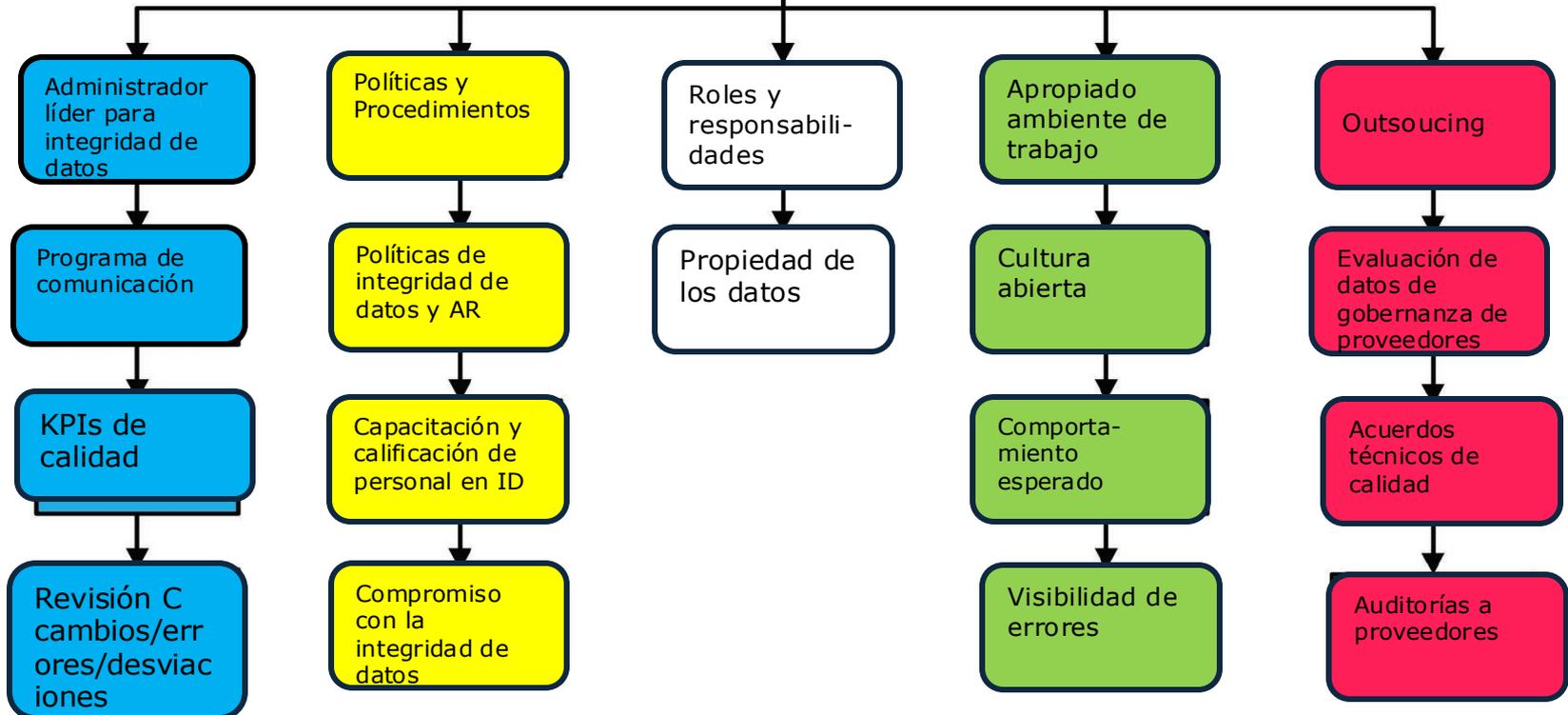
Control de cambios
CAPA
Sistema de AR





La gobernanza de datos

La alta dirección define prioridades, proporciona recursos, rompe la Resistencia organizacional al cambio.





Comité Técnico

Formado por los líderes funcionales y supervisores de la organización.

Las partes interesadas de cada una de las áreas funcionales clave deben estar representadas en el comité técnico.

AREA	PROCESO	RESPONSABLE
PRODUCCIÓN		
CONTROL DE CALIDAD		
ALMACENES		
VALIDACIÓN		
SEGURIDAD E HIGIENE		
MANTENIMIENTO		
SERVICIOS TECNICOS		
ASEGURAMIENTO		
MICROBIOLOGÍA		
RECURSOS HUMANOS		
SISTEMA DE GESTIÓN DE CALIDAD		
DOCUMENTACIÓN		

Lista de verificación de integridad de datos



LISTA DE VERIFICACIÓN DE INTEGRIDAD DE DATOS



No.	Pregunta	Respuesta (Sí, No, N/A)	Impacto	Plan de Mitigación
Seguridad y Control de Acceso				
1.	¿Se controla el acceso al sistema a través de credenciales de inicio de sesión únicas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	¿Existe un proceso definido y documentado para el control de acceso de los usuarios?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	¿Se revisan periódicamente las cuentas de usuario del sistema?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	¿Se definen y documentan diferentes accesos a nivel de usuario?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	¿Tiene el sistema capacidades para realizar lo siguiente? 1. Detección de credenciales incorrectas 2. Bloqueo de cuentas de usuario tras múltiples intentos incorrectos 3. Caducidad de la contraseña 4. Contraseñas oscuras durante la entrada	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	¿La hora del sistema puede ser cambiada por alguien más que por los administradores?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lista de verificación



LISTA DE VERIFICACIÓN DE INTEGRIDAD DE DATOS

No.	Pregunta	Respuesta (Sí, No, N/A)	Impacto	Plan de Mitigación
Proceso de acceso y revisión de datos				
7.	¿Impide el sistema modificaciones no autorizadas de los archivos de datos de origen almacenados en el Instrumento?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	¿Impide el sistema la eliminación de los archivos de datos de origen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	¿Impide el sistema cualquier modificación o eliminación de los archivos del Audit Trail (si están separados)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	¿Hay algún lugar intermedio antes de que se procesen y revisen los archivos? En caso afirmativo, ¿se controlan y verifican esas ubicaciones para detectar modificaciones y eliminaciones no autorizadas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.	¿Está definido y documentado el proceso de revisión de los datos de origen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.	¿Se utilizan las firmas electrónicas para la revisión y aprobación dentro del software del instrumento? En caso afirmativo, ¿cumple con los requisitos de CFR 21 Parte 11?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13.	¿El sistema interactúa con LIMS o cualquier otro software para el procesamiento y las aprobaciones? En caso afirmativo, ¿se validan las integraciones en cuanto a precisión y seguridad de los datos?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lista de verificación



LISTA DE VERIFICACIÓN DE INTEGRIDAD DE DATOS

No.	Pregunta	Respuesta (Sí, No, N/A)	Impacto	Plan de Mitigación
Audit Trail				
14.	¿El sistema proporciona capacidades al Audit Trail?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15.	¿Se ha probado el Audit Trail como parte del paquete de calificación y demuestra la conformidad con los requisitos de CFR 21 parte 11?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16.	¿Está definido y documentado el proceso de revisión del Audit Trail (empresarial y funcional)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17.	¿Se ha documentado la revisión funcional del Audit Trail en función de la frecuencia establecida?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



CAPAEM

Integridad de datos proceso Sistema de laboratorio



Ejemplo de Evaluación de riesgos de ID para procesos y sistemas de laboratorio



Contexto:

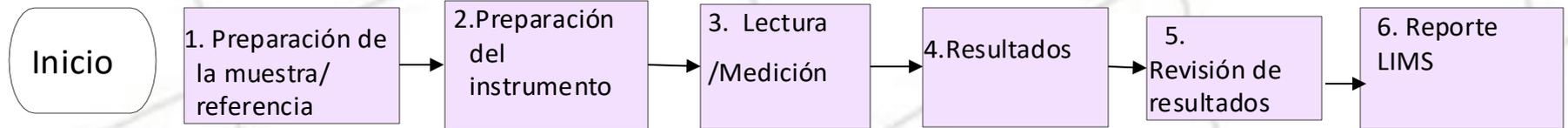
- ❖ El dispositivo UV es un instrumento autónomo, no conectado a una red. Este dispositivo se entrega con una computadora de escritorio estándar con Windows 7 como sistema operativo.
- ❖ Las actividades de pesaje se completan mediante balanzas que están conectadas a una impresora. Estas balanzas están calibradas y el estado de calibración se controla y verifica mediante procedimientos.
- ❖ La configuración de la balanza está bloqueada.
- ❖ El acceso a la balanza está separado del personal del laboratorio.
- ❖ Las hojas de trabajo analíticas preparadas están disponibles para la prueba de ensayo UV y estas hojas son parte del proceso de control de la documentación.

Evaluación de riesgos de ID para procesos y sistemas de laboratorio



Mapeo de procesos

Para este ejemplo, el mapeo de procesos se identifican 6 sistemas y sus subsistemas.



Evaluación de riesgos de ID para procesos y sistemas de laboratorio



3) Datos (papel/electrónicos) e identificación del sistema.

	1	2	3	4	5	6
Inicio	Preparación de muestra /Ref	Prep instrumento	Medición	Resultados	Revisión resultados	Reporte de resultados
GxP Datos	Papel	Papel/electrónico	Electrónico	Papel	Papel/electrónico	Electrónico
Sistema	dato crudo impresión balanza	Hojas de cálculo UV instrumento	UV instrumento	Hoja de cálculo	Hoja de cálculo UV instrumento	LIMS

b. Identificación de datos

Paso	1. Prep. de muestra/Ref	2. Prep. Instrumento	3. Medición	4. Resultados	5. Revisión de resultados	6. Reporte de resultados
Sistema 1: Datos crudos						
Elementos de datos GxP	Método ID Muestra ID Muestra ref. ID Analista Fecha y hora Balanza ID Pesadas (ticket) Solventes/Rectivos ID	Método ID Muestra ID Referencia ID Analista Fecha y hora UV ID	UV	Corrida ID UV absorbancias (impresora o manual) Cálculo del ensayo (s)	Revisión ID Fecha y hora Comentarios Revisión de Audit trail	LIMS
System 2: Balance						
Elementos de datos GXP	Configuración de Fecha/Hora*					

Evaluación de riesgos de ID para procesos y sistemas de laboratorio



Step	1. Preparación muestra/Ref	2. Prep Instrumento	3. Medición	4. Resultados	5. Revisión de resultados	6. Reporte de resultados
------	----------------------------	---------------------	-------------	---------------	---------------------------	--------------------------

System 3: UV

Elementos de datos GXP	Balanza (Sistema 2)	Configuración Fecha/hora* Analista/ Método	UV absorbancia* Meta dato* (corrida, analista fecha, hora, secuencia ID muestra)	Hojas de cálculo	Dato crudo Audit trail	LIMS
------------------------	---------------------	---	---	------------------	-------------------------------	------

System 4: LIMS

Elementos de datos GXP						ID Muestra ID Analista ID fecha y hora del resultado
------------------------	--	--	--	--	--	--

* Nota: de datos electrónicos de GxP que se pueden modificar, eliminar o reprocesar después de su creación

Categorización de datos y sistemas.

- Para este ejercicio se considerará únicamente con el instrumento UV. Las hojas de cálculo sin procesar de GxP (Validadas), las balanzas y LIMS están fuera del alcance.
- Estos sistemas deben tratarse en una evaluación separada.

Identificación y Evaluación de riesgos de ID para procesos y sistemas de laboratorio

Topico	Sub topico	Pregunta	Criterio de Aceptación	Cumple criterio	Descripción del GAP Riesgo
Gestión del ciclo de vida de los datos.	Captura/ingreso de datos	¿El sistema obliga a guardar en el momento de la entrada de datos GxP?	El sistema debe exigir el guardado inmediatamente después de la entrada de datos críticos. La entrada de datos antes de guardarlos en la memoria permanente con seguimiento de auditoría (servidor, base de datos) se considera memoria temporal. Se debe minimizar el tiempo que los datos se mantienen en la memoria temporal.	No	Es posible que los datos no se guarden al final de la medición. El sistema pregunta si es necesario guardar los datos o no
Gestión del ciclo de vida de los datos.	Copia de seguridad de restauración	¿Se mantiene un sistema de programación para las copias de seguridad manuales de datos y los procesos de copia de seguridad manuales son rastreables durante todo el proceso de realización de la actividad?	Para la copia de seguridad de datos manual, se mantendrá un sistema de programación. El sistema de programación deberá rastrear y notificar al personal apropiado cuando se requiera respaldo. Los procesos de respaldo manual deberán ser rastreables durante todo el proceso de realización de la actividad	No	No existe ningún sistema en lugar para respaldo y almacenamiento de sistemas independientes. (no conectado a una red) No hay horario fijo.
Gestión del ciclo de vida de los datos.	Copia de seguridad de restauración	¿Los cambios en el proceso de Copias de seguridad de datos siguen un proceso formal de control de cambios?	Cualquier cambio en las Copias de Seguridad de Datos programadas deberá seguir el proceso formal de gestión de cambios.	No	No existen registros de que los cambios a las copias de seguridad se gestionen a través de CC
Audit trail	Funcionalidad	¿Existe un registro de auditoría para la gestión de usuarios y la configuración del sistema?	Cuando se utilicen sistemas informáticos para capturar, procesar, informar o almacenar datos sin procesar electrónicamente, los datos incluirán la gestión del usuario y la configuración del sistema. Los elementos incluidos en Las pistas de auditoría deben ser aquellas relevantes para permitir la reconstrucción de la generación, modificación y eliminación de la configuración del sistema y de gestión de usuarios	No	No hay ningún registro de auditoría de gestión de usuarios disponible
Seguridad/Usuarios Control de accesos	Autenticación	¿El sistema requiere que se haga cumplir el cambio de contraseña en un intervalo definido?	El sistema debe exigir la aplicación de un cambio de contraseña en un intervalo definido.	No	El sistema no solicita cambios periódicos de contraseña.
Marcas de tiempo	Seguridad/Accesos	¿Pueden los roles que no son administradores de TI cambiar la configuración de fecha y hora del sistema (incluida la configuración de zona horaria)?	Sólo los administradores del sistema tendrán autoridad suficiente para cambiar la configuración de fecha y hora del sistema. Los roles que no sean de administrador tendrán acceso de solo lectura.	No	Todos los usuarios pueden cambiar fecha y hora. (incluida la zona horaria)

Evaluación de riesgos de ID para procesos y sistemas de laboratorio



Etapa/proceso	Función/Requisito o Paso de flujo de datos	Modo Potencial de falla	Efecto	S	O	D	RPN
Captura/ingreso de datos	¿El sistema obliga a guardar en el momento de la entrada de datos GxP?	Es posible que los datos no se guarden al final de la medición. El sistema pregunta si es necesario guardar los datos o no.	Los datos se pueden perder	5	3	4	60
Copia de seguridad de restauración	¿Se mantiene un sistema de programación para las copias de seguridad manuales de datos y los procesos de copia de seguridad manuales son rastreables durante todo el proceso de realización de la actividad?	No existe ningún sistema de respaldo y almacenamiento de sistemas independientes. (no conectado a una red) No hay horario fijo.	Los datos se pueden perder	5	4	2	40
Copia de seguridad de restauración	¿Los cambios en el proceso de Copias de seguridad de datos siguen un proceso formal de control de cambios?	Cambio no detectado	Los datos se pueden perder o alterar	5	4	2	40
Funcionalidad	¿Existe un registro de auditoría para la gestión de usuarios y la configuración del sistema?	No hay ningún registro de auditoría de gestión de usuarios disponible	Los niveles de usuario se pueden cambiar. (por ejemplo, un analista puede recibir derechos de administrador)	5	3	4	60
Autenticación	¿El sistema requiere que se haga cumplir el cambio de contraseña en un intervalo definido?	Los sistemas UV no requieren cambio periódico de contraseña.	Posible abuso de la contraseña de alguien	5	1	4	20
Aceso/ seguridad	¿Pueden los roles que no son administradores de TI cambiar la configuración de fecha y hora del sistema (incluida la configuración de zona horaria)?	Todos los usuarios pueden acceder a la configuración de fecha y hora (incluidas las zonas horarias).	El tiempo de creación de datos puede estar adulterado.	5	2	4	40

Evaluación de riesgos de ID para procesos y sistemas de laboratorio



Paso	Potencial Modo de Falla	Efecto	RPN	Acción de gestión de riesgos	S	O	D	RPN	Acción de gestión de riesgo	S	O	D	RPN
Captura/ingreso de datos	Es posible que los datos no se guarden al final de la medición. El sistema pregunta si es necesario guardar los datos o no.	Los datos se pueden perder	60	Introducir un PNO para describir los diferentes pasos para el usuario durante el análisis UV, incluido un proceso de revisión al final.	5	2	2	20	Actualice el software para ir a la versión que almacena automáticamente todas las ejecuciones.	5	1	1	5
Copia de seguridad de restauración	No existe ningún sistema de respaldo y almacenamiento de sistemas independientes. (no conectado a una red) No hay horario fijo.	Los datos se pueden perder	40	Introducir un proceso de copia de seguridad manual	5	2	2	20	Instale un sistema de respaldo completamente automatizado con un intervalo personalizado definido	5	1	1	5
Copia de seguridad de restauración	Cambio no detectado	Los datos se pueden alterar	40	Introducir al proceso al Sistema Control de Cambios	5	1	1	5	NA desde corto plazo la implementación es suficiente				0
Funcionalidad	No hay ningún registro de auditoría de gestión de usuarios disponible	Los niveles de usuario se pueden cambiar. (por ejemplo, un analista puede recibir derechos de administrador)	60	Implementar PNO de Audit trail	5	2	2	20	Incluso el nuevo software	5	2	2	20
Autenticación	Los sistemas UV no requieren cambio periódico de contraseña.	Posible abuso de la contraseña por el personal	20	Implementar un procedimiento para cambiar periódicamente las contraseñas.	5	1	2	10	Implementar reglas de contraseña automática en el sistema. (o actualizar el software)	5	0	1	0
Aceso/seguridad	Todos los usuarios pueden acceder a la configuración de fecha y hora (incluidas las zonas horarias).	El tiempo de creación de datos puede estar adulterado.	40	incluir un procedimiento definir R&R hacia la configuración de fecha y hora e incluir el control en la revisión periódica.	5	1	4	20	Actualice el software para incluir acceso a nivel de usuario en la configuración de fecha y hora (incluida la zona horaria)	5	0	1	0

Escalas



SEVERIDAD DEL RIESGO (S)		
Efecto	Descripción	Valor
Muy alta	Puede causar daño al cliente	5
Alta	Perdida de la función primaria del producto o servicio, el cliente no puede usar el producto o servicio	4
Moderada	Reduce el nivel de desempeño del producto o servicio, insatisfacción mayor del cliente	3
Baja	Nivel reducido de desempeño del producto o servicio insatisfacción menor del cliente	2
Ninguna	Efecto imperceptible	1

PROBABILIDAD DE OCURRENCIA (PO)		
Efecto	Descripción	Valor
Muy alta	Es casi inevitable, se observa diario o cada vez que se fabrica	5
Alta	Frecuente, semanal	4
Moderada	Ocasional, ocurre por lo menos una vez al mes	3
Baja	Rara vez ocurre, dos veces por año	2
Ninguna	No ha sucedido nunca, baja posibilidad de que ocurra en 2 años o más	1

Detección (D)		
Controles Actuales del proceso		
Efecto	Descripción	Valor
Muy baja	El proceso, producto o servicio defectuoso puede llegar al cliente, está latente y no se manifiesta en la fase de fabricación	5
Baja	El proceso, producto o servicio defectuoso puede llegar al cliente, debido a la baja fiabilidad de los controles existentes	4
Moderada	Moderada probabilidad de que el proceso, producto o servicio llegue al cliente	3
Alta	Baja probabilidad de que el proceso, producto o servicio llegue al cliente, sería detectado por los controles o en fases posteriores	2
Muy alta/Certeza	Remota probabilidad de que el defecto llegue al cliente, casi completa la fiabilidad de los controles	1



AMEF (análisis de modo y efecto de falla)

		MATRIZ DE RIESGOS PO*S*D				
		DETECCIÓN (D)				
PO	S	5	4	3	2	1
5	5	125	100	75	50	25
4	4	80	64	48	32	16
3	3	45	36	27	18	9
2	2	20	16	18	8	4
1	1	5	4	3	2	1

PRIORIDAD DE RIESGO ACCIONES DE GESTIÓN DE RIESGOS

VALOR (NPR)	Nivel	Riesgo	Prioridad de Acciones
NPR > a 26	Alto	Inaceptable	Deben tomarse acciones Inmediatas. Obligatorias
NPR = 7 a 26	Medio	Aceptable	Pueden tomarse acciones a mediano y largo plazo si así lo considera el comité
NPR = 1 a 6	Bajo	Insignificante	Acciones no necesarias para mitigar el riesgo controlado



PNO Ciclo de vida de la validación.

Describe el uso previsto, el plan maestro de validación, requisitos de usuario y funcionales, especificaciones de diseño, la matriz de trazabilidad, etc.

PNO control de cambios

PNO Seguridad de los datos. Copia de seguridad, recuperación ante desastres, recuperación de archivos. Política de contraseñas

PNO Buenas Prácticas de Documentación

PNO Seguridad. Acceso al edificio, centro de datos y redes

PNO CAPA. Seguimiento a desviaciones y planes de acción para corregirlas





La regulación esta enfocada a la:

- Responsabilidad de la Industria para asegurar la Seguridad, Eficacia y Calidad de los productos o servicios.
- La integridad de los datos es la garantía de que la información digital no está corrupta y solo aquellos autorizados para hacer lo pueden acceder a ella o modificarla.
- La integridad de datos describe los datos que se mantienen completos, precisos, coherentes y seguros durante todo su ciclo de vida.



La regulación esta enfocada a la:

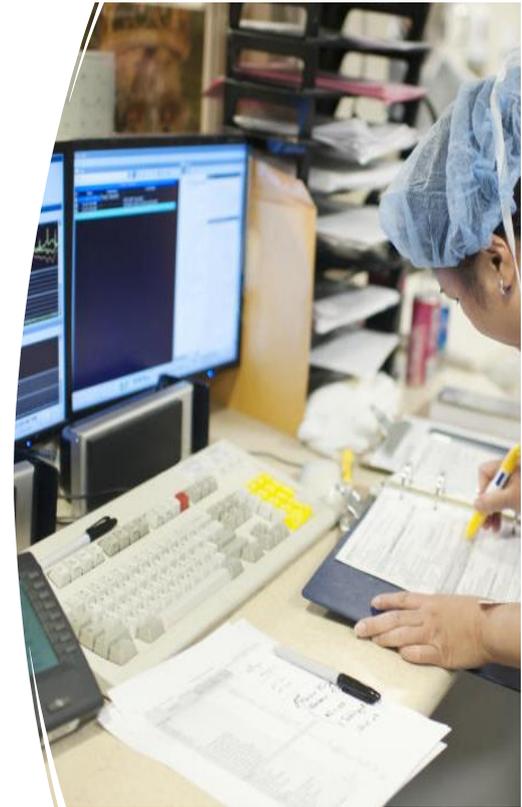


La forma en que se generan los datos reglamentarios ha seguido evolucionando en consonancia con el desarrollo continuo de tecnologías de apoyo, como el uso cada vez mayor de la captura electrónica de datos, la automatización de sistemas y el uso de tecnologías remotas; y la creciente complejidad de las cadenas de suministro y las formas de trabajo por ejemplo, a través de proveedores de servicios externos.



Los sistemas de apoyo a estas formas de trabajo pueden ir desde procesos manuales con registros en papel hasta el uso de sistemas totalmente computarizados.

El objetivo principal de los requisitos reglamentarios sigue siendo el mismo, es decir, tener confianza en la calidad y la integridad de los datos generados (para garantizar la seguridad del paciente y la calidad de los productos) y poder reconstruir las actividades.



Las guías mantienen estructura en tres grandes rubros



1a. Parte. Incluye las disposiciones generales, definiciones generales y tipos de registros.

2a. Parte. Sección de registros electrónicos, necesidad de firmas en los registros, los sistemas computarizados deben garantizar la exactitud, fiabilidad y coherencia de los datos introducidos y procesados. Restricciones de acceso a través de identificación y contraseñas.

3a. Parte. Énfasis en las firmas electrónicas y el control, cómo los cambios periódicos de contraseñas.





Integridad de datos: Problemas en la industria

Integridad de datos Warning Letter 2019	Cadena de suministros
	Reempaque desconocido en la cadena
	Diseño de áreas asépticas
	Integridad de datos principales causas

- 1. Vulnerabilidades en el sistema informático*
- 2. Se encontró que un CoA fue elaborado antes de que el lote fabricado fuera analizado.*

Integridad de datos: Problemas en la industria

No realizar las pruebas requeridas: Se realizaron los registros pero no se realizaron las actividades de muestreo y pruebas. Los auditores citaron a las empresas por no realizar estas actividades, mientras que los Certificados de Análisis (CoA) indican que se habían realizado las pruebas finales.

Falsificación de datos críticos: Falsificación de información de muestreo o resultados de pruebas en hojas de trabajo/cuadernos de registro/reportes de pruebas, incluida la fabricación de resultados o la transmisión de resultados cuando los datos originales no cumplieron con las especificaciones

Eliminación de datos: Eliminación o sobrescritura de datos electrónicos de resultados de laboratorio.

Deficiencias en los informes de desviaciones y la investigación de problemas de integridad de los datos: Deficiencias como alcance limitado de las investigaciones que no se extienden a los problemas de integridad de los datos, falta de planes de acción para abordar las deficiencias y cómo la unidad de Calidad evitará la recurrencia y falta de una evaluación integral.



Integridad de datos: Problemas en la industria

Integridad
de datos
Warning
Letter
2004 2007

Los usuarios pueden sobrescribir datos originales, no cuentan con contraseñas individuales.

Sistemas informáticos heredados no validados

Los registros electrónicos generados durante la fabricación del producto no se revisaron antes de liberar el lote

El sistema no se ha mantenido bajo los procedimientos establecidos de control de cambios



¿Qué es una warning letter ?

- Es una carta de **advertencia oficial** que la FDA envía a las empresas afectadas a consecuencia de una inspección fallida
-
- Antes de emitir una warning letter, la FDA solicita a la compañía que **responda a los hallazgos** que se encontraron durante la inspección
-
- Si la FDA considera que la respuesta de la compañía es **inaceptable** entonces emite la warning letter



Consecuencias
potenciales de una
warning letter

Confiscación del
producto, la detención
administrativa. La
aplicación de sanciones
monetarias civiles y/o
enjuiciamiento



BUENAS PRACTICAS DE DOCUMENTACIÓN

**Se deben de implementar las BPD para
reforzar la Integridad de Datos (ALCOA ++)**



El porqué de las Buenas Prácticas de Documentación

¿Por qué la documentación es esencial en una organización?

- Las BPD son una práctica regulada
- Asegura que todo el personal involucrado en un proceso sepa lo que tiene que hacer y cuándo hacerlo
- Asegura la existencia de evidencia documentada y su trazabilidad
- Proporciona la información que permite y hace posible una investigación cuando sea necesario



El porqué de las Buenas Prácticas de Documentación

¿Por qué es importante una Buena documentación?

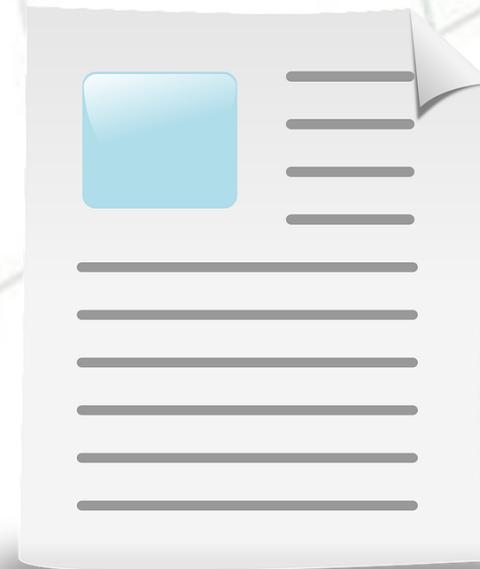
- Es una parte esencial del sistema de garantía de calidad y debe existir para cumplir los aspectos de las BPF (NOM-059, CFR, etc.)
- Las BPD es una práctica esperada por agencias regulatorias
- Tendremos Información correcta, completa, actual y consistente.
- Permite cumplir eficazmente con los requisitos de los clientes y partes interesadas.
- Contribuye a reducir las observaciones planteadas sobre prácticas de documentación inadecuadas.

BUENAS PRACTICAS DE DOCUMENTACION



Se aplican a muchos documentos y demuestra conformidad con los requisitos previamente establecidos y/o de la legislación o estándares de calidad como:

- COFEPRIS
- ISO 9001
- EXIPACT
- Clientes



BUENAS PRACTICAS DE DOCUMENTACION



Los registros deben ser:

- Concisos.
- Legibles
- Exactos
- Trazables

BUENAS PRACTICAS DE DOCUMENTACION



Concisos.

Debe contar la historia del proceso y ser entendible para todos los usuarios

Legibles.

Legible para clientes internos y externos

Exactos.

Documentos libres de errores

Trazables.

Cada aspecto del documento debe ser rastreable, como quién lo registró, cuándo, dónde y por qué.

¿ Cómo facilitamos este trabajo ?



¿Qué significa ser conciso?.

¿ Sus documentos están estandarizados ?

¿ Sus documentos son fáciles de usar por todos los usuarios ?

¿ Tenemos documentos que constantemente tienen errores?

¿ Nuestros documentos cuentan la historia completa?

El principio, el medio y el final de la fabricación de un medicamento

¿ Cómo facilitamos este trabajo ?



¿ Qué significa ser legible ?.

En una forma simple significa:

- ✓ Qué todos pueden leer y entender lo que está escrito
- ✓ No importa quién, dónde y qué. ¿Todos pueden leer los datos escritos o impresos ?

¿ Cómo facilitamos este trabajo ?



¿ Qué significa ser exacto ?.

- ✓ Los registros deben realizarse al momento de realizar la operación
- ✓ El proceso debe diseñarse para detectar cualquier error.



¿ Por qué debería de realizar estos registros ?

- ✓ Los registros y documentos son evidencia objetiva de que se está realizando la tarea.
- ✓ Si no se documentó no se realizó la actividad
- ✓ Se deben llevar bitácoras de registro de las pruebas analíticas o críticas de los equipos de proceso y de las áreas donde se procesa producto



Documentación

Etiquetas

Procedimientos analíticos

Especificaciones de MP, PT, ME, etc.

Instructivos de fabricación y acondicionamiento

Procedimientos estándar de operación

Bitácoras

Protocolos de validación

Registros de calibración

Registros de mantenimiento

Planos

MC

EMSF

Políticas

Comunicados organizacionales

Expedientes de personal



Documentación Identificación/Codificación



- ❖ Normalmente lo emite una persona o departamento de control de documentos.
- ❖ Todos los documentos **deben** tener un Código de documento único
- ❖ Cada página de un documento **debe** estar marcada con el número de página y el número total de páginas del documento.

PROCEDIMIENTO NORMALIZADO DE OPERACIÓN		
Logo	TÍTULO: Elaboración de procedimientos estándar de operación	
DEPARTAMENTO EMISOR : Documentación		
CÓDIGO: PF-D0-001	VERSIÓN: 02	SUSTITUYE A: Versión 01
FECHA DE EMISIÓN: Jul 2024	FECHA DE VIGENCIA: Jul 2027	PÁG. 1 DE 3

Documentación Identificación/Codificación



- ❖ Todos los documentos **deben** tener un nivel de revisión.
- ❖ Los documentos **deben** tener una fecha de vigencia y emisión

PROCEDIMIENTO NORMALIZADO DE OPERACIÓN		
Logo	TÍTULO: Elaboración de procedimientos estándar de operación	
DEPARTAMENTO EMISOR : Documentación		
CÓDIGO: PF-D0-001	VERSIÓN: 02	SUSTITUYE A: Versión 01
FECHA DE EMISIÓN: Jul 2024	FECHA DE VIGENCIA: Jul 2027	PÁG. 1 DE 3

Documentación Identificación/Codificación



Ejemplo de encabezado para
protocolo de validación de un
método analítico

PROTOCOLO DE VALIDACIÓN DE MÉTODO ANALÍTICO		
Logo	TÍTULO: Protocolo de validación de método para analizar Naproxeno en tabletas de 100 y 250 mg código XXX por HPLC.	
DEPARTAMENTO EMISOR : Desarrollo Analítico		
CÓDIGO: PV-DA-001	VERSIÓN: 01	SUSTITUYE A: Documento nuevo
FECHA DE EMISIÓN: Jul 2024	FECHA DE VIGENCIA: NA	PÁG. 1 DE 20

Cambios a Documentación.



Todos los cambios en la documentación **deben** documentarse en el **sistema de control de cambios**, revisarse y aprobarse.

Riesgo: Los cambios no controlados a documentos pueden derivar en que se utilice una versión de un documento no vigente.





LO QUE NO ESTA ESCRITO NO EXISTE



Lo que no se Registra, no se puede Medir y por lo tanto, no se puede Gestionar adecuadamente.

Solo por el echo de estar documentado, no significa que haya sido efectivo

La documentación confiable ayuda a encontrar la fuente de algún error.



Buenas Prácticas de Documentación

- ❖ La historia y las tendencias indican que la documentación siempre será el principal elemento que sirve de **Evidencia de Auditoria** para cualquier empresa
- ❖ Para demostrar que se están llevando a cabo todas las actividades señaladas por la regulación sanitaria.



Buenas Prácticas de Documentación

Una buena documentación es una parte esencial del SGC y por lo tanto se relaciona con todos los aspectos de las Buenas Prácticas de Fabricación.

- El objetivo principal del sistema de documentación es Diseñar, Establecer, Controlar, Monitorear y Registrar todas las actividades que puedan afectar el producto o servicio proporcionado.



BUENAS PRACTICAS DE DOCUMENTACION



Objetivos del sistema documental

DISEÑAR



IMPLEMENTAR



REGISTRAR



SUPERVISAR/
MONITOREAR



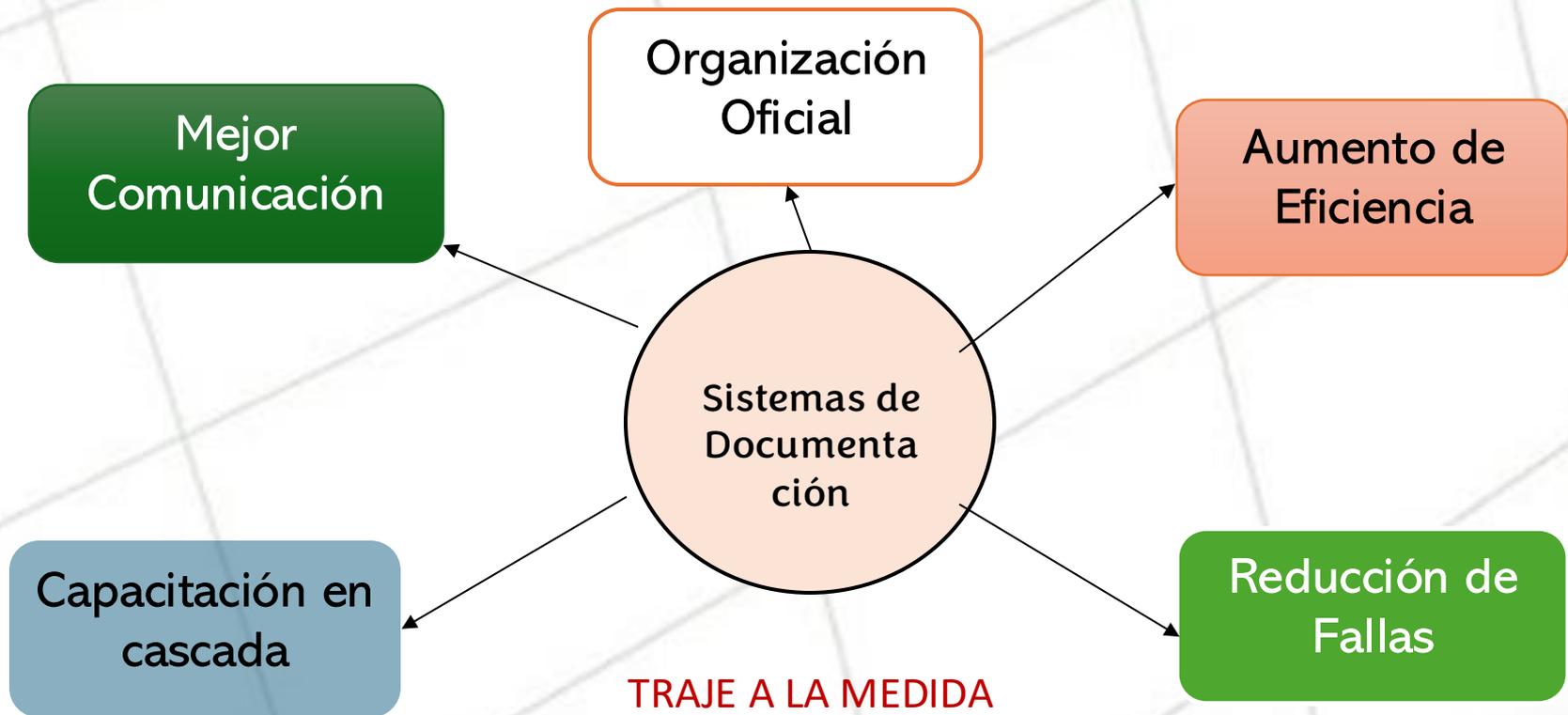
ASEGURAR TRAZABILIDAD/ EVIDENCIA:

Clara
Veraz
Exacta
Integra/Completa
Disponible
Legible

CONTROLAR/
MANTENER



SISTEMAS DE DOCUMENTACION



BUENAS PRACTICAS DE DOCUMENTACION



Definiciones

Buenas prácticas de documentación.

Herramientas creadas para asegurar el empleo correcto y permanente de los documentos, con la finalidad de garantizar que las operaciones se llevaron a cabo de manera adecuada y permiten la trazabilidad oportuna de la información.

Su objetivo es preservar la integridad de los datos de los documentos y registros importantes, y también pueden servir de guía sobre cómo registrar la información y almacenar los datos de forma adecuada.



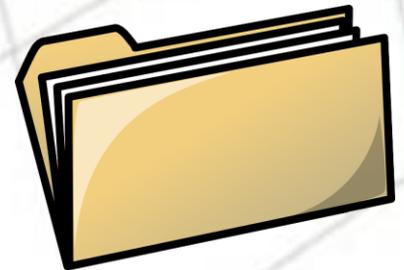
BUENAS PRACTICAS DE DOCUMENTACION



DEFINICIONES

Documento:

Escrito que contiene datos verdaderos de la realización y/o control de cada proceso. Información escrita que puede ser empleada, para probar que se realizó un hecho como la fabricación de un lote, un análisis, etc; y registrado en formatos, bitácoras, archivos, etc.



BUENAS PRACTICAS DE DOCUMENTACION



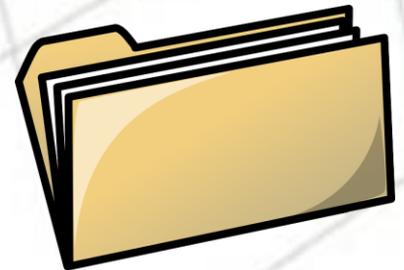
DEFINICIONES

Procedimiento Normalizado de Operación:

Documento que contiene las instrucciones necesarias para llevar a cabo de manera clara ordenada, completa y reproducible una operación.

Los PNO son parte del sistema de documentación operativa del laboratorio y planta por lo tanto deben ser escritos en español, debe emplearse vocabulario sencillo, indicando tipo, naturaleza, propósito y uso del documento.

La organización de su contenido será tal que permita su fácil comprensión.



BUENAS PRACTICAS DE DOCUMENTACION



DEFINICIONES

Registro de capacitación, Documento en el que se registra que se ha dado a conocer la información contenida en un documento a las personas que requieren conocerla, especialmente aquellas involucradas en el uso de un procedimiento.

Fecha de emisión, Fecha en que entra en vigor el procedimiento y hasta la publicación de la siguiente versión.

Fecha de vigencia, Tres años a partir de la fecha de emisión del PNO o cada vez que se modifiquen las disposiciones aplicables al establecimiento o las actividades descritas en el procedimiento.

Definiciones

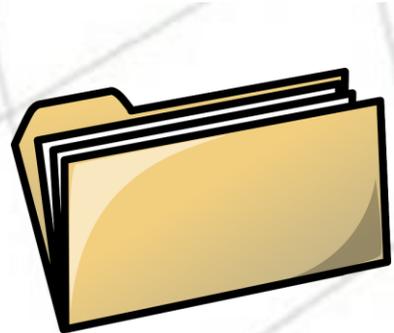
Catálogo:

Relación ordenada en la que se incluyen o describen de forma individual libros, documentos, personas, objetos, etc. que están relacionados entre sí.

Registro de calidad: Evidencia de las acciones realizadas para demostrar cumplimiento de las instrucciones.

Trazabilidad: A la capacidad de reconstruir la historia, localización de un elemento o de una actividad, por medio de registros de identificación.

BUENAS PRACTICAS DE DOCUMENTACION



Definiciones

Cifras significativas:

Dígitos necesarios para expresar la precisión de la medida.

Redondeo de valores numéricos

Acción realizada para obtener un número que solo contenga dígitos significativos

Integridad de datos

Los datos son confiables, completos, coherentes, rigurosos y seguros

Marco regulatorio



BPF (cGMP) Emitidas por diferentes autoridades regulatorias y guías emitidas por diferentes fundaciones no gubernamentales

- ❖ **WHO** Organización mundial de salud
- ❖ **MHRA** Agencia reguladora de medicamentos y dispositivos médicos de Reino Unido
- ❖ **TGA** Therapeutic Goods Administration de Australia
- ❖ **FDA** Agencia de administración de medicamentos y alimentos USA
- ❖ **ICH** Guía de la conferencia internacional de armonización
- ❖ **PICS** Pharmaceutical Inspection Convention
- ❖ **UE**
- ❖ **COFEPRIS**



NOM-059-SSA1-2015 BPF.



5.2 Documentación

- Los documentos deben definirse y apegarse a lo establecido.
- Los sistemas electrónicos necesitan entenderse y estar bien documentados.

Validados y disponer de controles adecuados.



NOM-059-SSA1-2015 BPF.



5.2 Documentación

- ❖ Escritos en idioma español
- ❖ Algunos documentos pueden existir en forma híbrida
- ❖ redactarse de manera ordenada y ser fáciles de comprobar
- ❖ El estilo y lenguaje de los documentos debe concordar con su intención de uso.





NOM-059- SSA1-2015 BPF.

5.2.2 Control de la documentación.

- Medidas de control para los documentos maestros y copias oficiales.
- El manejo de datos y registros se tienen que establecer tanto para los sistemas híbridos como para los manuales.
- Deben implementarse controles adecuados para documentos electrónicos tales como plantillas, formularios y documentos maestros.
- Debe disponerse de controles adecuados para asegurar la integridad de los registros a lo largo del período de retención.



NOM-059- SSA1-2015 BPF.

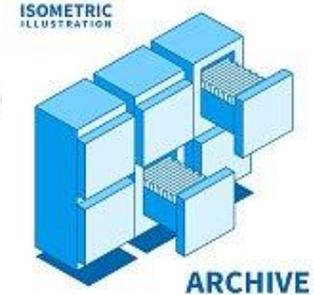


5.2.2 Control de la documentación.

- Los documentos **deben** diseñarse, prepararse, revisarse y distribuirse de acuerdo a lo establecido en el Sistema de Gestión de Calidad.
- **Deben** cumplir con las partes aplicables de las especificaciones de producto, de los expedientes de autorización de fabricación y comercialización.
- La reproducción de documentos originales no **debe** permitir la introducción de errores en el proceso de reproducción.



NOM-059-SSA1-2015 BPF.



5.2.3. Resguardo de documentos.

Debe definirse e implementarse:

- El lugar de resguardo de los documentos relacionados a la fabricación de los medicamentos.
- Medidas de control que aseguren la integridad de los documentos durante todo el periodo de almacenamiento



Debe mantenerse en resguardo el expediente de fabricación de cada lote al menos un **año después de su fecha de caducidad o cinco años después de que el lote fue liberado.**



NOM-059-SSA1-2015 BPF.



5.2.3. Resguardo de documentos.

El periodo de conservación de los documentos dependerá de la actividad que la documentación sustente.

La documentación crítica, incluyendo los datos primarios por ejemplo:

De validación o estabilidad, que respaldan la información del Registro Sanitario o autorización de comercialización **debe conservarse mientras la autorización sigue vigente.**

NOM-059- SSA1-2015 BPF.



5.2.3. Resguardo de documentos.

- Para productos en investigación, la documentación debe conservarse en resguardo al menos cinco años después de que la empresa haya registrado el producto en el último país.
- Cualquier tipo de resguardo distinto al tiempo mencionado debe fundamentarse con base en las disposiciones jurídicas aplicables.



NOM-059-SSA1-2015 BPD.

Los documentos deben ser aprobados, firmados y fechados ya sea que sean emitidos por medios manuales o electrónicos.

Los documentos del SGC deben revisarse periódicamente y mantenerse actualizados.

Debe dejarse espacio suficiente para permitir la realización de registros.

Los registros escritos a mano deben realizarse de forma clara, legible e indeleble.

El registro de actividades debe realizarse al momento de la actividad respetando el orden cronológico.

NOM-059-SSA1-2015 BPD.



CUALQUIER CORRECCIÓN AL REGISTRO DE UNA ACTIVIDAD O A UN DOCUMENTO DEBE SER FIRMADO Y FECHADO Y PERMITIR LA LECTURA DE LA INFORMACIÓN ORIGINAL.



CUANDO SE REQUIERA UNA EXPLICACIÓN DEL MOTIVO DE LA CORRECCIÓN DEBE DOCUMENTARSE; ESTOS REGISTROS DEBEN CONTENER LA FECHA E IDENTIFICAR QUIÉN REALIZÓ LA ACTIVIDAD.



DEBE EXISTIR UN MECANISMO QUE PERMITA IDENTIFICAR LAS FIRMAS Y RÚBRICAS DEL PERSONAL QUE EJECUTA LA OPERACIÓN.



Hallazgos más comunes de auditorías

Documentación

- Cambios realizados sin un control de cambios documentado
- Empleo de planos o documentos obsoletos
- Imposibilidad de confirmar la versión oficial de un documento
- Cifras significativas incorrectas
- Registro de la hora incongruentes
- Registro de datos incompletos.

Procedimientos

- No disponibles
- Inadecuados
- No son seguidos o el proceso ya cambio y no se actualizo el PNO
- Modificaciones a procedimientos no adecuada



Deficiencias en la documentación:

Mala práctica	Consecuencia
<p>Documentos No controlados, por ejemplo: Sin un número de identificación único y sin número de versión</p>	<p>Aumenta el riesgo potencial de omisión o la pérdida de datos críticos, fácil modificación/falsificación de registros, uso de documentos obsoletos y no autorizados.</p>
<p>Espacios previstos para la entrada de datos sin suficiente espacio</p>	<p>Datos encimados, poco legibles, no registro de toda la información, riesgo de perder la trazabilidad.</p>



Deficiencias en la documentación:

Mala practica	Consecuencia
Adición de páginas a documentos (por ejemplo, reportes) para permitir una completa documentación	El número de referencia a cualquiera de las páginas agregadas no está claramente relacionada en la página de registro principal, así mismo las páginas adicionadas no se encuentran numeradas, firmadas y fechadas.
Instrucciones ambiguas	Puede llevar a incoherencias/registro incorrecto de datos



Deficiencias en la documentación:

Mala práctica	Consecuencia
Condiciones de almacenamiento inadecuadas	Puede permitir la modificación no autorizada. Uso vencido y/o borradores de documentos o causar la pérdida de documentos maestros
Las versiones actualizadas no se distribuyen de manera oportuna	Puede haber un riesgo de que las versiones obsoletas puedan utilizarse por error si están disponibles para su uso.



Deficiencias en la documentación:

Mala práctica	Consecuencia
Sin la justificación de copias distribuidas a áreas o personal que no lo requiere	Pérdida del sistema de control Perdida de la trazabilidad Riesgo potencial de falsificación y robo de la información
Corrección a datos críticos sin ninguna justificación Registros incompletos	Pérdida de la integridad de datos Falsificación de la información

PRINCIPALES DOCUMENTOS LEGALES



- LICENCIA SANITARIA
- AVISO DE FUNCIONAMIENTO
- CERTIFICADO DE BPF
- ALTA DE RESPONSABLE SANITARIO
- REGISTROS SANITARIOS VIGENTES
- EXPEDIENTE LEGAL DE CADA PRODUCTO
- FARMACOPEA EDICION VIGENTE, SUPLEMENTOS



SALUD
SECRETARÍA DE SALUD

Cofepris 
Comisión Federal para la Protección
contra Riesgos Sanitarios

PRINCIPALES DOCUMENTOS TECNICOS



- ❖ Manual de Calidad
- ❖ Plan Maestro de Documentación
- ❖ Plan Maestro de Validación
- ❖ Política de Calidad
- ❖ Procedimientos
- ❖ Protocolos
- ❖ Organigrama
- ❖ Perfiles de Puesto
- ❖ Descripción de puesto

PRINCIPALES DOCUMENTOS TECNICOS



- Expediente Maestro para cada Producto
- Información sometida para la obtención del Registro Sanitario
- Orden Maestra de Producción
- Orden Maestra de Acondicionamiento
- Planos y diagramas
- Programas y planes
- Instructivos
- Listados y guías de verificación
- Catálogo de firmas



PRINCIPALES DOCUMENTOS TECNICOS



- Especificaciones y certificados analíticos
- Métodos analíticos
- Gráficos de control
- Bitácoras o formatos de registro, etiquetas
- Informes, reportes
- Acuerdos técnicos



Clasificación de la documentación



¿Qué hacemos con la gran variedad de documentos del SGC:

Clasificar los documentos por niveles de impacto, para que sea mas fácil el manejo y se tengan en forma mas clara las responsabilidades.



Niveles de documentos y la pirámide documental

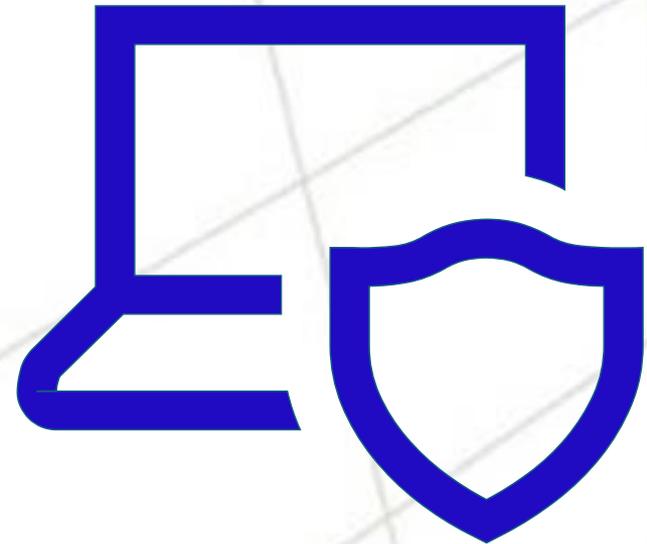


Nivel 1 Legal . generada por los gobiernos, OMS, FDA, EMA, LEYES, REGLAMENTOS, NORMAS, REGISTROS SSA, FEUM Se utilizan como base para el desarrollo de los documentos de otros niveles.

Nivel 2 Documentos Maestros

El contenido depende de los criterios de la empresa y generalmente engloban las Políticas y estrategias de la Alta Dirección.

Ejemplos: Expediente Maestro de Sitio de Fabricación, Manual de Calidad, Plan Maestro de Validación, Planes de Calidad.



Nivel 3 Procedimientos. Documentos más específicos por área o departamento que desglosan actividades generales que en ella se realizarán. Establecen sistemas organizacionales e interdepartamentales.

Ejemplo: PNO's, protocolos, especificaciones, programas de mantenimiento, programas de calibración, descripciones de puesto, métodos analíticos, etc.

Nivel 4 Instructivos. Documentos más específicos que el nivel 3, que generalmente incluyen actividades sencillas y puntuales dirigidas en su mayoría a nivel operativo.

Ejemplos: Instructivos, guías de trabajo, Instrucciones, Lineamientos, Listas de verificación.





Nivel 5 Registros (Formatos de colección de datos).

Documentos derivados como resultado de la ejecución de las actividades indicadas en los documentos de los niveles anteriores.

Reflejan la situación día a día. originados después de llevar a cabo procesos o actividades.

Ejemplo: Bitácoras, Hojas de trabajo, Certificados, Etiquetas, Registros de distribución.

Todos los formatos deben de codificarse de tal manera que se pueda identificar a que PNO pertenecen.



Ejemplo de pirámide documental

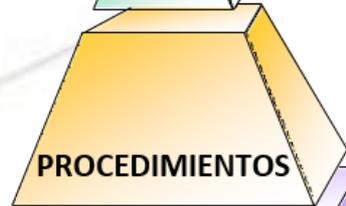


NIVEL 1



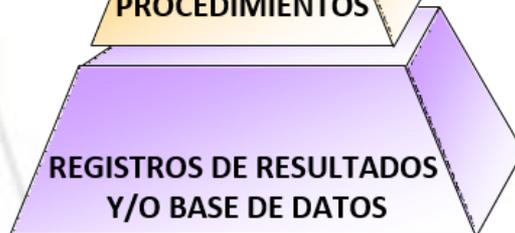
Declaración de Política y Objetivos de Calidad

NIVEL 2



Define ¿QUÉ?, ¿QUIÉN?, ¿CUÁNDO?, ¿DÓNDE?

NIVEL 3



Muestra las evidencias que el sistema de Gestión de Calidad está funcionando.

Ejemplo de pirámide documental

CAPAEM



Ejemplo de
pirámide
docur

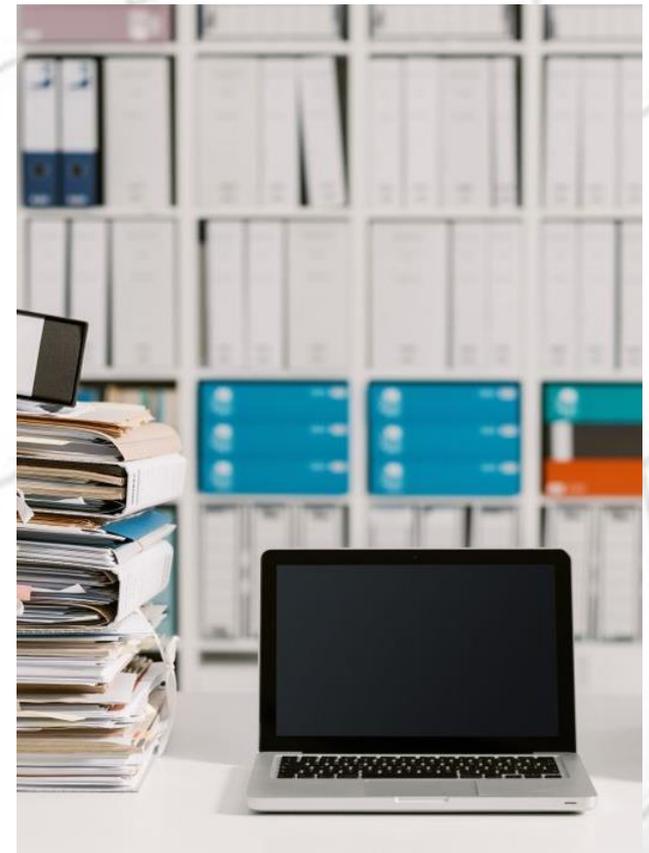
Ejemplo de
pirámide
documental



Implementación/actualización del Sistema de Documentación



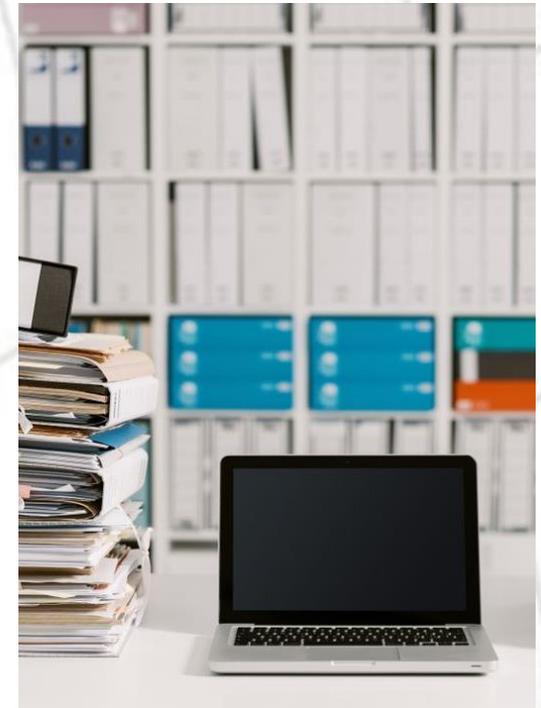
1. Definir nivel de documentos (Pirámide documental)
2. Sistema de codificación de documentos y formatos
3. Definir PNOs del sistema de documentación
4. Mapa de procesos y subprocesos. Verificar que PNOs require cada subproceso



Implementación/actualización del Sistema de Documentación



5. Generar/actualizar los documentos
Revisión y aprobación
6. Capacitación y Emisión de la documentación
7. Mejora continua



1. Definir el nivel de documentos



NIVEL 1



Declaración de Política y Objetivos de Calidad

NIVEL 2

PROCEDIMIENTOS

Define ¿QUÉ?, ¿QUIÉN?, ¿CUÁNDO?, ¿DÓNDE?
Procedimientos, Protocolos, Documentos
Maestros, Planos, Políticas

NIVEL 3

REGISTROS DE RESULTADOS
Y/O BASE DE DATOS

Muestra las evidencias que el
sistema de Gestión de Calidad está funcionando.

2. Sistema de codificación de documentos



Codificación de documentos

AB-XY-000

AB = Tipo de documento

XY = Área

000 = no de documento consecutivo

Codificación de formatos de registro

Fn-AB-XY-000

Fn = No. de formato (n)

AB = Tipo de documento

XY = Área

000 = no de documento consecutivo

2. Sistema de codificación de documentos



Codificación de documentos	Codificación de formatos de registros
AB-XY-000	Fn-AB-XY-001
PN -SG-001	F1 -PN-SG-001, F2 -PN-SG-001
MA-FQ-001 (Método Analítico)	F1 -MA-FQ-001
PG-RH-001 (PNO General)	F1 -PG-RH-001
PV-VA-001 (Plan de validación) RV-VA-001 (Plan de validación)	Sin formatos F1 -RV-VA-001
MA-MI-001 (Método Analítico) PC-RH-001 (Instructivo de Trabajo)	F1 -MA-MI-001 F1 -IT-MI-001

2. Sistema de codificación de documentos



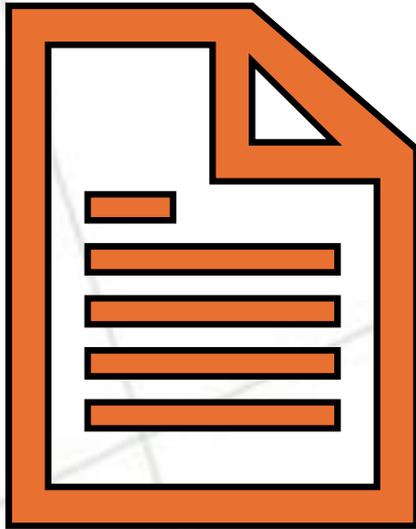
Ejemplo de formato: Lista Maestra de Procedimientos Normalizados de Operación

No.	NOMBRE DEL DOCUMENTO	VERSION	CODIGO	FECHA DE EMISIÓN	FECHA DE PROXIMA REVISION
1	Elaboración de procedimientos normalizados de operación	01	PN-DO-001		
2	Control de la documentación	01	PN-DO-002		
3	Registros y documentación	01	PN-DO-003		
4	Procedimiento para elaborar Instructivos de Trabajo	01	PN-DO-004		
5	Procedimiento para elaboración de documentos	01	PN-DO-005		
	F2-PN-DO-001-REV001				

A primera vista podemos identificar que es el formato no. 2 del procedimiento normalizado de documentación versión 001. Revisión del formato (REV001)



3. Definir procedimientos del Sistema de documentación



1. PNO Elaboración de procedimientos estándar de operación
2. PNO Elaboración y control de documentos
3. PNO Registros y Buenas Prácticas de documentación

4. Procesos y subprocesos procesos NOM-059

PNO Elaboración de PNOS
PNO Elaboración y control de documentos
PNO Registros y buenas prácticas de documentación

GARANTIA DE CALIDAD

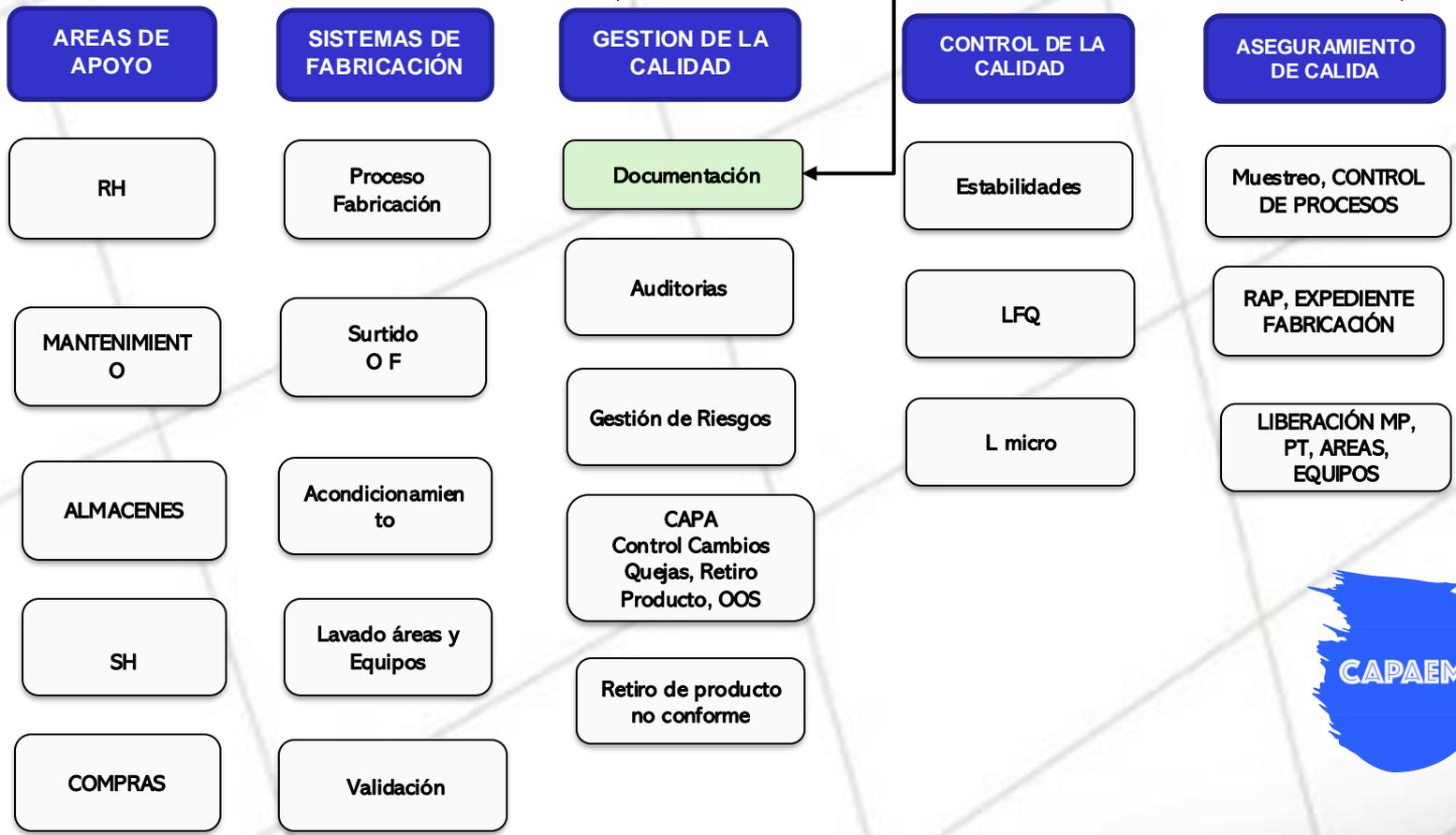
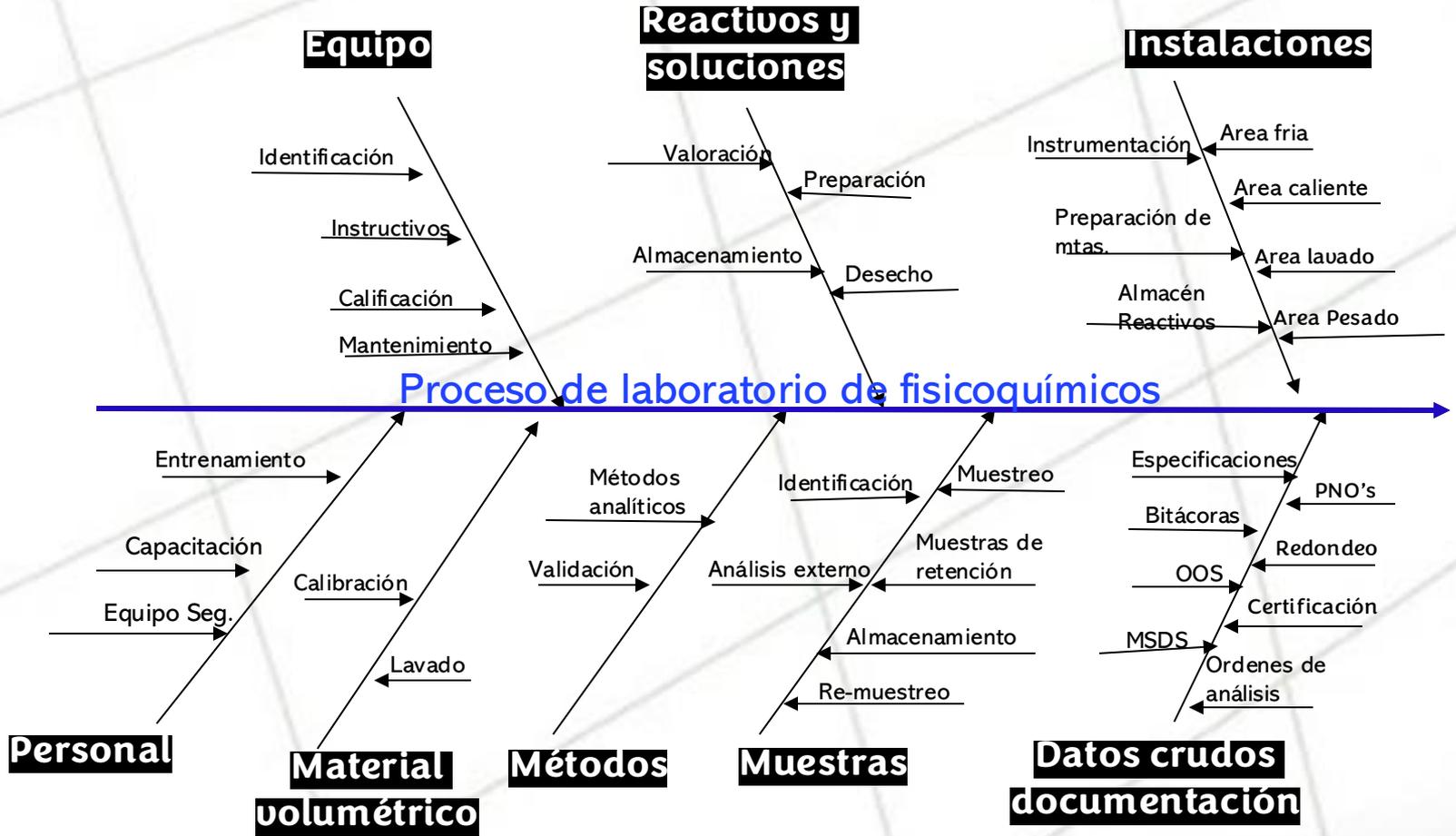


Diagrama de Ishikawa





**¿ Con
cuántos
documentos
opera una
planta?**

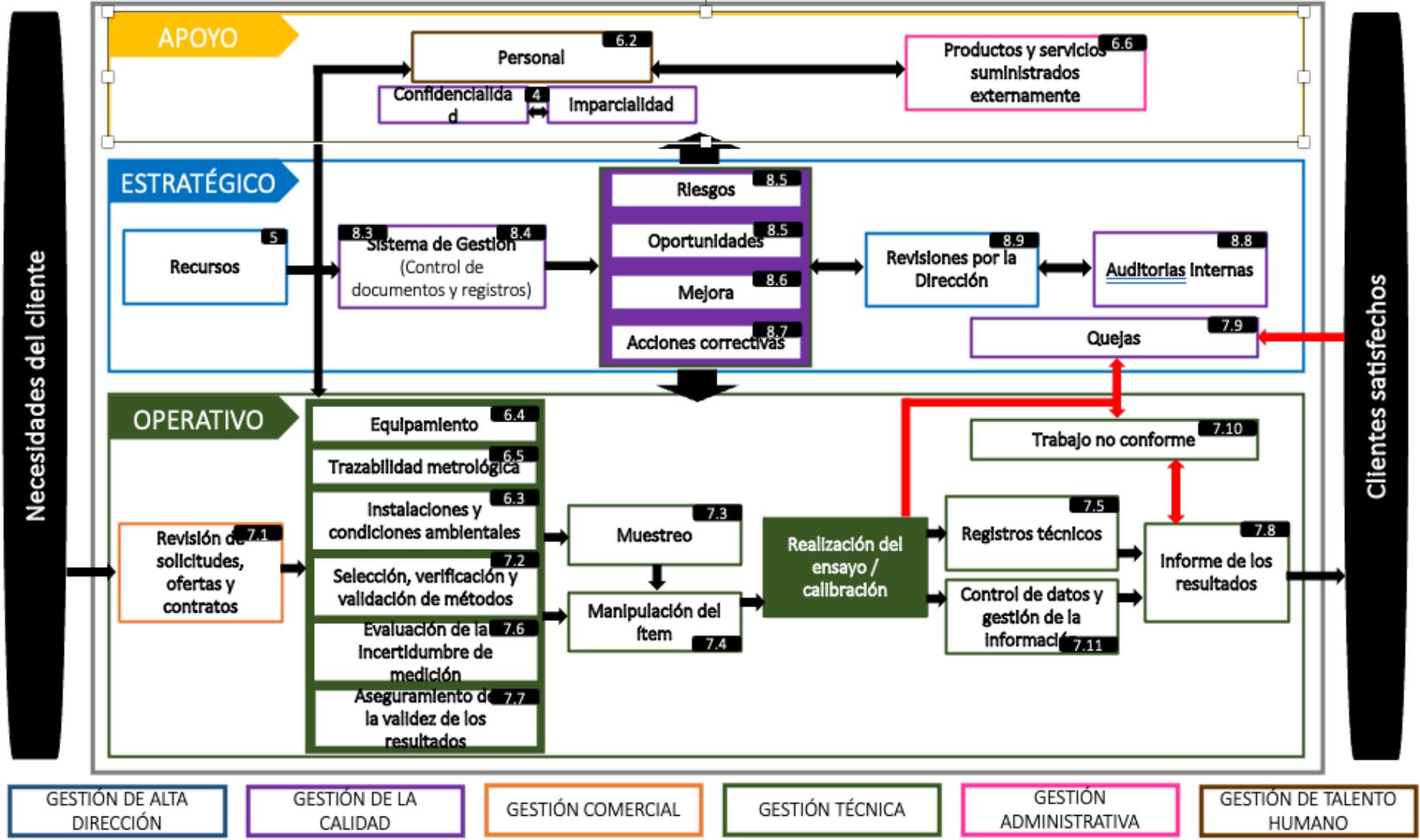
Objetivo:

- ❖ No duplicar actividades en diferentes áreas
- ❖ Integrar todos los procesos de una organización al SGC.
- ❖ Contar con un sistema documental amigable, ligero y con cumplimiento regulatorio

4. Mapa de procesos Mnx 17025



MAPA DE PROCESOS DEL LABORATORIO



1. PNO de elaboración de procedimientos normalizados de operación

Un PNO nos permite:

- Mostrar que el trabajo fue realizado
- El proceso se ejecutó paso a paso
- Evita errores
- Encuentra fuentes de problemas
- Cumplimiento con las BPF
- Capacitación de personal de nuevo ingreso



1.0 PNO de elaboración de procedimientos normalizados de operación

Un PNO :

- Contiene instrucciones detalladas muy explícitas de un proceso.
- Define los pasos esenciales, la secuencia de ejecución y precauciones a tomar para reproducir un proceso.



PNO de elaboración de procedimientos normalizados de operación

Un PNO :

- Es estándar permite a todos realizar de la misma manera el proceso descrito
- Describe y da instrucciones
- Están disponibles para todo el personal en su área de trabajo y sirven de consulta
- Permiten revisión y verificación de cada etapa del proceso
- Dan control y trazabilidad, son la base para demostrar cumplimiento ante auditorías.

PNO Procedimiento para hacer Procedimientos



Reglamento de insumos para la salud, puntos mínimos que debe incluir un PNO en general:

1. Objetivo
2. Alcance
3. Responsabilidades
4. Desarrollo
5. Bibliografía

También indica que los documentos deben ser:

1. Revisados
2. Autorizados
3. Codificados
4. Distribuidos
5. Implementados
6. Vigentes
7. Actualizados

PNO de elaboración de procedimientos normalizados de operación



PROCEDIMIENTO NORMALIZADO DE OPERACIÓN		
	TÍTULO: Elaboración de Procedimientos Estándar de operación	
DEPARTAMENTO EMISOR : Documentación		
CÓDIGO: PN-DO-001	VERSIÓN: 02	SUSTITUYE A: Versión 01
FECHA DE EMISIÓN: Jul 2024	FECHA DE VIGENCIA: 2027	PÁG. 1 DE 10

1. Revisados
2. Autorizados
3. Codificados
4. Distribuidos
5. Implementados
6. Vigentes
7. Actualizados

PNO de elaboración de procedimientos normalizados de operación



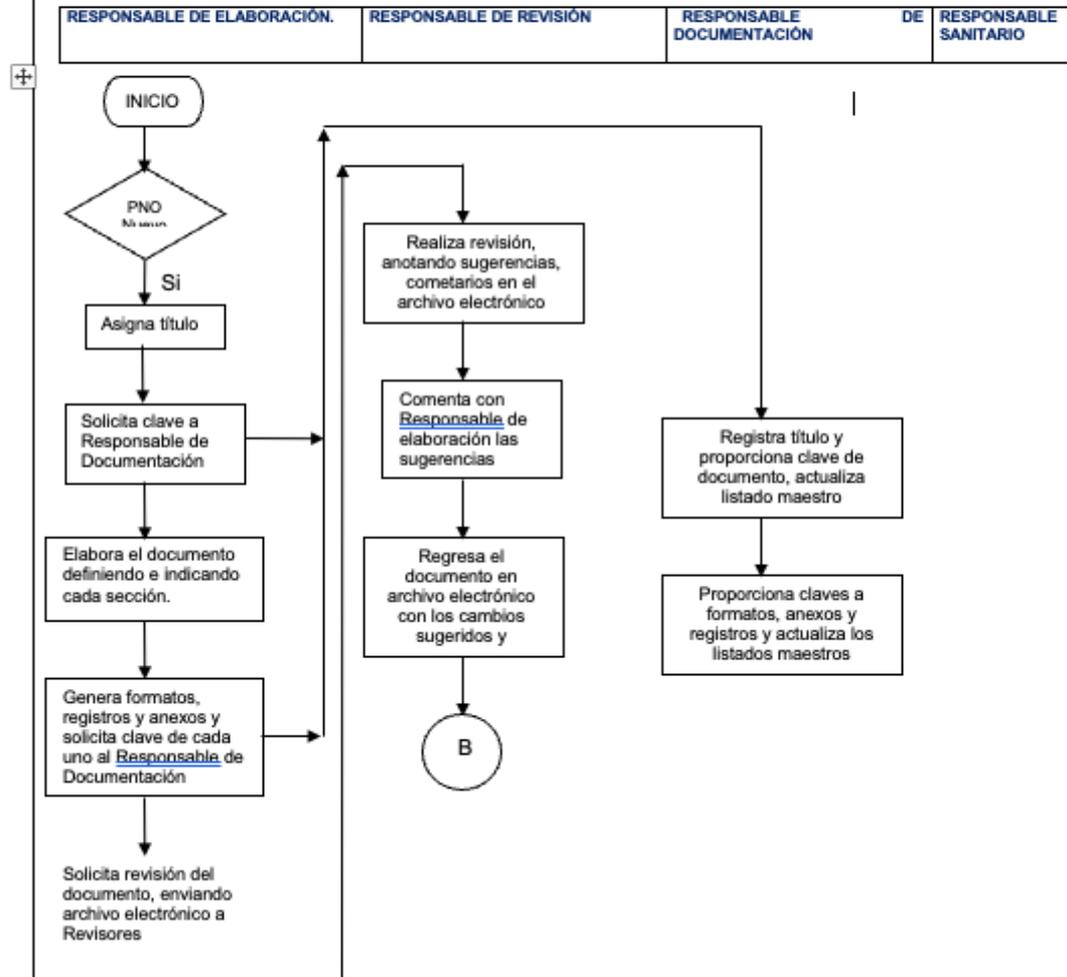
¿Cuál es el Objetivo de un Procedimiento Estándar de Operación ?

1. Especificar y detallar las actividades y operaciones de un proceso, de forma ordenada y secuencial.
2. Identificar a los responsables de la ejecución de cada etapa del proceso.

TÍTULO:		
FECHA DE EMISIÓN:	FECHA DE VIGENCIA:	PÁG. 2 DE

Diagrama de flujo del proceso (Permite identificar responsables de las actividades, los puntos críticos del proceso descrito y establecer la secuencia lógica del mismo)

9.0 DIAGRAMA DE FLUJO



PROCEDIMIENTO NORMALIZADO DE OPERACIÓN



Logo	TÍTULO:	
DEPARTAMENTO EMISOR:		
CODIGO:	VERSIÓN:	SUSTITUYE A:
FECHA DE EMISIÓN:	FECHA DE VIGENCIA:	PÁG. <u>1</u> DE

SECCIÓN DE FIRMAS

Elaboró, Reviso, Autorizo

- 1.0 Objetivo
- 2.0 Alcance
- 3.0 Responsabilidades
- 4.0 Definiciones y Generalidades
- 5.0 Desarrollo del Proceso
- 6.0 Formato y Anexos
- 7.0 Referencias Bibliográficas
- 8.0 Histórico de Cambios
- 9.0 Registros de Calidad
- 10.0 Diagrama de Flujo

5.0 Desarrollo del Proceso Personal que elabora el PNO	Elaboración de Nuevos Procedimientos.
Jefe de área	Revisión de Procedimientos.
Gerente de área	Aprobación del Procedimiento

5.0 FORMATOS Y ANEXOS:

LISTADO DE FORMATOS	
CLAVE FORMATO	NOMBRE

6.0 REFERENCIAS BIBLIOGRAFICAS

7.0 HISTORICO DE CAMBIOS

VERSIÓN	DESCRIPCION DEL CAMBIO / JUSTIFICACION	FECHA

8.0 REGISTROS DE CALIDAD:

Nombre del registro	Responsable de su custodia	Tiempo de retención.

PNO ELABORACIÓN DE PROCEDIMIENTOS ESTÁNDAR DE OPERACIÓN

PROCEDIMIENTO NORMALIZADO DE OPERACIÓN

Logo

TÍTULO: **Elaboración de procedimientos estándar de operación**

DEPARTAMENTO EMISOR : **Documentación**

CÓDIGO:
PF-D0-001

VERSIÓN: **02**

SUSTITUYE A:
Versión 01

FECHA DE EMISIÓN:

Jul 2024

FECHA DE VIGENCIA:

Jul 2027

PÁG. **1 DE 3**

SECCIÓN DE FIRMAS

	PUESTO	FIRMA Y FECHA
ELABORADO POR:		
REVISADO POR:		
AUTORIZADO POR:		

PNO ELABORACIÓN DE
PROCEDIMIENTOS
ESTÁNDAR DE
OPERACIÓN



PNO ELABORACIÓN DE PROCEDIMIENTOS ESTÁNDAR DE OPERACIÓN



1. OBJETIVO:

Establecer los lineamientos a seguir para la elaboración, emisión, revisión, aprobación y autorización de los Procedimientos Normalizados de Operación.

2. ALCANCE:

Este PNO aplica para la elaboración, emisión, revisión y aprobación de todos los procedimientos normalizados de operación elaborados en :
XXXX

3. RESPONSABILIDADES:

Es responsabilidad del personal asignado a la elaboración Procedimientos Normalizados de Operación:

4. DEFINICIONES Y GENERALIDADES:

Del PNO que se esté elaborando



3. Responsabilidades



Es responsabilidad del personal involucrado en el proceso como: Químicos, Coordinadores, líderes, Gerentes y Dirección General.

- ✓ Dar revisión, seguimiento y/o aprobar los Procedimientos Normalizados de Operación verificando que se cumplen los lineamientos internos y regulatorios descritos en el PNO.
- ✓ Asignar a personal capacitado para la elaboración de Procedimientos Estándar de Operación



Es responsabilidad del personal asignado a la elaboración de procedimientos normalizados de operación.

3. Responsabilidades

- ✓ Cumplir con los lineamientos descritos en el PNO de elaboración de procedimientos normalizados de operación.
- ✓ Dar aviso de cualquier necesidad de modificación al PNO de elaboración de procedimientos estándar de operación



3. Responsabilidades Asignadas

Es responsabilidad del personal asignado al control de la documentación:

Asignar la clave de identificación a cada procedimiento, así como distribuirlo, controlarlo y conservarlo por el tiempo requerido, así como asegurarse de la revisión y la actualización oportuna de acuerdo a lo descrito en el ***PNO de Control de Documentos.***

PNO ELABORACIÓN DE PROCEDIMIENTOS ESTÁNDAR DE OPERACIÓN



5.0 DESARROLLO DEL PROCESO:

- Redacción:
- Verbos en conjugados en tercera persona: (**Utilice, realice, elabore, asigne**, etc.)
- Indicar con precisión quién, cómo, cuándo, cómo
- Hacer referencias cruzadas a métodos, formatos, PNOS, etc.
- Generar los formatos de registro necesarios
- Recolección de firmas
- Capacitar el PNO
- Emitir el PNO



PNO ELABORACIÓN DE PROCEDIMIENTOS ESTÁNDAR DE OPERACIÓN



6. LISTADO DE FORMATOS:

LISTADO DE FORMATOS	
CLAVE	NOMBRE
F1-PF-DO-001	PROCEDIMIENTO NORMALIZADO DE OPERACIÓN.
F2-PF-DO-001	LISTADO MAESTRO DE PROCEDIMIENTOS Y FORMATOS
F3-PF-DO-001	SOLICITUD PARA NUEVO DOCUMENTO
F4-PF-DO-001	REGISTRO DE CAPACITACION.
F5-PF-DO-001	EXÁMEN DE CAPACITACIÓN



7. BIBLIOGRAFÍA:

8.0 HISTORICO DE CAMBIOS

VERSIÓN	DESCRIPCION DEL CAMBIO / JUSTIFICACION	FECHA

9. DIAGRAMA DE FLUJO:

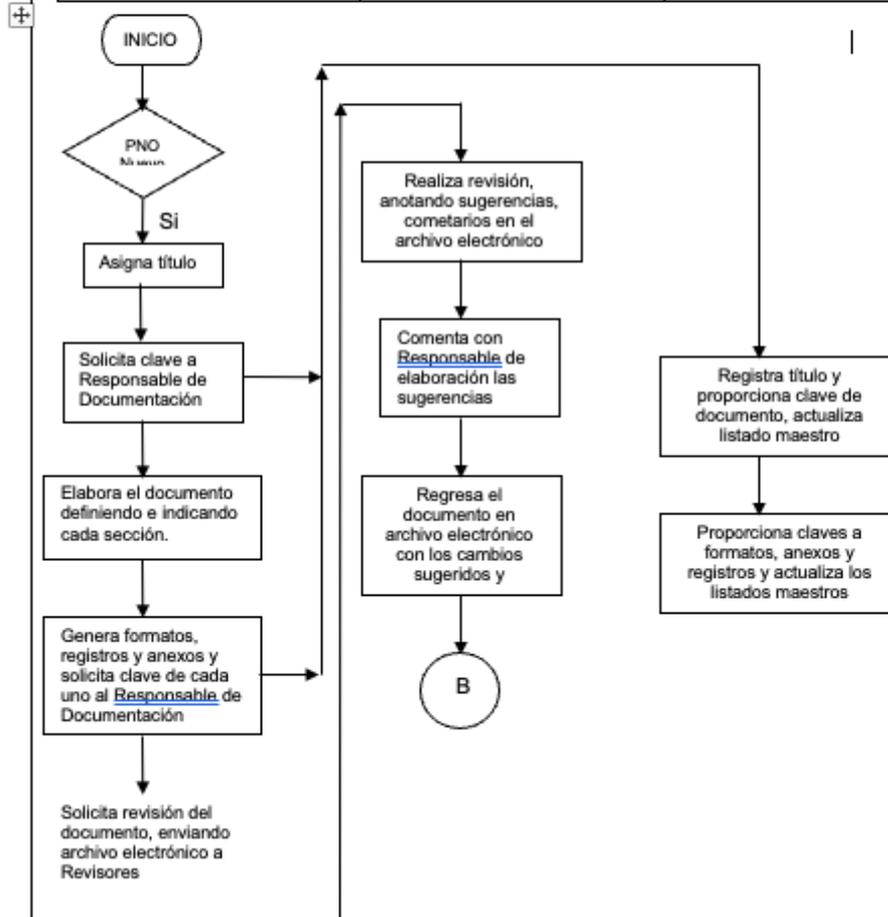
PNO ELABORACIÓN DE PROCEDIMIENTOS ESTÁNDAR DE OPERACIÓN



TÍTULO:		
FECHA DE EMISIÓN:	FECHA DE VIGENCIA:	PÁG. 2 DE

9.0 DIAGRAMA DE FLUJO

RESPONSABLE DE ELABORACIÓN.	RESPONSABLE DE REVISIÓN	RESPONSABLE DOCUMENTACIÓN	DE	RESPONSABLE SANITARIO
-----------------------------	-------------------------	---------------------------	----	-----------------------



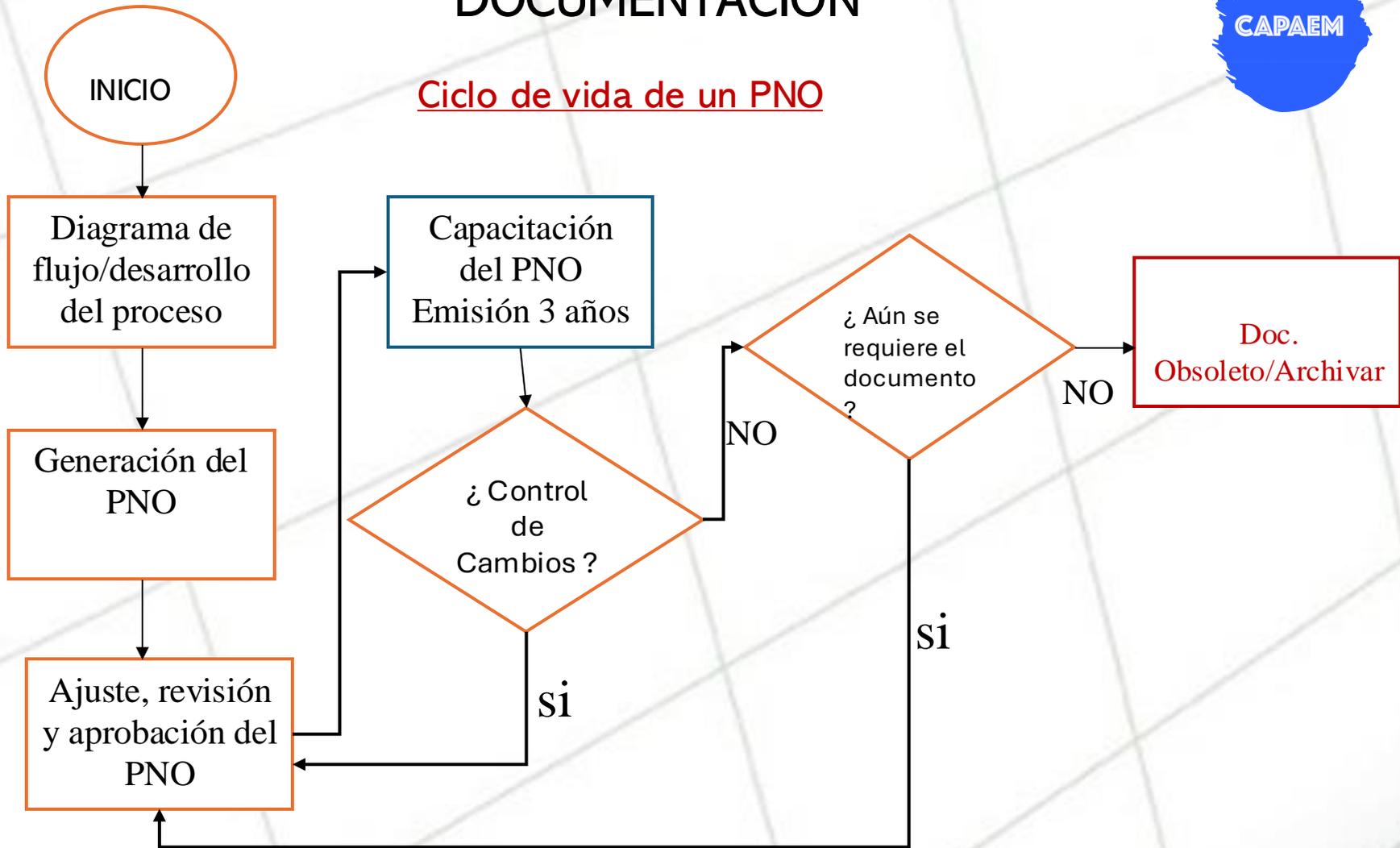


Cualquier modificación realizada a un PNO y/o documento del Sistema de Gestión de la Calidad estará previamente autorizada de acuerdo al procedimiento de **control de cambios**.

BUENAS PRACTICAS DE DOCUMENTACION



Ciclo de vida de un PNO





2. PNO de elaboración y control de documentos

La estructura y características del documento como:

- Clasificación de los documentos (procedimientos, instructivos, registros, protocolos, reportes, etc.)
- Codificación/Identificación (por áreas, departamentos, gerencias, etc.)
- Contenido del Encabezado y de pie de página
- Cómo se debe de hacer la redacción de cada punto (tipo de letra, tamaño de letra, espaciado entre renglones, numeración, sangrías, uso de negritas, subrayado, etc.)
- Manejo de anexos, graficas, tablas, figuras, fotografías, diagramas, referencias bibliográficas, etc.



2. PNO de elaboración y control de documentos

- Cuándo y cómo se da de alta un nuevo documento
- Cómo se procede con la autorización y distribución
- Cómo se da la difusión/capacitación del nuevo documento
- Qué medidas de seguridad se utilizan para el control de las copias
- Cómo se hará el respaldo de los documentos, de datos electrónicos, cuándo, en dónde y definirá las responsabilidades.
- Cuando se debe o puede modificar un documento, el uso de control de cambios
- Vigencia de los procedimientos
- Actualización de procedimientos
- Baja de procedimientos

2. PNO Elaboración y control de documentos



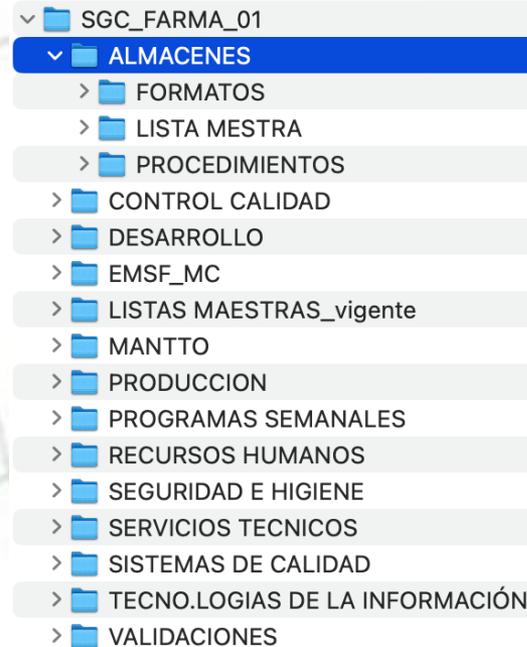
Tipos de documentos

Los documentos del SGC que describen los procesos de soporte dentro del alcance de la NOM-059-SSA 2015, se codifican y elaboran de acuerdo a los PNO que describen la elaboración de cada tipo de documento

Documento	Codificación Ver PNO
Bitácoras de Registro	PF-FQ-019
PNOS	PF-DO-001
Protocolo Estabilidad	PF-FQ-015
Especificación	PF-FQ-004
Ordenes de análisis	
Fórmulas Maestras	
Planes de Validación	
Orden maestra de producción	
Protocolo de Validación	
Orden Maestra de Acondicionamiento Requerimientos de usuario	
Protocolos de Validación de Métodos	
Hojas de Seguridad	
Manual de Calidad	
Expediente de sitio de fabricación	
Análisis de Riesgos	

2. PNO Elaboración y Control de documentos

1. Las responsabilidades para aprobar y autorizar los documentos antes de su emisión
2. Distribución de copias autorizadas y/o controladas
3. Control de la vigencia de los documentos y actualización
4. El método para identificar los cambios y el estado de la revisión de los documentos
5. El método para asegurar que las versiones vigentes de los documentos se encuentren disponibles en los lugares de uso y consulta
6. El método para prevenir el uso no intencionado de los documentos obsoletos y para que sean retirados.





3. PNO Registro de Datos y Buenas Prácticas de Documentación



3. PNO Registro de datos de Calidad y BPD

Definiciones



- ❖ **Registro de Calidad:** Evidencia de las acciones realizadas para demostrar cumplimiento de las instrucciones.
- ❖ **Trazabilidad:** a la capacidad de reconstruir la historia, localización de un elemento o de una actividad, por medio de registros de identificación.
- ❖ **BPD:** Buenas prácticas de documentación. Herramientas creadas para asegurar el empleo correcto y permanente de los documentos, con la finalidad de garantizar que las operaciones se llevaron a cabo de manera adecuada y permiten la trazabilidad oportuna de la información



3. PNO Registro de datos de Calidad y BPD

Definiciones



CAPAEM

- ❖ **Catálogo:** Relación ordenada en la que se incluyen o describen de forma individual libros, documentos, personas, objetos, etc. que están relacionados entre sí.
- ❖ **Cifras Significativas:** Dígitos necesarios para expresar la precisión de la medida.



3. PNO Registro de datos de Calidad y BPD

Proceso:



CAPAEM

- Usar bolígrafo de tinta azul indeleble (no plumón, pluma fuente) y letra de molde.
- Registrar los datos de una forma clara y concisa.
- Registrar los datos inmediatamente después de la actividad. Los registros extemporáneos documentarlos a través de una desviación.



3. PNO Registro de datos de Calidad y BPD

Proceso



CAPAEM

- No encimar, no sobre-escribir los datos.
- No utilizar corrector, marcador, plumones, bolígrafo de tinta de gel, lápiz, papeles autoadheribles (etiquetas o Post-it)

3. PNO Registro de datos de Calidad y BPD



Reglas de escritura

Utilizar el sistema internacional de unidades de medida para el registro de datos.

Utilizar formato de 24 h para el registro del tiempo

Ejemplo: 14:54 h

Registrar la fecha utilizando los siguientes formatos:

**Ejemplo: 24/Feb/2023 o
24-Feb-2023 o
24 . Feb . 2023 o 24/03/23**



3.0 PNO Registro de datos de Calidad y BPD



EJEMPLO DE UNIDADES AUTORIZADAS POR EL SISTEMA INTERNACIONAL DE UNIDADES.

MAGNITUD	UNIDAD	SÍMBOLO
Longitud	Metro	m
Masa	Kilogramo Tonelada	kg t
Tiempo	Segundo Minuto Hora Día Año	s min h d a
Temperatura termodinámica	Kelvin	K
Temperatura Celsius	Grado Celsius	°C
Cantidad de sustancia	Mol	mol
Superficie	Metro cuadrado	m ²

3. PNO Registro de datos de Calidad y BPD



Reglas de escritura

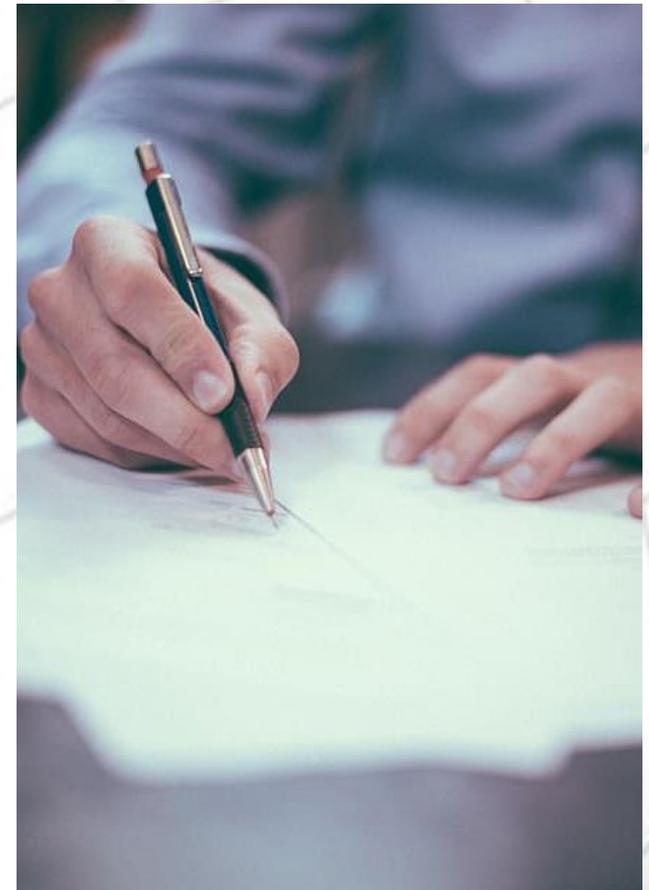
Para el reporte de resultados analíticos utilizar valores numéricos de acuerdo a lo indicado en la especificación o de acuerdo a la lectura del equipo.

Ejemplo: 0.1125 mg

Redondear los resultados numéricos al final de la operación.

Cuando el dígito a redondear es mayor o igual a 5, el siguiente dígito a la izquierda se incrementa.

Cuando el dígito a redondear es menor a 5, el dígito que se encuentra a su izquierda no sufre ninguna modificación



PNO Registro de datos de Calidad y BPD



Correcciones y Cancelaciones

Cruzar una línea diagonal de izquierda a derecha y de abajo hacia arriba.

Escribir el dato correcto al abajo, firmar y fechar.

Ejemplo:

Lote: ~~LM12001~~

LM12002

P. Pérez
24/Ene/2024

Registro de datos de Calidad y BPD



Correcciones y Cancelaciones

Ejemplo:

Corrección incorrecta

N/A P. Pérez 24-Oct-23

Lote: ~~AJK149J008-NF~~ NE

N/A P. Pérez 24-Oct-23

Corrección correcta

N/A P. Pérez 24-Oct-23

Lote: ~~AJK149J008-NF~~ AJK149J008-NE

Registro de datos de Calidad y BPD



Cancelaciones de espacios en blanco

- Ejemplo:

	P. Pérez	Resultado en %
Lactosa anhidra lote : KLAAN-01	24/Ene/2024	0.8
Lactosa monohidrato lote: KLMON-02		6.9

N/A

P. Pérez
24/Ene/2024

PNO Registro de datos de Calidad y BPD



Firmas

Firma: Inicial del nombre y primer apellido de acuerdo a lo registrado en el catalogo de firmas

Cuando en un documento se involucre el nombre de la persona, utilizar la firma de acuerdo al catálogo de firmas.

Al ingreso de un empleado se debe capacitar en el presente PNO de BPD y registrar su firma en el catálogo de firmas.

Firma por ausencia la persona que tenga en mismo nivel jerárquico o superior, anteponiendo las siglas "P.A.", en el momento que no se encuentre la persona solicitada

Actualizar el catálogo de firmas cada año.

En caso de que antes del año ocurra algún cambio, como promoción o baja de un empleado registrar en el catálogo de firmas la modificación indicando la fecha

PNO Registro de datos de Calidad y BPD

Firma Electrónica



Diferencia entre registro manual y registro electrónico:

Registro manual:

Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas escritas a mano.

Registro electrónico:

Conjunto de información que incluye datos electrónicos (texto, números, gráfico) que es creado, modificado, mantenido, archivado, restaurado o transmitido a través de un sistema computarizado.



Firma electrónica: compilación de datos de diversos símbolos o serie de símbolos ejecutados, adoptados o autorizados por una persona para que se relacionen legalmente a su firma en manuscrito.

La **firma electrónica** es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

Identificar al firmante de manera inequívoca.
Asegurar la integridad del documento firmado.

Password o contraseña

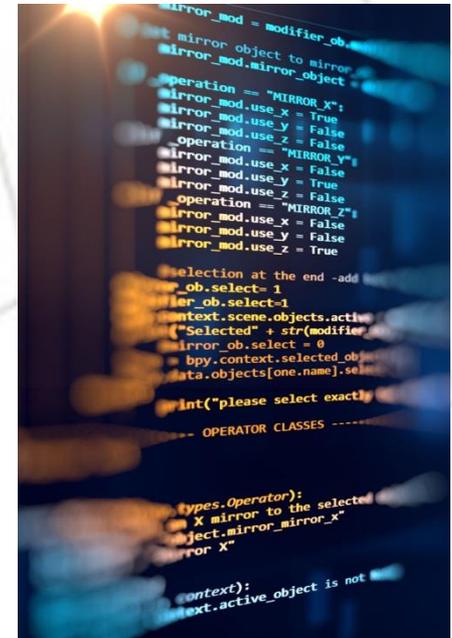
Una firma escaneada **No es una firma electrónica, ni digital, ni biométrica**



Firmas electrónicas



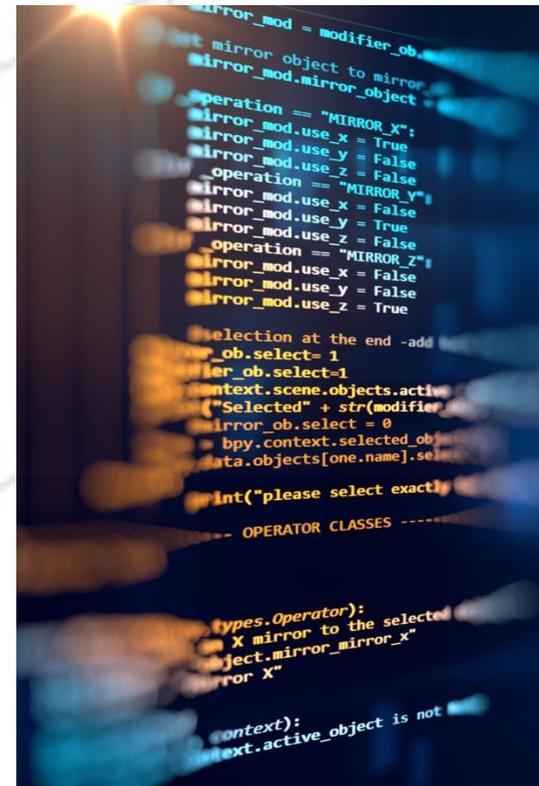
- Deben ser Únicas e intransferibles
- Emplear al menos dos elementos distintos tales como un ID (código) y una contraseña
- El aseguramiento de que la emisión de los ID y contraseñas sea revisada, renovada o revisada periódicamente.



Firmas electrónicas



- Mecanismos de protección de las transacciones para evita el uso no autorizado
- Establecer la fecha a partir de la cual las firmas electrónicas son vigentes y equivalentes a las formas en manuscrito (autógrafas)





Biometrica:

Método para verificar la identidad de un individuo sobre la base de la medida de las características físicas del individuo o de acciones repetibles, siempre que estas características o acciones sean a la vez únicas y mensurables para ese individuo

Algunos ejemplos son:

Huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano.



Resguardo de la documentación



- El área de documentación realiza el resguardo de los documentos originales físicos y de los archivos electrónicos
- Control de acceso a área de resguardo, personal autorizado y registro de consulta.
- Se debe contar con el proceso para garantizar que los documentos no se van a “perder en caso de un siniestro”



Resguardo de la documentación

The logo for CAPAEM, consisting of a blue brushstroke shape with the text "CAPAEM" in white capital letters inside it.

CAPAEM

- Expediente de lote

Un año después de la caducidad del producto.

- Protocolos

Hasta que haya un cambio, se guarda el histórico

PNOS

- 3 años a al momento de sufrir un cambio.





Qué documentos y registros debe conservar una organización.

Las expectativas regulatorias son:

Verificar los procesos, productos, materiales, proveedores, equipos, instalaciones y sistemas de distribución.

Los documentos y registros que demuestren que un medicamento fabricado cumplió con los requisitos de Pureza, identidad, seguridad, eficacia e inocuidad.



Qué documentos y registros debe conservar una organización.

Deben estar disponibles los documentos que permitan trazar la historia de la fabricación de un medicamento desde el ingreso de materiales pasando por la fabricación, control y distribución.

- Procedimientos
- Planes específicos de análisis
- Registros e informes.
- Expediente de fabricación
- Protocolos y Reportes
- Todo aquello que se requiera demostrar cumplimiento de la regulación

**¡¡ Gracias por
su atención !!**

