



UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO



FACULTAD DE QUÍMICA

**INTEGRIDAD DE DATOS EN SISTEMAS COMPUTARIZADOS DE LA
INDUSTRIA FARMACEUTICA**

ENSAYO

Que para obtener el Título de:

INGENIERO QUÍMICO

Presenta:

LUIS GREGORIO GARCÍA ORTIGOZA

Asesor académico: Dr. Julián Cruz Olivares

TOLUCA, MÉXICO

Agosto 2025

Contenido

INTEGRIDAD DE DATOS EN SISTEMAS COMPUTARIZADOS DE LA INDUSTRIA FARMACEUTICA.....	1
Objetivo.....	4
Desarrollo	6
Industria farmacéutica.	7
Elaboración de Fármacos	8
Buenas Prácticas farmacéuticas	8
Aseguramiento de calidad.....	9
Calidad.....	9
Auditoria.....	10
Actividades GxP	11
Buenas prácticas de documentación.....	11
Buenas prácticas de laboratorio.....	11
Integridad de Datos	13
ALCOA plus.....	13
Agencias reguladoras.....	14
COFEPRIS (Comisión Federal para la Protección contra Riesgos Sanitarios).....	14
FDA (Por sus siglas en ingles Food and Drug Administration- Agencia de Alimentos y Medicamentos)	14
CFR 21 PART 11 (Code of Federal Regulations Parte 11)	15
EMA (Por sus siglas en ingles European Medicines Agency)	15
INVIMA (Instituto Nacional de Vigilancia de Medicamentos y Alimentos)	16
Validación.....	16

Sistemas Computarizados	17
Componentes de un sistema computarizado	20
Sistemas computarizados globales	20
Registro electrónico	22
Firma electrónica	22
Audit Trail	23
Normatividad local de los sistemas computarizados	23
Criterios para firmas electrónicas	24
Validación de sistemas computarizados	25
Líder del proyecto	26
Dueño del sistema	27
Dueño del proceso	27
Área de Validación de sistemas computarizados	28
Fases de la validación de los sistemas computarizados	28
Planeación	28
Especificar y diseñar	29
Especificación de Requerimientos de Usuario (ERU)	29
Construir y probar	31
Análisis de riesgos	32
Documentación técnica	33
Especificación de configuración	34
Descripción de Roles	34
Los roles que se consideraran en este trabajo son	35

Matriz de accesos y privilegios.	37
Listado de Usuarios.	38
Ejecución	40
Calificación de infraestructura	41
Calificación de Instalación.	42
Protocolo de Pruebas de Aceptación en Sitio.	42
Protocolo de Aceptación de Usuario	43
Control	44
Retiro	46
Revisión Anual de Audit Trail del sistema computarizado	49
Revisión periódica de Audit Trail.	54
Conclusiones.	57
REFERENCIAS BIBLIOGRAFICAS	61

INTEGRIDAD DE DATOS EN SISTEMAS COMPUTARIZADOS DE LA INDUSTRIA FARMACEUTICA.

Introducción

La industria farmacéutica ha evolucionado a lo largo de la historia, desde la obtención, uso y comercialización de lociones; obtención de tinturas, extractos y pomadas en pequeños laboratorios por parte de los boticarios; hasta la creación de fármacos biotecnológicos adaptados al perfil genético de cada paciente. La revolución industrial, con la construcción de nueva maquinaria permitió la elaboración masiva de los medicamentos, dando origen a un nuevo sector: la industria farmacéutica, que a partir de entonces adquirió la responsabilidad de la investigación, desarrollo y comercialización de nuevos medicamentos ^(1,2). Y aunque han existido desaciertos como la Talidomida (un fármaco que provocó el nacimiento de bebés con problemas en extremidades) ⁽³⁾, en general la evolución de la industria farmacéutica ha favorecido que la humanidad pueda tener una mejor calidad de vida.

Hoy en día la industria farmacéutica enfrenta muchísimos retos, el más reciente, durante la pandemia fue obtener una vacuna en tiempo récord contra el virus del COVID 19, mismo que ha generado 182 millones de contagios y 3.95 millones de muertes en el mundo ⁽⁴⁾. La obtención de la vacuna fue posible gracias a los avances científicos y tecnológicos a los que el hombre ha llegado; y al esfuerzo en conjunto de los gobiernos y las diferentes empresas participantes, trabajando en conjunto con el único objetivo de encontrar una vacuna que fuera eficaz y tuviera la potencia necesaria para combatir al virus antes mencionado.

La elaboración de los medicamentos, resulta ser un trabajo en conjunto que requiere la suma de esfuerzos de diferentes áreas de una empresa. En términos generales, dichas áreas son: almacén, mantenimiento, aseguramiento de calidad, laboratorio de análisis fisicoquímico, producción, recursos humanos, finanzas, validación, por mencionar algunas; es importante mencionar que ningún área es más importante que otra, si no que la sinergia de estas va dirigida a un fin común, el cual es el bienestar y mejorar la calidad de vida del paciente. Dependiendo de la organización y la filosofía de trabajo de las empresas farmacéuticas estas áreas pueden tener los

nombres antes mencionados, u otros diferentes, incluso la fusión de algunas de estas áreas.

A lo largo del proceso productivo de la manufactura de un medicamento se genera información que nos ayuda a asegurar la identidad, concentración, inocuidad y potencia de dicho fármaco. Características mínimas necesarias, que deben tener los medicamentos para poder ser administrados y consumidos con confianza. La información que se genera en los laboratorios de análisis fisicoquímico y microbiológico de la industria farmacéutica es salvada en papel y lápiz, posteriormente puede ser documentada en bitácoras físicas para poder dar cumplimiento y certeza de las buenas prácticas de laboratorio normadas por las diferentes entidades regulatorias. En el caso de las áreas de manufactura y almacén, la información se descarga en expedientes físicos los cuales integran toda la historia de un determinado número de piezas fabricadas de un producto desde el arribo de cada uno de sus materiales que lo componen, hasta su despacho como producto terminado en los andenes del almacén.

Sin embargo, algunas otras industrias farmacéuticas enfocadas en la mejora continua de sus procesos y que cuentan con ciertos recursos, generan y documentan la información en sistemas computarizados, desde la recepción de los materiales, el análisis de las materias primas, materiales, graneles, semiterminados, y productos terminados; hasta el despacho de los productos terminados; todo el proceso es seguido y documentado de forma digital.

Toda actividad que se ejecute en la industria farmacéutica debe ser confiable e íntegra. El generador de información máquina o persona debe de cumplir con ciertos criterios que aseguren que esta es apegada a la integridad de datos para poder asegurar el cumplimiento regulatorio que exigen las entidades regulatorias nacionales como extranjeras. La Integridad de Datos se refiere a la precisión y legibilidad de los datos respaldados, para eso toda información deberá ser legible, entendible, la información debe ser registrada en el momento que se originó, o una

copia fiel de la información original y exacta. Además de deben poder ser descargados, salvados y rastreables ⁽⁴⁾.

El tener una trazabilidad de la información, ayuda a la industria farmacéutica a encontrar la causa raíz en situaciones que puedan llegar a presentarse, así como tener la información disponible para cualquiera que sea el interés de la documentación, como puede ser trabajar en la mejora continua de los procesos y/o productos.

Todo proceso en manufactura, laboratorios, áreas de aseguramiento de calidad, logística o distribución que genere información relacionada con la calidad del producto, debe retarse, en cuanto a su función y desempeño por medio de pruebas de reproducibilidad y repetitividad, proceso al cual llamamos validación, según la Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas prácticas de fabricación de medicamentos, define a la Validación como, la evidencia documental generada a través de la recopilación y evaluación científicas de los datos obtenidos en la calificación y de las pruebas específicas, a lo largo del todo el ciclo de vida de un producto, cuya finalidad es demostrar la funcionalidad, consistencia y robustez de un proceso dado en cuanto a su capacidad para entregar un producto de calidad.

Para el caso de los sistemas computarizados es un conjunto de elementos que la Norma Oficial Mexicana NOM-059-SSA1-2015 en su numeral 9.13.1 indica que aquellos que impactan la calidad del producto e integridad de datos deben validarse, pero no indica los pasos a seguir, sin embargo, existen más Normas y regulaciones internacionales de las cuales se apoya la industria farmacéutica nacional para definir y normar el proceso de validación de sistemas computarizados y así poder garantizar la integridad de datos de la información que generan y procesan estos últimos.

Objetivo

- El objetivo del presente trabajo es evidenciar la importancia de la integridad de datos en los sistemas computarizados en la industria farmacéutica.

- Que el presente trabajo sea una guía para el lector, cuando llegue a tener la tarea de asegurar la integridad de los datos de los registros electrónicos emitidos por sistemas computarizados, teniendo las bases y los conocimientos necesarios para diseñar los planes y estrategias a realizar.

Desarrollo

Industria farmacéutica.

Se entiende a la industria farmacéutica como al sector empresarial dedicado a la fabricación, preparación y comercialización de productos químicos medicinales para el tratamiento y prevención de las enfermedades ⁽⁵⁾. Es un sector con elevado nivel de desarrollo, especialización, investigación e innovación. Siendo la innovación una necesidad intrínseca del sector, para la preservación del valor de la vida humana ⁽⁶⁾. Para lo cual es necesario que los proyectos paseen por varios años de investigados, para garantizar la concentración, inocuidad y potencia, de los mismos.

Esta industria llego a México en la última década siglo XIX, pues establecieron en México empresas farmacéuticas extranjeras que importaban sus medicamentos sintetizados químicamente y ya dosificados, lo que hacía más fácil su administración; desplazando a las antiguas boticas. Pero a mediados del siglo XX iniciaron la producción en nuestro país, a finales de este siglo, la medicina de patente y la especialidad farmacéutica estaban en su apogeo⁽⁷⁾.

En 1940 nuestro país se convirtió en el principal proveedor de hormonas esteroideas El doctor Rusell Marker encontró en las dioscórea (la diosgenina o sapogenina) la estructura básica del ciclo pentano-perhidrofenantreno, que es el precursor de todas las hormonas esteroideas: corticoides, progestágenos, estrógenos y andrógenos ⁽⁸⁾. Pero el uso desmedido de la planta generó su agotamiento, teniendo que recurrir a la síntesis del compuesto.

Actualmente la industria farmacéutica en México cuenta con aproximadamente 200 empresas, que cuentan con muy buenas instalaciones, equipo y tecnología; así como personal preparado; con lo cual abastecen a más del 70% de las necesidades del país ⁽⁸⁾.

Elaboración de Fármacos

Lograr un nuevo medicamento es un proceso complejo, que requiere una gran cantidad de tiempo y dinero; y está sometido a una creciente cantidad de exigencias por los organismos reguladores ⁽⁹⁾.

La fabricación o proceso de manufactura son todas aquellas operaciones involucradas en la elaboración o producción de un medicamento desde la recepción de insumos, liberación, almacenamiento y distribución como producto terminado.

Todas y cada una de las actividades dejan un rastro, un historial de quién, qué y cuándo se realizó la actividad, esta puede ser en físico o electrónico, es fundamental que esta información esté disponible para su consulta futura y la organización debe de asegurar mediante procedimientos que la información estará disponible para su consulta. La disponibilidad, legibilidad, precisión y atribución de los datos es vital para la toma de decisiones, mejora continua y estandarización de los procesos.

Los procesos de la industria farmacéutica deben estar estandarizados, lo cual significa que todas y cada una de las acciones a realizar se ejecutan con una metodología o receta, cuando estas se modifican, debe hacerse de manera planeada y controlada, para lo cual existe los controles de cambio y cuando no se hacen de manera planeada la acción se documenta en una desviación.

Buenas Prácticas farmacéuticas

Para la elaboración de un medicamento es obligatorio cumplir con ciertas normas de correcta fabricación (NCF) que permitan garantizar la calidad y seguridad para el paciente, la aplicación de estas normas va desde las materias primas, almacenamiento, fabricación y distribución ⁽¹⁰⁾. La calidad de las materias primas se certifica rutinariamente y es de suma importancia seguir el desarrollo del proceso.

Aseguramiento de calidad.

Conjunto de actividades planeadas y sistemáticas que lleva a cabo una empresa, con el objeto de brindar la confianza, de que un producto o servicio cumple con los requisitos de calidad especificados. (Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas Prácticas de Fabricación de Medicamentos, DOF 05/02/2016).

Aseguramiento de Calidad en la industria Farmacéutica se concibe como un área, con integrantes reconocidos uno a uno como la autoridad de calidad, quienes tienen los conocimientos técnicos necesarios para poder tomar decisiones al respecto de los procesos o productos dada una situación la cual puede ser no planeada o fuera de lo normado. La gestión de las operaciones de Aseguramiento de Calidad, así como los registros normativos pueden administrarse en un Sistema de Gestión de calidad, en el mercado existen diferentes tipos de Sistemas de gestión de calidad.

Calidad.

La Norma Oficial Mexicana NOM-059-SSA1-2015, indica que la calidad es cumplir con lo requerido con el cliente en productos o servicios, es decir que lo que entregamos al cliente va a satisfacer sus necesidades, por las cuales nos solicitó el producto o servicio. Es importante tener un estándar, una especificación la cual se convierte en una guía de los pasos y procedimientos a seguir de manera repetitiva para entregar siempre productos de calidad.

Como se mencionó anteriormente, todos los procesos que se realizan en la industria farmacéutica son realizados siguiendo un procedimiento de operación el cual debe estar alineado a los requerimientos regulatorios, el seguir esta práctica asegura la calidad en los productos o servicios. La actividad con la cual los sitios se aseguran de que las actividades que se realizan obedecen a los procedimientos de operación se conoce como Auditoria.

Auditoria.

Es un proceso sistemático, independiente y documentado para obtener evidencias y evaluar de manera objetiva el proceso de fabricación de los medicamentos, con el fin de determinar el nivel en que se cumplen los criterios establecidos por la Norma Oficial Mexicana NOM-059-SSA1-2015 (Buenas Prácticas de Fabricación de Medicamentos, 2016, 05 de febrero). No solo se evalúan los criterios de la norma mexicana, ya que la auditoria puede ser de un organismo extranjero. Los criterios establecidos por la NOM 059, deben estar documentados en los procedimientos de operación y especificaciones de productos o servicios que serán destinados para el cliente. El proceso de auditoria es y debe ser realizado por un externo, existen sitios que definen ejercicios de auditoria con personal y recursos del mismo sitio para identificar los posibles hallazgos de incumplimientos de los procedimientos, esto ayuda a ser oportunos y corregir los errores en lo que se estén incurriendo.

Un proceso de auditoria no debe de sentirse como un enemigo, pues los hallazgos indican las áreas de oportunidad que los sitios tienen. Los sitios no deben de prepararse para recibir a una Auditoria ya que en su mayoría, después de agendada la auditoria el sitio se prepara para recibirla y es como arreglar la casa cuando se recibirán visitas, lo correcto sería que el sitio estuviese prepara para recibir a un auditoria en cualquier día del año, es decir, que sus procesos están suficientemente robustos y estandarizados, y están alienados al día en los requerimientos regulatorios nacionales e internaciones, motivo por el cual los sitios deben de estar atentos a las actualizaciones de las regulaciones a la cuales están en cumplimiento regulatorio. Para el caso de la norma Mexicana NOM-059-SSA1-2015, su actualización se publica en el Diario Oficial de la Federación, y en este documento oficial, en el apartado de transitorios se menciona el tiempo en el cual los sitios de manufactura de productos farmacéuticos tendrán que cumplir los requerimientos regulatorios de dicha Norma.

Actividades GxP

Por sus acrónimos en inglés entendamos a aquellas actividades GxP, como Good: Buenas, x: todas aquellas actividades que se desarrollan desde la manufactura, hasta la distribución de un fármaco e impactan directamente la calidad del producto., Practices: Prácticas. De esta forma cuando nos refiramos a actividades GxP se entenderá que son Buenas Prácticas de... manufactura, laboratorio, distribución, logística, por mencionar algunas.

Buenas prácticas de documentación.

Conjunto de reglas y lineamientos relacionadas entre sí que garantizan la trazabilidad documental en cada una de las actividades GMP (Good Manufacturing Practice-Buenas Prácticas de Manufactura) y no GMP, (Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas Prácticas de Fabricación de Medicamentos, 2016, 05 de febrero). Debemos de considerar que las buenas prácticas de documentación se realizan en papel o bien en sistemas computarizados. Existe una relación directa entre las Buenas prácticas de documentación y la integridad de datos, ya que ambas indican que un registro debe de tener dueño y que las actividades deben ser registradas por quien la realizo de forma contemporánea y precisa.

Buenas prácticas de laboratorio

Conjunto de reglas, procedimientos operacionales y prácticas establecidas para asegurar la calidad e integridad de las actividades realizadas en el laboratorio y de los datos analíticos obtenidos de ensayo y pruebas. (Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas Prácticas de Fabricación de Medicamentos, 2016, 05 de febrero). Los analistas de laboratorio, en su mayoría realizan actividades relacionadas directamente con la liberación del producto y la calidad de este; donde cada actividad debe estar correctamente documentada, debe de poder trazarse de tal forma que se pueda visualizar, quien la realizó, cuando se realizó; la información generada debe ser original, precisa y legible, adicional a esto, esta información debe de estar disponible para su consulta futura.

Buenas prácticas de almacenamiento y distribución.

Son parte del aseguramiento de calidad, el cual garantiza que la calidad de los medicamentos es mantenida a través de todas las etapas de la cadena de suministro desde el sitio de fabricación hasta la farmacia. Se debe de garantizar que se cumplan las especificaciones de almacenamiento y distribución de las materias primas, semiterminados y terminados, que la exposición a la temperatura y humedad estén dentro de lo que indican las condiciones de almacenamiento del producto.

Buenas prácticas de fabricación

Conjunto de lineamientos y actividades relacionadas entre sí, destinadas a asegurar que los medicamentos elaborados tengan y mantengan las características de identidad, pureza, seguridad, eficacia y calidad requeridas para su uso. (Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas Prácticas de Fabricación de Medicamentos, 2016, 05 de febrero). Las buenas prácticas de fabricación son todas aquellas operaciones que se realizan en el espacio físico destinado a la manufactura de los medicamentos, toda actividad que se realice debe estar normada en un procedimiento de operación alineado a las normas aplicables nacionales o internaciones. La manufactura de un fármaco como producto final podemos dividirla en dos etapas. La fabricación de mezclas, semiterminados o producto terminado, este es el fármaco en su forma farmacéutica, el cual puede ser solida o líquida. Después pasamos al acondicionado, es decir colocar el fármaco en un recipiente que no interactúe y provoque degradación o reacción química con este y un empaque de presentación de venta.

Toda actividad debe estar documentada en los expedientes de fabricación los cuales pueden ser físicos o electrónicos, en ellos se documentan los parámetros críticos de las diferentes actividades que se realizan para obtener un producto terminado.

Integridad de Datos

La integridad de los datos se refiere a la integridad, coherencia y precisión de los datos. Los datos completos, consistentes y precisos deben ser atribuibles, legibles, registrados contemporáneamente, originales o una copia auténtica y preciso, lo anterior describe el termino ALCOA. (Department of Health and Human Services Food and Drug Administration, 2018). La integridad de los datos debe estar presente desde que se genera el dato y debed existir controles que aseguren que no puede modificarse, que se puede almacenar, respaldar, y restaurar de manera segura.

La integridad de los datos es fundamental a lo largo del ciclo de vida de los datos de GMP, incluida la creación, modificación, procesamiento, mantenimiento, archivo, recuperación, transmisión y disposición de los datos una vez finalizado el período de retención del registro. El diseño y los controles del sistema deben permitir una fácil detección de errores, omisiones y resultados aberrantes a lo largo del ciclo de vida de los datos.

ALCOA plus.

ALCOA plus complemento de ALCOA, e implica más seguridad del registro generado, asegurando que este sea Integro, Consistente, Perdurable y esté Disponible para las necesidades de consulta. se describe en la Tabla No. 1.

ALCOA	Descripción
Atribuible	Los datos deben indicar quién y cuándo fueron realizados. Cualquier cambio introducido debe ser notificado con las informaciones de quién, cuándo y porqué. Los datos deben indicar su origen
Legible	Los datos deben ser guardados de forma permanente en un formato duradero de forma que puedan ser leídos
Contemporáneo	Los datos deben ser recogidos en el mismo momento de la realización del trabajo, así como la fecha y la hora en este mismo orden
Original	Los datos deben ser identificados como originales o copias exactas certificadas
Preciso	Cualquier cambio introducido debe ser notificado con las informaciones de quién, cuándo y porqué
Íntegro	Los datos deben incluir todos los análisis efectuados en una misma muestra (repetidos, reanálisis)
Consistente	Se espera una secuencia lógica al notificar fecha y hora del dato
Perdurable	Los datos recogidos en hojas de trabajo, cuadernos de laboratorios, en formato electrónico han de ser leibles a lo largo tiempo
Disponible	Los datos asociados deben estar disponibles y accesibles para su revisión y auditoría

Tabla No. 1⁽¹⁵⁾

Agencias reguladoras.

La industria farmacéutica es una de las más reguladas debido a su impacto en la salud humana, los fabricantes de medicamentos deben estar en cumplimiento a los criterios de las diferentes regulaciones y legislaciones según el país donde se fabriquen y/o comercialicen sus productos. Hoy existen tratados internacionales que determinan criterios para la liberación y comercialización de ciertos productos farmacéuticos.

A continuación, enlistamos algunos organismos reguladores de la industria farmacéutica de México y el mundo.

COFEPRIS (Comisión Federal para la Protección contra Riesgos Sanitarios)

Organismo mexicano derivado de la secretaria de salud, encargada de la verificación de las buenas prácticas de laboratorio mediante la Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas Prácticas de fabricación de medicamentos, publicada en el Diario Oficial de la Federación el 05/02/2016.

FDA (Por sus siglas en ingles Food and Drug Administration- Agencia de Alimentos y Medicamentos)

Caracterizada por ser una de las agencias regulatorias más importantes en el mundo, sus altos estándares de calidad y minuciosas inspecciones la convierten en una referencia, han sido pioneros en la regulación de varios procesos en la industria farmacéutica. La relación comercial más viva es con Estados Unidos ya que existen presencia de varias farmacéuticas de origen estadounidense en México.

Esta agencia pertenece al Departamento de Salud y Servicios humanos de Estados Unidos, se encarga de la protección de la salud pública mediante la regulación y supervisión de las medicinas, productos biológicos, equipos médicos, vacunas,

suplementos alimenticios y productos veterinarios, entre otros, su sede se encuentra en Maryland y cuenta con 223 oficinas y 13 laboratorios ⁽¹²⁾.

CFR 21 PART 11 (Code of Federal Regulations Parte 11)

La publicación No. 54, Vol. 62, Reglas y Regulaciones de la FDA, publicada el 20 de Marzo de 1997, documento que dicho organismo mapeo de 1991 a 1994 a los registros electrónicos y firmas electrónicas generados en las diferentes industrias, farmacéuticas, veterinarias, alimentos, dispositivos médicos entre otros, su impacto en la mejora de usar menos papel para los registros, buscando en como soportar que una firma electrónica y registros electrónicos son igual de auténticos a los registros y firmas manuscritas, se recibió propuestas y comentarios de las industrias involucradas para normarse los nuevos criterios y requerimientos y es así como el Código de Regulaciones Federales en su capítulo 21, correspondiente a (Food and Drugs) alimentos y fármacos, capítulo 1, subcapítulo A, parte 11.

En agosto de 2003 se publicó la (Guidance for Industry Part 11, electrónico Records; Electronic signatures Scope and Application) Guía para la industria Parte 11, Registros electrónicos; Firmas electrónicas Alcance y aplicación, la cual se enfocó en tres elementos principales:

Acotar los registros a considerar como registros y firmas electrónicas.

Enfocarse en los criterios y requerimientos para la validación, tratamiento de los registros de auditoría, respaldo y restauración de los registros.

Normar los requisitos para cumplimiento de validación y el tratamiento de los registros de auditoría.

EMA (Por sus siglas en ingles European Medicines Agency)

Organismo descentralizado de la Unión Europea, fundado en 1995, que tiene su sede en Londres. La agencia es responsable de las evaluaciones científicas de los

tratamientos médicos desarrollados por las compañías farmacéuticas para uso en la Unión Europea, [130820_DS_Farmaceutica_ESP.pdf \(www.gob.mx\)](#)

Entidad reguladora de 28 países que forman parte de la unión europea, así como Islandia, Noruega, Lichtenstein, la cual impacta alrededor de 500 millones de personas. Sus estándares son reconocidos internacionalmente lo que permite que los laboratorios europeos sean uno de los mayores exportadores de medicamentos en el mundo.

INVIMA (Instituto Nacional de Vigilancia de Medicamentos y Alimentos)

Agencia reguladora de Colombia y países latinoamericanos, sus auditorías suelen ser igual de minuciosas que las de FDA y EMA, auditores preparados que llevan un puntual seguimiento de auditorías previas y seguimiento de estas.

Conocer a las agencias reguladoras es muy importante en la industria Farmacéutica, ya que los criterios de cumplimiento de las áreas, procesos y productos son indicados por estas agencias, para el caso de los sistemas computarizados, debemos de revisar en ellas como clasifican a los sistemas computarizados y que esperan de ellos, es decir si solicitan que se validen.

Validación.

Las áreas de validación en las empresas farmacéuticas son las encargadas de retar a los procesos de manufactura, métodos analíticos, actividades que son sensibles de auditorías de entidades regulatorias, con el fin de estandarizar los procesos, y se documente en sus procedimientos, recetas, y o métodos, el cómo realizar la actividad, para evitar desviaciones que se traducen en retrabajos, quejas, reclamos, perdidas monetarias e impacto mediático de la marca de la empresa. A continuación, se presenta como definen a la validación las diferentes entidades regulatorias.

Evidencia documental generada a través de la recopilación y evaluación científica de los datos obtenidos en pruebas cualificadoras y específicas a lo largo de todo el

ciclo de vida de un producto, cuyo objetivo es demostrar la funcionalidad, consistencia y robustez de un determinado proceso en su capacidad de ofrecer un producto de calidad, (NOM 059 SSA 2015)

La validación es la confirmación, mediante pruebas objetivas, de que se cumplen los requisitos previamente establecidos para el uso de un proceso o sistema, (FDA)

Acción de comprobar, en concordancia con los principios de las BPM (Buenas Prácticas de Manufactura), que cualquier procedimiento, proceso, equipo, material, actividad o sistema, realmente conduce a los resultados esperados, (INVIMA, Instituto Nacional de Vigilancia de Medicamentos y Alimentos)

Las definiciones de validación de las agencias coinciden en la necesidad de probar los parámetros de los procesos involucrados en las GxP, por sus siglas en inglés, Buenas prácticas de (laboratorio, manufactura, documentación, distribución, obtener y documentar los resultados esperados. Y ese algo puede ser procesos equipos o actividades.

Sistemas Computarizados

Un sistema computarizado está conformado por hardware, software, procedimientos, personas, bases de datos y documentación en interacción con su entorno ⁽¹¹⁾.

La NOM 059 SSA 2015 lo define como, “cualquier equipo, proceso u operación que tenga acoplada una o más computadoras y un software asociado o un grupo de componentes de hardware diseñado y ensamblado para realizar un grupo específico de funciones”

Los softwares de los sistemas computarizados pueden ser simples, estos cuentan con un programa básico llamado firmware, que sirve para operar el instrumento con operaciones muy básicas, mismo que ejecuta actividades con solo oprimir un botón ya que ambos conviven en un mismo equipo, salvan la información y reportan en su

memoria interna o emite un reporte físico en forma de ticket por medio de una impresora acoplada al sistema. Pueden ser usados en laboratorios o en el área de producción como ejemplo podemos tener al contador de partículas en el aire Figura 1. Aun siendo básicos los firmwares estos pueden configurarse, para realizar dicha tarea se debe de apoyar del manual y las diferentes regulaciones para definir roles, privilegios y configuración del sistema. Este tipo de sistemas suelen ser muy simples en los criterios regulatorios a cumplir pues no llegan a contar con Audit Trail y su capacidad de almacenamiento llega a estar limitada, se mencionó anteriormente que pueden llegar a tener memoria interna, es decir que algunos no llegan a tenerla y esto significa que la información no puede ser consultada en el sistema en eventos futuros, lo cual es un riesgo en caso de que los datos impresos lleguen a dañarse perderse o extraviarse. Las necesidades del sitio y por medio de los controles a implementar se decidirá si sistemas con esas características pueden ser usados en el sitio.



Figura 1. Contador de Partículas en el aire Met One

Existen también sistemas computarizados más complejos, (Figura 2). Los cuales trabajan con un software instalado a una estación de trabajo o PC, para administrar el sistema y operar el equipo o instrumento al cual será conectado. Esto significa que existe más interacción entre el sistema computarizado y el usuario permitiendo una administración más robusta y una programación de las tareas más efectivas y eficaces, dependiendo su configuración. La configuración de este tipo de sistemas da alcance desde el tiempo que el sistema permanece en inactividad por no uso, bloqueo por número de intentos fallidos de inicio de sesión, información que se

registrara en el Audit Trail, y más criterios que dependen del sistema computarizado su diseño, cabe mencionar que incluso se puede configurar el tipo de reporte que se desea generé el sistema, en cuanto haya concluido la actividad para la cual fue diseñado y configurado.



Figura 2. Electroforesis Capilar Karat32 EC_poster.jpg (1600×900) (inolab.com)

En el mercado existen diferentes sistemas para realizar la misma tarea, queda a la industria farmacéutica elegir cual adquirir, considerando aquel que se ajuste más a sus necesidades y presupuesto.

También puede ser un sistema computarizado una hoja de cálculo usada para la obtención y tratamiento de datos crudos, calibración verificación y calificación de instrumentos, emisión de reportes de condiciones ambientales, entre otras. Las hojas de cálculo son usadas en manufactura y laboratorio. Es importante mencionar a las hojas de cálculo e identificarlas como un sistema computarizado, siempre y cuando los datos con los que trabajen sean datos relacionados a la liberación de un lote, manejo de estabilidades y demás criterios regulatorios o información sensible de auditarse, estas también deben de tener su procedimiento de uso, pues siempre debe de ser estandarizada su operación para la obtención de registros. Así como la documentación técnica que indique su configuración, gestión de usuarios y privilegios de accesos, configuración de celdas y columnas, fórmulas que tendrá, distinguir las celdas habilitadas para ingresar información de las celdas protegidas que impidan la modificación de la información que puedan sesgar los resultados obtenidos. Recordemos que la implementación de un sistema computarizado es para hacer más robusto y confiable un proceso, sustituir los registros originados por

papel y lápiz que hayan sido o puedan ser modificados por el autor o por algún otro obligando el dato a cumplir especificaciones, criterios de aceptación o dictámenes. En la Norma 059 SSA 2015 en el numeral 9.9.2.3 se menciona el criterio, Verificación continua de proceso, el cual puede ser verificado y controlado por Hojas de cálculo que también deben ser validadas.

Componentes de un sistema computarizado.

Los componentes de un sistema computarizado son físicos (hardware) y digitales (software). Los físicos son el instrumento que ejecutara la actividad por la que fue adquirido, es decir, son los equipos o instrumentos de laboratorio o manufactura, tituladores, espectrómetros, espectrofotómetros, contadores de partículas, determinadores de carbono orgánico total, por mencionar algunos.

Los digitales son aquellos con los que el usuario tendrá interacción para configurar y operar el equipo o instrumento, obtendrá datos e información para sus intereses. El software es la aplicación que ejecuta las tareas, el cual debe contar con su manual de uso realizado por el proveedor del sistema computarizado este debe de ser compartido al líder del proyecto para que él lo comparta con el dueño del sistema y dueño del proceso quienes lo tomaran como base para la configuración del sistema computarizado el cual debe ser conforme a las necesidades del negocio y cumplimiento regulatorio

Los equipos o instrumentos están diseñados para operarse sin la necesidad de un sistema computarizado, es decir de forma manual, sin embargo, es necesario que el instrumento y/o equipo sea operado por medio de la aplicación y que este si puede usarse manualmente en el instrumento, se restrinja su uso normándolo en la documentación técnica del sistema computarizado y el procedimiento de operación.

Sistemas computarizados globales.

Existen sistemas computarizados usados para la administración del inventario en un sitio de manufactura, los laboratorios y los almacenes logísticos.

En un sitio pueden existir sistemas computarizados globales, los cuales son gestionados y administrados por un administrador global que en ocasiones puede ser por el proveedor del sistema computarizado o por un administrador global perteneciente al sitio, esto usualmente ocurre en las industrias transnacionales. Para los sistemas computarizados globales, se recomienda tener a un administrador local en el sitio el cual gestionara al sistema computarizado para eventos que no sean necesarios escalar al administrador global, estos quedaran definidos en la configuración del sistema computarizado y documentados en la documentación técnica del sistema computarizado.

Un ejemplo de sistema computarizado global es SAP, como compañía SAP, es uno de los principales productores mundiales de software para gestión de procesos de negocio, y desarrolla soluciones que facilitan el procesamiento eficaz de datos y el flujo de información entre las organizaciones ⁽¹⁶⁾.

Para realizar la validación de un sistema computarizado como SAP se recomienda crear un grupo de trabajo con integrantes de las diferentes áreas a las cuales impactara la implementación del Sistema computarizado. Posterior a esto, se debe mapear el proceso, este deberá de quedar definido y documentado en un control de cambios donde cada área deberá de documentar los cambios que sufrirán sus procesos definidos, previo a la implementación y como esta los impactara. El proveedor dará un acompañamiento puntual con cada uno de los integrantes de las áreas para diseñar el Sistema computarizado alineado al proceso y necesidades del negocio.

Se recomienda que una vez adquirido el sistema se instale y se realice el proceso de validación del sistema computarizado, ya que al dejar pasar el tiempo este se obsoleta a los nuevos requerimientos de las normatividades, y se requieren tareas adicionales para poder poner el sistema con sus características obsoletas en ambiente operativo.

Definido lo que es un sistema computarizado, tipos y sus componentes, pasaremos a los criterios mínimos necesarios para poner en ambiente productivo un sistema computarizado posterior a su adquisición, instalación, configuración y comprobar que cumple con su funcionamiento, según lo requerido.

Registro electrónico

Cualquier combinación de texto, gráficos, datos, audio, imágenes u otra representación de información en forma digital que es creada, modificada, mantenida, archivada, recuperada o distribuida por un sistema informático. Los sistemas computarizados asociados a los equipos o instrumentos de los laboratorios de la industria farmacéutica, procesan registros electrónicos de productos como reactivos, materia prima, materiales de empaque, graneles, semiterminados o productos terminados, desde información como número de lote, métodos de análisis, fecha de manufactura y fecha de expira, procesamiento de las muestras, datos generados como resultados y reportes emitidos, son todos estos Registros electrónicos de los cuales debe asegurarse su integridad.

Firma electrónica.

Compilación de datos informáticos de cualquier símbolo o serie de símbolos ejecutados, adoptados o autorizados por un individuo para ser el equivalente legalmente vinculante de la firma manuscrita del individuo ⁽¹³⁾. Cada una de los tratamientos que se realice a los registros electrónicos debe de tener una trazabilidad de quien la realizo y esa se da por la Firma electrónica, la cual puede estar constituida por datos biométricos, que corresponden a un único ente por ser características propias de un único individuo, en la industria la Firma electrónica por lo regular se compone de dos elementos un código de identidad y una contraseña compuesta por caracteres alfanúmeros y símbolos, la combinación de estos la hace más segura.

Audit Trail

Registro electrónico seguro, generado por computadora y con marca de tiempo que permite la reconstrucción del curso de los eventos relacionados con la creación, modificación o eliminación de un registro electrónico. El Audit Trail de un sistema computarizado refleja las acciones realizadas tanto administrativas como operativas, responden las siguientes interrogantes.

¿Quién realizó la acción?, responde al dueño del registro electrónico.

¿Cuándo se realizó el registro?, fecha y hora que se ejecutó la acción cuando se generó el registro

¿Qué registro se realizó? Las acciones que se realizan en un sistema son de control de muestras y/o materiales, ejecución de análisis, ingreso y modificación de datos variables de una porción de producto con características casi iguales conocido como lote y dictamen del lote, esto corresponde a la parte operativa, del sistema computarizado, la administrativa corresponde a la gestión de usuarios, equipos o instrumentos.

Normatividad local de los sistemas computarizados

La NOM-059 SSA1 2015, indica que los sistemas computarizados que impactan en la calidad del producto e integridad de datos deben estar validados, lo cual implica asegurar y retar que estos cumplan los criterios para los que fueron diseñados. Se recomienda tener un control, es decir deben estar inventariados, documentados en un listado de sistemas computarizados, el cual debe de estar actualizado en el sistema de documentación del sitio, como control del programa de mantenimiento del estado validado.

El acceso a los sistemas debe contar con protección y control, para ingresar a estos debe ser mediante un usuario y contraseña. Así mismo establecer un bloqueo de usuario por ingresos fallidos.

Los sistemas computarizados una vez instalados deben ser administrados, tener una clara descripción de roles en el sistema, así como una correcta segregación de privilegios de acuerdo con las necesidades del negocio y cumplimiento a la integridad de datos. Lo anterior debe ser documentado y cualquier cambio en la configuración del sistema deberá ser justificada.

Hoy en día, en los laboratorios de algunas o la mayoría de las industrias farmacéuticas no aprovechan al máximo los atributos con los que cuentan sus equipos y sistemas computarizados en el laboratorio, tales como firmas electrónicas de primer y segundo nivel, uso de Audit Trail, la correcta segregación de funciones, así como una descripción de roles. Presentan cierta resistencia al cambio, al cumplimiento, a la integridad de datos, a hacer uso de una herramienta electrónica que tenga una correcta segregación de privilegios, descripción de roles y un registro electrónico que nos indique con fecha, hora y originador de los datos ingresados en el sistema, así como los cambios tanto a nivel operativo como de administradores.

En ocasiones los sistemas no cumplen todos los requerimientos, aquellos que son solicitados en la ERU (Especificación de Requerimientos de Usuario) y definidos en la NOM 059 SSA 2015 y son los siguientes:

- Deben contar con un sistema de protección, integridad y respaldo de la información, los cuales deben determinarse basados en la documentación de evaluación de riesgos del sistema computacional ya que de no cumplir se determinarán acciones de mitigación para el incumplimiento.
- El acceso y legibilidad de los datos debe asegurarse durante todo el tiempo de retención, ya que, en auditorías, los datos son solicitados y el que no se tenga disponibles se documentara como un incumplimiento a integridad de datos.

Criterios para firmas electrónicas:

- Éstas deben ser únicas para cada persona e intransferibles, una firma electrónica tiene la misma validez que un afirma autógrafa.

- Cuando el uso de firmas electrónicas sea adoptado, se debe establecer la fecha a partir de la cual las firmas electrónicas son vigentes y equivalentes a las firmas autógrafas.
- Las firmas electrónicas deben contar con al menos dos elementos distintos tales como un código de identificación y una contraseña.
- Las firmas electrónicas deberán estar enlazadas a sus respectivos registros electrónicos que aseguren que las firmas no han sido alteradas, copiadas o de alguna manera, transferidas a un registro electrónico para ser falsificadas por medios ordinarios.
- En caso de que la firma electrónica sea realizada mediante tokens o dispositivos biométricos, el sistema deberá asegurar que no puede emplearlo otra persona y que se han implementado medidas de control necesarias.
- El acceso a éstos debe ser controlado. El Sistema debe bloquear un usuario después de una cantidad definida de intentos de inicio de sesión fallidos.

Estos requerimientos son similares a los que solicita FDA, para la validación de los sistemas computarizados según el CFR en su capítulo 21 parte 11,

Validación de sistemas computarizados.

Entendemos por Validación de un sistema computarizado como el conjunto de actividades en las cuales se reta al sistema computarizado, su configuración y operación para lo que fue adquirido. Es verificar y documentar por medio de evidencias, lo que se encuentra descrito en la documentación técnica del sistema computarizado la cual documenta la configuración del sistema, así como su funcionalidad, segregación de funciones en el sistema y el cumplimiento regulatorio. En la validación del sistema computarizado aseguramos el cumplimiento de ALCOA plus de los datos que emite y procesa el sistema por medio de las pruebas diseñadas para asegurar la autenticidad del dato por sí mismo y por su fuente.

Las normatividades nacionales o extranjeras no describen el cómo realizar el proceso de validación de un sistema computarizado, incluso la NOM-059 SSA1

2015, solo menciona 3 ocasiones el termino sistema computarizado. Existen empresas que se dedican a realizar la actividad y emiten y publican guías de validación de sistemas computarizados. El documento GAMP 5 (Good Automated Manufacturing Practices) en su versión 2 ofrecen una guía que establece una metodología para asegurar la correcta implementación de sistemas informáticos en empresas del sector regulado como la industria farmacéutica, y que estos, funcionen según las expectativas del cliente. Las buenas prácticas sobre validación de sistemas propuestas por GAMP 5 son un referente o estándar en el sector, aunque no son de obligado cumplimiento mediante normativas o leyes ⁽¹⁷⁾. Para la compilación del documento GAMP 5, participaron expertos de las entidades regulatorias FDA (Estados Unidos), MHRA (Reino Unido) y Bezirksregierung Münster (Alemania), aunque no hay colaboraciones de Cofepris, no podemos concluir que no existe alcance para México ya que los cumplimientos regulatorios dan alcance al lugar donde se comercializara el producto y la NOM 059 SSA 2015 en su numeral 9.13.5.1 indica lo siguiente: “ Todo cambio a un Sistema computacional debe realizarse de acuerdo al sistema de control de cambios, incluyendo configuraciones de Sistema, deben aplicarse de acuerdo a un proceso predefinido y controlado que comprenda la definición del impacto del cambio y las actividades de verificación resultantes, incluyendo pruebas regresivas”.

Existen diferentes figuras en el proceso de validación los cuales desempeñan diferentes roles, algunos no son propios de un área en específica, ya que dependiendo del usuario final del sistema computarizado. las áreas tendrán un rol. Los roles son los siguientes.

Líder del proyecto.

Es aquel que se encargará de gestionar el sistema computarizado con el proveedor y será el canal de comunicación del sitio con el proveedor, atenderá los comentarios del dueño del sistema y dueño del proceso, así como el área responsable de la validación del sistema computarizado, su figura debe de mantenerse desde la necesidad de adquirir el sistema computarizado hasta poner en ambiente operativo

el sistema computarizado. La cronología del proyecto así como las acciones y las fechas compromiso de estas serán monitoreadas por el líder del proyecto, se recomienda que sea una persona capacitada en las diferentes áreas, que involucrarán la validación de un sistema computarizado es decir, debe conocer de las reglamentaciones locales e internacionales de los requerimientos normativos y regulatorios a cumplir de un sistema computarizado así como la administración, segregación y criterios operativos a configurar en el sistema computarizado. Su responsabilidad concluye cuando el sistema computarizado es validado y el dueño del sistema y el dueño del proceso definen los criterios a seguir para mantener el estado validado del sistema computarizado, el líder del proyecto delegará las tareas de administración y operación que haya adquirido al dueño del sistema y dueño del proceso de acuerdo con su rol.

Dueño del sistema.

Rol encargado de la administración del sistema, sus responsabilidades inician en cuanto el proveedor instala el sistema computarizado, la presencia del dueño del sistema estará en todo el ciclo de vida del sistema computarizado, la gestión de los usuarios que soliciten el acceso al sistema será atendida por el Dueño del sistema, las modificaciones que se realicen en la configuración del sistema también serán atendidas por el dueño del sistema siempre y cuando sean previamente controladas por sistemas de calidad mediante un Control de Cambios y/o desviación. Su responsabilidad concluye cuando el sistema sea retirado de uso. La pericia y destreza en el uso del sistema computarizado se obtiene del conocimiento proporcionado por el proveedor y de la documentación técnica que este mismo entrega al sitio.

Dueño del proceso.

Es el usuario que usará en ambiente operativo el sistema computarizado, cualquier situación con el sistema previo a su validación, la atenderá con el líder del proyecto y dueño del sistema, posterior a la validación esta deberá de ser atendida con el dueño del sistema.

El diseño, configuración del sistema y los requerimientos del negocio definirán los roles del dueño del proceso en el sistema computarizado, así como los privilegios a los cuales se les dará acceso a los usuarios, siempre cuidando los requerimientos normativos y la segregación de funciones, un usuario no puede ser dueño del dato generado y revisor de este.

Área de Validación de sistemas computarizados.

Área responsable de ejecutar la validación del sistema, mediante la ejecución de pruebas retará la administración del sistema versus la documentación y configuración que realice el dueño del sistema. Y retará la operación del sistema, con pruebas que simularan un día a día, en el uso del sistema con la documentación proporcionada por el dueño del proceso y la configuración realizada por el dueño del sistema y al proveedor. Es responsable de verificar el resultado de las pruebas y el cumplimiento de las mismas ejecutadas por el proveedor mediante los protocolos IQ:Installation Qualification-Calificación de Instalación y OQ:Operation Qualification-Calificación de Operación . Es responsable de asegurar el mantenimiento del estado validado de los sistemas computarizados, evaluando los posibles eventos no planeados que puedan afectar el estado validado del sistema computarizado.

Fases de la validación de los sistemas computarizados

Planeación

Esta fase surge de la necesidad del área quien requiere el sistema computarizado para ejecutar y gestionar un proceso analítico, de manufactura y/o logístico, el cual generará información GMP o regulatoria.

Para tener un sistema que cumpla los requerimientos normativos, las diferentes áreas con las cuales el sistema computarizado tendrá contacto deberán evaluar el impacto que el sistema tendrá en sus procesos, y exponer los requerimientos a cumplir por el futuro sistema. Se recomienda crear un grupo de trabajo en donde se definirán los roles de las áreas tales como líder del proyecto, dueño del sistema y

dueño del proceso, es conveniente aclarar que un área no debe desempeñar más de un rol, con el fin de evitar que sea juez y parte, para evitar conflicto de interés en la construcción y validación del sistema, así como la gestión de este, acto que es relacionado a la integridad de datos, ya que la actividad de un área debe ser auditada por un área diferente.

Especificar y diseñar

Es en esta fase donde la Especificación de Requerimientos de usuario es gestionada por el líder del proyecto y el dueño del sistema, quienes indicaran por medio del documento “Especificación de Requerimientos de Usuario” al proveedor lo que se espera realice y cumpla el sistema computarizado.

Especificación de Requerimientos de Usuario (ERU)

Surgida la necesidad de un sistema computarizado, las expectativas que el cliente tenga de él, se documentaran en el documento Especificación de requerimientos de usuario. Este consiste en una serie de requerimientos operativos, de seguridad, criterios regulatorios a cumplir, de integridad de datos, las actividades que se espera realice el sistema, los diferentes accesos que tendrán los usuarios y como serán clasificados estos con los accesos asignados, la necesidad de una firma electrónica y el nivel de firma para los registros generados, incluyen restricciones a los registros como eliminación y ocultamiento de datos crudos o resultados, los requisitos que debe de cumplir la gestión de usuarios, el tratamiento de información y respaldo de la misma, incluyendo adicional la recuperación del sistema y su información en caso de desastre. De manera adicional da alcance a la infraestructura y su configuración en la cual se instalará el sistema computarizado, así como los reportes que genere y al respaldo de la información, así como el histórico y tiempo de retención de los registros. La infraestructura del sistema es muy importante ya que la compatibilidad del sistema y esta aseguran un correcto funcionamiento del sistema computarizado, ya que por problemas de compatibilidad en ocasiones el sistema llega a corromperse evitando el ingreso al mismo y/o el acceso y tratamiento de la información que el sistema tiene.

Toda actividad que se realice en el sistema e información que se genere debe de estar reflejada de forma fiel en el Audit Trail del sistema; el cual es el histórico de las actividades e información alimentada y generada en y por el sistema computarizado, atendiendo a las preguntas básicas de ¿Qué se realizó?, ¿Quién la realizó?, ¿Cuándo se realizó?; los valores anteriores y los nuevos posterior, una vez concluida la actividad.

Los sistemas computarizados se operan y administran, algunos cuentan con más de un Audit Trail, un Audit Trail Administrativo y un Audit Trail Operativo. En el Audit Trail administrativo se registran las acciones ejecutadas por los administradores del sistema, tales como gestión de usuarios, acciones como gestión del aplicativo, como alta de instrumentos o consumibles del mismo, respaldo de la información o envío de información del instrumento y el sistema computarizado. En el Audit Trail operativo se registran las acciones realizadas por los operadores del sistema, si el este es del tipo para registrar y realizar disoluciones, en el Audit Trail se reflejará las disoluciones realizadas por el mismo, la información que se alimente al realizar la actividad se reflejará en el Audit Trail. Es decir, si se registran datos como el lote, producto, tipo de corrida, y más información que al realizar la auditoria del sistema computarizado nos permita trazar la información correspondiente de ¿Qué?, ¿Quién? ¿Cuándo?, preguntas que se atienden a una auditoria de trazabilidad de la información.

La Especificación de Requerimientos del Usuario deberá ser proporcionada por el dueño del proceso a el proveedor del sistema computarizado. Los tiempos en los cuales los proveedores deben de dar respuesta al documento, queda a consideración del dueño del proceso, en algunos casos suele ser lo que indica los procedimientos o las instrucciones de trabajo de los sitios en los que se está realizando la adquisición del sistema computarizado. La respuesta del proveedor se documenta y entrega al futuro usuario del sistema computarizado en el documento: “Especificación Funcional”, el cual incluye la respuesta a cada uno de los requerimientos, esta puede ser cumple o no cumple, queda a criterio del futuro usuario del sistema el decidir si adquiere o no el sistema computarizado.

Se debe documentar el plan de validación con los diferentes requerimientos de cada una de las áreas que participara en la validación con las diferentes actividades que realizara con los respectivos entregables.

En esta fase las diferentes áreas determinan las actividades que ejecutaran cada una de ellas, esto tendrá que documentarse en el plan de validación y en un registro de calidad. Entiéndase que como es un cambio planeado se documentara en un Control de Cambios, el cual es una actividad normativa según la NOM 059 y deberá de registrarse en el sistema de gestión de calidad del sitio, asignando actividades con los diferentes responsables y fechas compromiso a ejecutarse. Es importante ser holísticos en el proceso y que la evaluación de los involucrados sea realizada a conciencia con el fin de evitar incumplimientos en el proceso que ejecutara el sistema computarizado.

Es conveniente generar un timeline o línea del tiempo con las fechas compromiso de los entregables con el fin de dar un seguimiento a la validación del sistema computarizado.

Construir y probar

El sistema computarizado es construido por el proveedor de acuerdo con los requerimientos documentados en la especificación de requerimientos de usuario, y se entrega al dueño del proceso el cual gestiona la instalación del sistema en la infraestructura sobre la cual se usará en su ambiente operativo, entiéndase que en este punto el sistema aún no está en ambiente operativo y que puede realizarse modificaciones.

Cuando el sistema no cumpla requerimientos solicitados en la especificación de requerimientos de usuario, debe de realizarse un análisis de riesgo para evaluar a los posibles incumplimientos y decidir si se validará. En caso de que no se acepten las acciones de mitigación de los riesgos, el sistema puede regresarse al dueño del proceso y deberá modificarse, esto implicaría versionarse el sistema y la

documentación que exista hasta el momento, deberá actualizarse para documentar la nueva versión del sistema.

Análisis de riesgos.

Documento normativo el cual dimensionará los posibles incumplimientos, derivados de los hallazgos de no cumplimiento a los requerimientos de usuario del sistema computarizado, documentados en la especificación funcional, como respuesta negativa de los requerimientos del sistema.

Las áreas encargadas de evaluar los posibles incumplimientos son el líder del proyecto, dueño del sistema, dueño del proceso, validación y aseguramiento de calidad. Quienes definirán acciones a realizar para reducir el riesgo de incumplimiento del sistema computarizado, usualmente se entiende que lo que no se cumple en el sistema computarizado se restringe en papel, es decir para los incumplimientos del sistema computarizado se definirán acciones que serán documentadas en la documentación técnica y procedimiento de operación del sistema computarizado.

Después que el sistema fue construido por el proveedor del sistema, el responsable de la infraestructura debe de tenerla lista y disponible para realizar la instalación del sistema computarizado

La instalación del sistema computarizado la realiza el proveedor del sistema, se recomienda que se encuentre presente el líder del proyecto, el dueño del sistema y el dueño del proceso para verificar en una primera revisión que el sistema esta alineado a los requerimientos de la ERU y que los incumplimientos sean los mismos declarados y documentados en el análisis de riesgos.

Después de la instalación del sistema computarizado, se configura por el dueño del sistema, esta actividad se debe de realizar apoyados de la especificación funcional y el análisis de riesgos, ya que ambos indican los requerimientos que cumple el

sistema y aquellos requerimientos que no cumplió. Para aquellos que se identificaron y se documentaron en el análisis de riesgos como posibles riesgos de incumplimientos y se incluyeron acciones, el área de validación debe verificar que existen controles que previenen incumplimientos y que estos son efectivos. La configuración del sistema debe ser tal que el sistema permita a los usuarios dueños del proceso usar el sistema en ambiente operativo y al administrador permita la administración de usuarios.

Las funciones del análisis de riesgos son dos, una es dimensionar el riesgo del sistema por sus incumplimientos a la Especificación de requerimientos de usuario y la segunda es determinar el periodo de revisión periódica del sistema posterior a su liberación, mientras más alto el riesgo del sistema más pronto será la revisión de este.

La administración de los accesorios del equipo que está asociado al sistema computarizado debe ser del dueño del proceso, ya que esta actividad es operativa.

Documentación técnica

Es la documentación que refleja la configuración del sistema computarizado, está la realiza el dueño del sistema quien una vez validado el sistema tomará el rol de administrador del sistema, la documentación se compone de 4 documentos los cuales son la especificación de configuración, descripción de roles, matriz de accesos y privilegios y listado de usuarios.

También se puede considerar documentación técnica a los manuales del sistema, sin embargo, su elaboración es responsabilidad del proveedor del sistema o bien cuando se adquiere el sistema computarizado, deben de venir acompañados por los manuales, proporcionados por el proveedor del sistema computarizados y son entregados al dueño del proceso.

La documentación técnica debe estar completa, actualizada y vigente para poder validar un sistema computarizado, adicional, su contenido debe estar impactado con

acciones de mitigación de los posibles hallazgos de incumplimientos documentados en el Análisis de riesgo del sistema computarizado con controles que garanticen la integridad de datos de los sistemas computarizado.

Especificación de configuración.

Documento que describe la configuración del sistema computarizado, las políticas con las que fue configurado, los criterios al seguimiento de los registros, los parámetros críticos con los cuales se pondrá el sistema en ambiente operativo y los cuales no podrán modificarse sin un registro de calidad, ya sea por Control de cambios o desviación. La ruta que seguir para configurar al sistema computarizado y poder visualizarse se documenta en la Especificación de Configuración. Para dar cumplimiento regulatorio debe de restringirse el eliminado de información por el dueño del sistema y el dueño del proceso. En caso de que el sistema no pueda configurarse para evitar la eliminación de la información o que este permita ocultar información, en el análisis de riesgos se documenta la restricción la cual se realizará como una acción; que se documente en la especificación de configuración la nota, que restrinja se elimine y oculte información. Si la información con riesgo de eliminar u ocultar corresponde al proceso operativo la restricción debe de documentarse en el procedimiento de operación.

Descripción de Roles.

Un rol en los sistemas computarizados es una descripción de que los usuarios tendrán en el sistema de acuerdo con las funciones que ejecutara en el sistema y el equipo o instrumentos asociados. El sistema será operado por diferentes usuarios, los cuales desempeñarán una diferente función, tendrán un diferente rol, estos serán de acuerdo con la necesidad del negocio, es necesario describir las acciones que cada uno de los roles desempeñara en el sistema computarizado sin que se empalmen responsabilidades, es decir que cada rol debe de tener una única actividad y que esta debe de ser diferente a la que realice otro rol distinto. Un sistema computarizado puede ponerse en ambiente operativo con al menos un usuario por rol del sistema computarizado. Sin embargo, se recomienda que haya

más de un usuario por rol, en caso de que no se encuentre en sitio alguno de los encargados y exista la necesidad de realizar actividades con el rol.

Los roles que se consideraran en este trabajo son:

Analista

Rol asignado a los recursos que realizaran los análisis fisicoquímicos. Los usuarios con el rol también son responsables de asegurar se cumplan las buenas prácticas de laboratorio y de documentación, así como acompañamiento al proveedor en los mantenimientos preventivos o correctivos que se realicen al sistema computarizado.

Desarrollador de Métodos

El rol es considerado siempre que el sistema tenga la funcionalidad de generar métodos analíticos con el fin de hacer estandarizado los análisis fisicoquímicos, que se realicen para la identificación de una molécula en particular, detección de una concentración, identidad o potencia. De manera adicional, el rol se usará en caso de que el equipo asociado al sistema computarizado requiera configuraciones especiales. Entiéndase que la configuración del equipo asociado al sistema computarizado le corresponde al rol desarrollador de métodos, por ser esto una actividad operativa y la configuración del sistema computarizado le corresponde al Administrador del sistema. Es responsable de asegurar el cumplimiento de las buenas prácticas de documentación y laboratorio.

Supervisor

Su función será la revisión y aprobación de métodos y análisis fisicoquímicos, así como la gestión de los consumibles del equipo y del sistema computarizados. En caso de que el sistema computarizado permita la revocación de firmas el usuario con rol supervisor asignado será el responsable de realizar dicha acción.

Administrador

Es el rol responsable de la administración del sistema computarizado, y gestión de los usuarios en el sistema. En caso de que el proveedor de servicio requiera realizar alguna actividad necesaria para mantener el estado validado del sistema con los privilegios del administrador. El administrador del sistema dará el soporte y acompañamiento al proveedor de servicio.

Después de una intervención al sistema computarizado por parte del proveedor de servicio, el dueño del proceso y dueño del sistema, revisaran el sistema computarizado verificando que se haya mantenido el estado validado del sistema computarizado, esta actividad debe realizarse antes de usarlo ya que si la actividad del proveedor impacto el estado validado los análisis que se realizaron también se encontraran comprometidos y tocara evaluar el impacto al análisis por medio de una desviación

En el sistema las cuentas asignadas a los usuarios deben ser personalizadas, no debe haber cuentas genéricas, ni administrativas ni operativas, la cuenta asignada al proveedor de servicio se recomienda que mientras el proveedor no esté realizando actividades en el sistema computarizado, permanezca inactiva.

El procedimiento normalizado de operación documentará el calendario de los mantenimientos preventivos del sistema computarizado considerando responsabilidades para el dueño del sistema y dueño del proceso con el fin de mantener el estado validado del sistema.

El sistema computarizado recibirá un mantenimiento preventivo y/o en caso de ser necesario correctivo, el proveedor de servicio recibirá un rol con los mínimos niveles de acceso, solo los necesarios que le permitan ejecutar su operación; no contará con privilegios de administración ya que se tiene el riesgo de que el proveedor realice una acción con la cual el sistema pierda su estado validado.

Se normará en el procedimiento de operación las intervenciones del proveedor del servicio, en donde se asegure la trazabilidad de las acciones ejecutadas en el sistema, así como las revisiones que se realizarán en el sistema posterior a su intervención por el dueño del proceso y dueño del sistema para asegurar que la intervención no afecte el estado validado del sistema.

Matriz de accesos y privilegios.

Es el documento técnico que describe los privilegios a los cuales tendrán acceso los diferentes roles del sistema computarizado, el proveedor usualmente no entrega segregado el sistema o lo entrega con una matriz genérica, la cual no cumple con el principio mínimo de privilegios, que se deben asignar a cada uno de los roles definidos. Instalado el sistema y concluida la ejecución de la Calificación de Instalación, el dueño del sistema debe de segregarlo, una vez concluida la segregación, el dueño del proceso debe retar la matriz en un ambiente operativo, con cada uno de los roles que el dueño del sistema configuró y segregó, estas pruebas no deben realizarse con producto de liberación ya que hasta este punto el sistema aún no se encuentra validado.

Cuando las pruebas de reto a la matriz de accesos y privilegios por parte del dueño del proceso sean satisfactorias, el dueño del sistema debe asegurar que la configuración realizada al sistema computarizado sea la adecuada, que cumplirá con la integridad de datos y los criterios normativos. Ya que la configuración del sistema ya no podrá modificarse, al menos que se genere un registro de calidad, una desviación. Una vez que la configuración del sistema esté aprobada y vigente debe de mantenerse sin modificaciones.

Los roles configurados, los privilegios asignados a cada rol y la configuración del sistema deben de mantenerse durante todo el ciclo de vida del sistema computarizado; si existen cambios, estos deben de ser planeados y documentados en un registro de calidad y en el control de cambio. Si el cambio no fue planeado y es el resultado de la mala operación o administración del sistema, debe de documentarse en un registro de calidad, como desviación.

El formato de una matriz de accesos y privilegios puede ser de la siguiente forma

Privilegios	Usuario Administrador	Supervisor	Desarrollador de Métodos	Analista
A	X			
B		X		
C			X	
D				X
E	X			

Tabla No 2. Matriz de accesos y privilegios

Listado de Usuarios.

Es la documentación técnica donde se registran a los usuarios que tiene acceso o tuvieron acceso al sistema, el rol y estatus el cual puede ser activo o inactivo. Existen sistemas que solicitan un nombre corto para dar de alta al usuario, si fuese el caso, el nombre debe documentarse en el Listado, para tener una correcta trazabilidad y evitar duplicidad de nombres, la gestión de usuarios en el sistema computarizado es realizada por el administrador del sistema y para poder solicitar el alta en el sistema, el usuario debe estar entrenado en el uso y operación del sistema computarizado y el equipo o instrumento asociado a este. El entrenamiento puede ser por el proveedor del sistema, o por personal entrenado, con ayuda de manuales y del procedimiento de operación del sistema e instrumento.

El Listado de usuarios es una documentación técnica viva, es decir, la necesidad del negocio en el sistema computarizado es gestionar usuarios por medio de solicitudes de alta, cambio o baja de usuarios, es necesario y recomendable normar el proceso para estandarizar las actividades.

Al revisar el estado validado del sistema computarizado debe de existir una correcta trazabilidad de los usuarios en el sistema con el Listado de usuarios, en caso de existir diferencias estas deben de soportarse con las solicitudes de alta, baja y/o

cambio, con el fin de que cualquier usuario en el sistema cuente con su evidencia de estar validada su alta en el sistema.

Los sistemas computarizados cuando son adquiridos usualmente incluyen una cuenta de administración, la cual tiene acceso a todos los privilegios del sistema, es decir, que puede realizar cualquier actividad, tanto administrativa como operativa. Con esta cuenta el proveedor instala el sistema en la infraestructura sobre la cual se operará. Una vez echo eso, se da de alta a un administrador, este comienza con la segregación de funciones en el sistema, generando o editando los roles de acuerdo con las necesidades del negocio y cumpliendo con integridad de datos y la segregación de funciones. La cuenta administración con todos los privilegios debe ser declarada en el listado de usuarios y en la documentación técnica que impacte su existencia, ya que este es un incumplimiento a cuentas personalizadas por lo que debe colocarse un control sobre dicha cuenta, un control de acceso, en la contraseña de dicha cuenta.

El formato de un listado de usuarios puede ir de la siguiente forma:

Listado de Usuarios, del sistema: XXXXX, versión: YYYY, edición: No. Z

Usuarios Activos

Número	Nombre	Nombre corto	Rol
1	Usuario Número 01	USER01	Administrador
2	Usuario Número 02	USER02	Desarrollador de Métodos
3	Usuario Número 03	USER03	Supervisor
4	Usuario Número 04	USER04	Analista.

Usuarios Inactivos

Número	Nombre	Nombre corto	Rol
1	Usuario Número 01	USER01	Administrador
2	Usuario Número 02	USER02	Desarrollador de Métodos
3	Usuario Número 03	USER03	Supervisor
4	Usuario Número 04	USER04	Analista.
5	Proveedor de Servicio	PROVER	Analista

Ejecución

Es el proceso en el cual se verifica la configuración de políticas, administración operación y segregación del sistema versus la documentación técnica y procedimientos de operación, mediante las pruebas diseñadas en los diferentes protocolos. Se recomienda que en la ejecución participen expertos entrenados por los dueños del proceso, dueños del sistema y el proveedor del sistema para realizar un reto holístico. Deben de realizarse las actividades, simulando un día a día de la operación, considerando las acciones operativas de los roles definidos en el sistema con base a los diferentes procedimientos de operación. Es decir, si en el sistema se realizan métodos, el rol desarrollador de métodos creará un método en el sistema, si el sistema está alineado al cumplimiento de CFR 21 parte 11 y ALCOA plus para registros y firmas electrónicas, los métodos a revisar se aprueban previo a usarse.

El método creado y aprobado en el ejemplo anterior, será tomado por el rol del analista y realizará la corrida analítica. En cuanto se concluya el análisis y el sistema genere un reporte de resultados, debe de retarse la modificación de los resultados

y en caso de que el sistema lo permita el Audit Trail del sistema deberá de contener la modificación. Si el sistema permite la modificación de resultados, este debe de estar evaluada en el análisis de riesgos del sistema, donde se indicará el documento que condicione las ocasiones en las cuales se permite hacer la modificación y las acciones a seguir en caso de realizar una modificación.

Una de las pruebas sustanciales y necesarias en la validación del sistema computarizado debe ser la prueba de restauración y respaldo para garantizar que en caso de que el sistema se corrompa y presente una falla, se pueda acceder nuevamente a él. Es decir que exista un espejo del sistema al momento en que se corrompió y que pueda restaurarse en la infraestructura, esta actividad se hace siguiendo los procesos normados de respaldo y restauración de sistemas computarizados.

Cada uno de los diferentes protocolos debe tener prerequisites necesarios para iniciar la ejecución y la descripción de las pruebas a realizarse, criterios de aceptación de estas, apartados para documentar incumplimientos en caso de existir y la conclusión de los resultados.

Todas las pruebas que ejecuta el área de validación se documentan en diferentes protocolos de acuerdo con la etapa de validación que se esté ejecutando, las cuales son los siguientes:

Calificación de infraestructura

Cuando el proveedor da respuesta a la Especificación de Requerimientos de Usuario, indica los criterios que debe de cumplir la infraestructura sobre la cual se instalará el sistema computarizado, el sitio prepara la infraestructura y cuando indica que esta lista se realizan la ejecución de pruebas correspondientes de validez documentadas en el Protocolo de Calificación de Infraestructura, este es ejecutado por el área de validación en conjunto con el área encargada de dar soporte y mantenimiento a los equipos computacionales, en esta etapa se reta el equipo en la cual se instalará la aplicación, los requerimientos de capacidad, procesador,

seguridad, aplicaciones necesarias para su mantenimiento, versión entre otros. Concluido el Protocolo de Calificación de Infraestructura con resultados satisfactorios, se realiza el Reporte de Calificación de Infraestructura y se envía a aprobación de las áreas correspondientes involucradas en la calificación de infraestructura.

Calificación de Instalación.

Una vez que nos aseguramos de que la infraestructura esta lista para instalar el sistema computarizado, realiza la instalación el proveedor del sistema y ejecuta pruebas que nos aseguran que la instalación fue realizada correctamente, que el sistema es compatible con la infraestructura y podrá ser gestionado y operado sin posibles futuros incidentes. Concluido el protocolo con resultado satisfactorio en cada una de sus pruebas, se documenta el resumen de sus pruebas y el resultado de estas, en el Reporte de pruebas de Instalación. Al final Protocolo y Reporte se envían a aprobación.

Protocolo de Pruebas de Aceptación en Sitio.

Es verificar la respuesta a la Especificación de Requerimientos de Usuario, a los requisitos de configuración que se dijo que cumplía y que fueron configurados por el administrador del sistema y también se verifica los controles colocados a los requisitos que se identificaron como posibles incumplimientos con controles documentados en el Análisis de Riesgos del sistema, el proceso de gestión de usuarios y gestión del equipo o instrumento que tenga asociado, gestión y revisión de Audit Trail, perfiles y matrices de accesos de los usuarios en el sistema.

Para el caso de los incumplimientos documentados en el análisis de riesgos, recordemos que se mencionó que el control que no se puede gestionar en el sistema sería en papel y es necesario realizar pruebas donde se rete y se verifique el control. Existen sistemas que pueden administrar más de un equipo, el alcance de la validación de un sistema computarizado debe acotarse para los equipos que se estén considerando validar, documentados en el plan de validación, la

documentación técnica del sistema, así como los procedimientos de operación puede dar alcance a los diferentes equipos con los cuales sea compatible el sistema, sin embargo, como se mencionó anteriormente si el alcance solo es a ciertos equipos, debe ser documentado en el protocolo y en el reporte del mismo.

Protocolo de Aceptación de Usuario

Posterior a la ejecución y aprobación del Protocolo de Aceptación de Sitio, se ejecuta el Protocolo de Aceptación de Usuario, el cual abarca las pruebas en el ambiente operativo del aplicativo, así como el tratamiento de los datos generados, la integridad de los registros generados por el sistema, las firmas electrónicas y trazabilidad de registros electrónicos que el sistema generará en las diferentes actividades que desempeñará en un día de operación considerando los diferentes procesos que ejecutará, con alcance a los reportes que el sistema emitirá para asegurar que los reportes no pueden ser modificados posterior a su generación y aprobación en caso que el sistema cuente con firmas electrónicas de revisión y/o aprobación.

Las pruebas del protocolo deben tener dictamen satisfactorio y contar con su evidencia correspondiente, en caso de hallazgos durante la ejecución del protocolo, se documentan y se evaluará que cambios deben realizarse al sistema computarizado o a la documentación, se podrá avanzar a la siguiente etapa hasta que la prueba se repita con las nuevas consideraciones y los cambios documentados. Para estos casos evaluar si el análisis de riesgos debe actualizarse, ya que la el incumplimiento se pudo generar por un incumplimiento no mapeado o un incumplimiento mal controlado, y todos los posibles incumplimientos detectados en la planeación o durante la implementación del sistema computarizado deben documentarse, dimensionarse y proponer controles en el sistema computarizado para evitar incumplimiento a integridad de datos durante la operación del sistema computarizado posterior a su liberación en ambiente operativo.

Concluidos los protocolos con resultados de sus pruebas satisfactorias, debe emitirse un reporte de liberación, documentando el alcance de la liberación, así

como los resultados de las pruebas. En caso de que una o más pruebas hubiesen resultado como no satisfactorias,

Control

Una vez validados los sistemas computarizados, es responsabilidad del dueño del proceso y dueño del sistema el mantenimiento y validación del sistema computarizado.

Los sistemas computarizados, se administran y controlan en un listado de sistemas computarizados con sus identificadores y un programa de verificación del mantenimiento validado mediante revisiones periódicas. en un tiempo determinado posterior a su validación, Este tiempo se determinará por el nivel de riesgo del sistema que se documente en el análisis de riesgo del sistema.

La revisión de Audit Trail, accesos y privilegios es una actividad que permite verificar que la configuración del sistema se ha mantenido de acuerdo con la validación del sistema. Los privilegios asignados a los roles de los usuarios deben corresponder con la documentación técnica: Matriz de accesos y privilegios, Descripción de roles y Listado de Usuarios.

En cuanto el sistema sea puesto en ambiente operativo se debe de revisar el análisis de riesgos del sistema, en el cual se declara el impacto de la evaluación de los posibles incumplimientos para el cual se documentó. Considerando que se dejaron acciones que se retaron se implementaran en los diferentes protocolos.

El nivel de riesgos del sistema determinará los tiempos para los cuales el sistema computarizado debe de ser verificado su mantenimiento del estado validado, por revisiones de Audit Trail y revisiones periódicas.

Las revisiones de Audit Trail son la verificación documental y en la configuración y actividades realizadas en el sistema en un periodo de tiempo para asegurar que el sistema no ha sufrido modificaciones injustificadas sin registros de calidad como

desviaciones, controles de cambios o análisis de riesgos. Estas revisiones deben realizarse transcurrido un determinado tiempo, como una vez al año. Para sistemas que no cuenten con Audit Trail, es necesario que se genere una bitácora de Audit Trail, en la cual se documente las acciones que se realizan en el sistema, esta debe ser diferente de la bitácora de uso del sistema o instrumento el cual administra y gestiona el sistema computarizado.

Las revisiones de Audit Trail nos ayudan a garantizar la integridad de datos del sistema, y el mantenimiento al estado validado, ya que es una auditoria en la cual se verifica la configuración del sistema, los roles y privilegios de los usuarios que se encuentran dados de alta en el sistema, así como verificar que las acciones realizadas en el sistema cumplan con los criterios de ALCOA plus, criterios para los cuales la administración y la operación el sistema son confiables.

Para las actividades operativas en el sistema computarizado es necesario que exista una bitácora, de uso y documentar las actividades que se realizan en el sistema computarizado, esta puede ser elaborada en papel o bien, electrónica.

La documentación técnica que se verifica en la revisión de Audit Trail debe estar aprobada y vigente, debe de ser una imagen del sistema computarizado, la descripción de roles, la matriz de accesos y privilegios, así como la especificación de la configuración en caso de actualizarse debe de justificarse con un registro de calidad. No aplica el mismo caso para el listado de usuarios, el cual debe de coincidir con el sistema y en caso de que no coincida el estatus del usuario en el sistema, debe de estar justificado con la documentación que avale su estatus en el sistema de acuerdo con las buenas prácticas de documentación.

En caso de detectarse hallazgos en el sistema estos deben de evaluarse en conjunto con el dueño del sistema, dueño del proceso, el área de validación de sistemas computarizados, así como aseguramiento de calidad para decidir qué acciones realizar, es decir, si este pierde su estado validado o pueden realizarse las

acciones correctivas en el sistema o documentación y esto debe de quedar documentado en la investigación correspondiente.

En caso de ser necesario estas mismas figuras deben de evaluar si se actualiza el Análisis de Riesgos en el cual se documente el posible nuevo incumplimiento y de manera adicional se deben de evaluar las acciones a seguir en caso de que el sistema pierda su estado validado, tales como revalidación del sistema computarizado.

Una actividad de control del sistema computarizado es realizar el respaldo de la información configurada y generada en el sistema ya que en caso de falla se tiene un punto del cual partir y restaurar los registros electrónicos.

En ambiente operativo del sistema genera datos, los cuales por regla están asociados a los análisis que realiza el equipo asociado al sistema computarizado, y estos dejan una traza del dato. Cada vez que se libere un lote o lotes se debe realizar una revisión de Audit Trail del sistema para garantizar el cumplimiento de integridad de datos.

Retiro

La fase de retiro de un sistema computarizado consiste en sacarlo de ambiente operativo de forma controlada, es decir, con un registro de calidad, control de cambios. El cual se realiza de una forma planeada, evaluando y documentando los riesgos que implica el retiro de uso del sistema. Un control de cambios por retiro de uso de un sistema computarizado, el cual incluya la planeación a seguir para el retiro. Este control de cambios debe ser evaluado por todas las áreas que se impacten por retirar el sistema, se deben definir acciones a los procesos que se afecten de una forma controlada, con responsables y fechas compromiso a cumplir.

La documentación técnica de un sistema en retiro debe ser actualizada, documentando y evidenciando el estado actual del sistema en retiro. Todas las cuentas personalizadas activas en el sistema deben inactivarse y solo debe haber

una cuenta de acceso al sistema para consulta de la información generada mientras el sistema estuvo en el ambiente operativo.

La información generada en el sistema computarizado durante su ciclo de vida debe estar disponible por un periodo de tiempo el cual debe de estar alineado a los requerimientos de las regulaciones locales e internacionales las cuales norman la distribución de los fármacos en caso de ser otros países.

Descritas las fases del ciclo de vida de un sistema computarizado pasaremos a la integridad de los datos que se genera durante el ciclo de vida de un sistema computarizado y como se asegura el mantenimiento al estado validado del mismo.

Cumplimiento de Integridad de Datos

Existe una filosofía evolucionada del concepto Integridad de Datos, pues es una propiedad que asegura que los datos son únicos y verdaderos en el proceso farmacéutico. Como se ha mencionado anteriormente en todo el proceso que involucra la manufactura de un fármaco se generan datos, y esto son relevantes en diferente medida, dependiendo de la naturaleza del dato, y el lugar donde se generaron. Nos vamos a enfocar en los datos que tienen impacto Buenas Prácticas de Manufactura y en particular en los generados en los laboratorios de análisis fisicoquímico por los sistemas computarizados. Al inicio del párrafo se habló de una filosofía evolucionada, y es que Para la implementación de los primeros sistemas computarizados solo importaba el dato crudo que generara el sistema computarizado, es decir, solo se consideraba relevante el resultado obtenido por el uso de un sistema computarizado, pues se ingresaba a los sistemas con cuentas genéricas, no personalizadas, y no se vigilaba las veces que podían realizarse los análisis hasta obtener el mejor dato. con privilegios administrativos ya que no estaba acotada en accesos y podía configurar las ejecuciones al gusto con el fin de reportar valores dentro de especificación para requisiciones del cliente.

Las cuentas genéricas como su nombre lo indica no son cuentas personalizadas y los datos que generan no son datos atribuibles, es decir el dato no puede atribuirse

al autor de este. Las cuentas genéricas no estaban segregadas, ni acotaban el acceso y esta tenía privilegios administrativos y operativos, es decir se podía modificar al gusto del operador el sistema computarizado.

Cualquier usuario que tenga acceso a la cuenta puede ingresar al sistema y ejecutar un análisis y reportarlo si este no se firma con una firma autógrafa no puede atribuirse al autor. Mencionamos que en caso de existir una firma autógrafa podría ubicarse al autor del dato, pero eso no es del todo cierto ya que si el dato se generó con una cuenta genérica cuando se rastree en el sistema, se identificara como autor del dato a la cuenta genérica que comentamos anteriormente, no es una cuenta personalizada.

Es importante mencionar que las cuentas genéricas se documentan en los listados de usuarios y de ser posible, para su control se inactivan o se mantienen en ese estatus en el tiempo de vida del sistema computarizado.

Al tener un control de las cuentas genéricas los datos cumplen su criterio atribuible, ya que cualquier dato generado corresponderá a una cuenta personalizada asignada a un usuario. La legibilidad de los datos corre riesgo de incumplimiento cuando se registran de manera autógrafa en papel tomado el dato del sistema, ya que por la transcripción del dato del sistema a el papel puede errarse en el registro, los datos generados por el sistema deben de estar documentados en un reporte de tipo no modificable el cual sea idéntico a lo visualizado en el sistema, para cumplir con los criterios de CFR 21 parte 11.

El sistema de integridad tiene varias funciones, una de ellas es establecer una búsqueda de datos respondientes a malas prácticas detectadas mediante auditorías, por distintas entidades sanitarias a la industria farmacéutica.

Las dos actividades que verifican el estado validado del sistema computarizado son la revisión Anual de Audit Trail del sistema computarizado y la Revisión periódica del sistema computarizado analizaremos cada una por separado.

Revisión Anual de Audit Trail del sistema computarizado.

Es la revisión sistemática de las actividades realizadas en el sistema computarizado en el transcurso de al menos un año de su liberación, en la cual se revisan que las actividades realizadas por el dueño del sistema, el dueño del proceso y el proveedor de servicios se encuentre dentro sus funciones descritas en el procedimiento de uso, y documentación técnica.

La actividad se documentará en un protocolo de revisión Anual de Audit Trail en el cual se registrarán los puntos a revisar, el dictamen de los puntos a revisar y los hallazgos que se detecten. De acuerdo con la clasificación del hallazgo y el impacto al estado validado del sistema se generarán registros de calidad, desviaciones para hacer la investigación, que nos permita identificar el origen del incumplimiento y generar las acciones correspondientes para corregir el error y evitar su recurrencia. Cualquier modificación que se haya realizado en el sistema computarizado debe estar soportado por controles de cambios o bien cuando el dueño del proceso o dueño del sistema detecten una modificación deben de dar aviso al área de validación para poder evaluar el impacto al estado validado y determinar si el sistema es sacado de uso hasta regresarlo a su estado validado.

La revisión se realiza a los registros de Audit Trail que se generaron se registraron posterior a la fecha de liberación del sistema computarizado, lo cual corre a partir del reporte de liberación de validación del sistema computarizado.

Los registros de Audit Trail deben cumplir con ALCOA, es decir los datos deben ser atribuibles de poder identificarse al dueño del dato. Legibles, que el dato se entienda y hable por sí mismo. Contemporáneo, es decir, que los datos se registraron en cuanto se generaron. Original, que el dato es verdadero, tal cual como se originó. Y preciso, que el dato contiene todos sus elementos.

Los sistemas computarizados al adquirirse e instalarse estos tienen una cuenta full, es decir es una cuenta que tiene todos los privilegios, y esta puede realizar

actividades administrativas como operativas y esta cuenta es con la que se administra el sistema y el equipo asociado a este durante la instalación. Esta cuenta no puede eliminarse y no se recomienda se realice, ya que es conveniente que exista una cuenta full en caso de que se presente una contingencia en el sistema computarizado y tenga que restaurarse la aplicación y se requiera instalar la aplicación desde el inicio. Las actividades permitidas de la cuenta full se documentarán en la documentación técnica y al hacer la revisión del Audit Trail se revisará que en caso de haberse utilizado la cuenta full, haya sido solo para actividades permitidas. En caso de que se hubiese utilizado para actividades no descritas en la documentación técnica se tendrá que documentar como hallazgo y dependiendo del impacto a la validación del sistema computarizado este se clasificara y se generara los registros de calidad correspondientes.

Las acciones deben ser en cuentas personalizadas, asignadas a usuarios con acceso autorizado, en caso de que existan cuentas genéricas en el sistema el acceso debe estar restringido, es decir deben estar con estatus inactivo y debe estar declarada en el listado de usuarios. Por lo general existen las cuentas genéricas en el sistema ya que cuando el proveedor instala el sistema computarizado y ejecuta el protocolo de calificación del sistema computarizado, una de las pruebas del sistema es que permita la creación de cuentas, motivo por el cual el proveedor del sistema crea cuentas genéricas, para poder ejecutar la prueba y dictaminarla como satisfactoria. Pero al realizar el Audit Trail del sistema no debe de haber acciones de cuentas genéricas, y en caso contrario se documentará como hallazgo y dependiendo del impacto a la validación del sistema computarizado este se clasificará y se generará los registros de calidad correspondientes.

Las acciones que se identifiquen en el Audit Trail del sistema computarizado de los administradores, del sistema deben estar relacionadas a sus acciones rutinarias de un administrador, es decir deben ser de gestión de usuarios, modificaciones permitidas y justificadas de fecha y hora, ingreso al sistema para realizar ajustes de fecha y hora en caso de requerirse, previa autorización del dueño del proceso ya que si se detecta que el sistema no tiene configurado la fecha y hora

contemporáneas, el dueño del proceso debe asegurar que el sistema no genere datos con fecha y hora contemporáneas, en caso contrario se tendrá que documentar como hallazgo el cual tiene impacto al reporte emitido con fecha y hora incorrecta. El estado validado del sistema no se ve afectado.

Los datos emitidos por el sistema computarizado deben ser contemporáneos, por esta razón del registro de la fecha y hora del sistema debe ser contemporánea, En caso de que de no ser así debe ajustarse la fecha y hora por el administrador del sistema y esta actividad debe registrarse en las bitácoras de Audit Trail y uso del equipo. Si se generaron datos con fecha y hora no contemporánea debe documentarse el hallazgo e investigar por que los controles de verificación del dato fallaron y robustecerlos.

Anteriormente se documentó que lo que no se le dé alcance por el sistema se matara en papel, es decir, que aquellos incumplimientos del sistema por su diseño o naturaleza documentados en la Especificación Funcional se colocaran controles en la documentación técnica o en el procedimiento de operación.

Para aquellos sistemas que no cuenten con Audit Trail, se normara en el procedimiento de operación y en la documentación técnica que las actividades del uso de equipo por los administradores se registraran en la bitácora de Audit Trail la cual debe de tener los siguientes campos o formato.

Fecha de la actividad	Autor de la actividad	Actividad	Razón de cambio	Valor anterior	Valor nuevo	Revisor de la actividad

Tabla No 3. Formato de Bitácora de Audit Trail.

Si bien no habrá un registro de como trazar las actividades de los administradores, el sistema evidenciará la gestión de los usuarios y del equipo asociado al sistema computarizado. Entonces cuando se gestione el equipo o accesorios por el dueño del proceso también se registrarán estas acciones en la bitácora de Audit Trail.

Los equipos asociados a los sistemas computarizados cuentan con bitácoras de uso, en esta se registran las actividades ordinarias operativas. En la industria farmacéutica, se analizan y se registran por lotes, por tal en la bitácora se documenta el tipo de análisis que se le realizó al lote, quien lo realizó, y cuando se ejecutó la actividad, todos los lotes analizados en el equipo deben registrarse en las bitácoras de uso.

En caso de omitir registros en las bitácoras de Audit trail y de uso del sistema computarizado se documentará como hallazgo y se debe evaluar el impacto del registro no documentado y en caso de afectar el estado validado debe generarse la desviación correspondiente.

Cualquier hallazgo que se detecte en el Audit Trail del sistema debe evaluarse para identificarlo como una actividad rutinaria o no, y así realizar una búsqueda profunda en la configuración del sistema y compararla con la Especificación de Configuración del sistema.

La configuración del sistema computarizado debe coincidir con la que se verifico la validación del sistema y esta debe de ser la misma en caso contrario el sistema computarizado ha perdido el estado validado, y ahora debe evaluarse el uso del sistema hasta que se revalide de nuevo el sistema. Adicional debe de generarse una desviación para investigar el origen del desvió y generar las acciones correspondientes.

Los roles del sistema computarizado deben de coincidir con el documento Descripción de roles del negocio, declarados y verificados en la validación inicial. Para los sistemas en los cuales no se configuran roles si no que esto se definen con los privilegios que se asignan a un grupo particular de usuarios, los privilegios deben de coincidir de acuerdo con los declarado en la descripción de roles y matriz de accesos y privilegios.

En caso de que los roles no coincidan debe de investigarse generando una desviación y para que no vuelva a ocurrir deben generarse acciones de la desviación correspondiente.

Los privilegios de los roles también deben de coincidir con el documento Matriz de accesos y privilegios y lo documentado en la validación inicial en caso de incumplimiento se debe investigar, ya que el estado validado del sistema se ha impactado. Debe evaluarse el impacto al estado validado y los roles impactados, así como los datos que se generaron con los usuarios del rol impactado en caso de no haberse generado datos, el impacto solo será al estado validado del sistema computarizado.

Los usuarios dados de alta en el sistema deben estar declarados en el listado de usuarios, pero si llega a ocurrir que no se encuentren en el Listado de usuarios, que recordamos es un documento vivo que se actualiza en un periodo de tiempo, se debe contar con su alta o cambio de rol en el sistema computarizado y el rol que tengan el sistema debe coincidir con el declarado en el listado de usuarios, en caso contrario debe de documentarse el hallazgo. Y si el usuario hubiese generado datos en el sistema computarizado debe generarse la desviación correspondiente.

Debe revisarse la evidencia de las revisiones de Audit Trail que se realizan al dictaminar un lote dictaminado por el sistema computarizado y en caso de que no se esté realizando, se debe documentar el hallazgo y generarse el registro de calidad correspondiente y dejar acciones que asegure que no vuelva a repetirse el incumplimiento.

El sistema computarizado debe respaldarse periódicamente por plan o por necesidades del negocio y documentarse en un programa de cumplimiento de respaldos, el dueño del sistema debe presentar las evidencias del respaldo y de los cumplimientos al programa, en caso de no haberse realizado se debe documentar el hallazgo y generar la desviación correspondiente.

Se ha documentado una serie de criterios a revisar y en cada uno se indicó que en caso de que hubiese hallazgos se generara la desviación correspondiente sin

embargo esta debe generarse por los hallazgos detectados en la revisión anual de Audit Trail y no por cada uno de los hallazgos detectados.

Las áreas como integridad de datos, validación del dueño del sistema y el dueño del proceso evaluarán el impacto al estado validado del sistema y determinarán si el sistema computarizado puede seguir en ambiente operativo de ser así se recomienda que se realice un análisis de riesgos. En caso de que el sistema computarizado pierda su estado validado avisar al dueño del proceso y dueño del sistema para tomar decisiones y acciones sobre el sistema computarizado.

El dueño del proceso debe evaluar si versiona el Análisis de Riesgos, es decir si los hallazgos detectados durante la revisión de Audit Trail corresponden con los incumplimientos del sistema documentados en la Especificación Funcional a los cuales se les asignaron acciones de control y mitigación, o son incumplimientos del sistema a los cuales no se les dio alcance por lo que en cualquiera de los casos es necesario versionar el análisis de riesgos.

El área de integridad de datos define como se reporta el cierre de la revisión de Audit Trail, ya que esta puede ser con un reporte de revisión de Audit Trail donde se documente cada una de las pruebas que se realizaron para verificar que el sistema mantiene su estado validado y que no se han ejecutado acciones o una plantilla prellenada a manera de checklist que registre el cumplimiento o no de los puntos verificados. Adicional se documentan los hallazgos con la respectiva desviación que se hubiese generado en caso de aplicar.

Revisión periódica de Audit Trail.

Es la revisión holística del sistema computarizado en la cual se verifica documental y operativamente que el sistema mantiene los criterios con los cuales fue validado y puesto en ambiente operativo. El periodo de tiempo en el que se debe realizar la revisión periódica del sistema computarizado se define por el análisis de riesgos del sistema y su nivel de riesgo, para sistemas con riesgo alto, la revisión debe ser un año posterior a su dictamen

La revisión da alcance a la documentación de sistemas computarizados a los registros de calidad que se generaron en el periodo de revisión, posterior a la liberación de la validación del sistema computarizado. Puede haber cambios planeados, controles de cambio o cambios no planeados, desviación; en los cuales se documente acciones que impacten al sistema computarizado y su documentación técnica. Estos registros con sus acciones y estatus correspondientes deben documentarse en la revisión. En caso de que existan acciones abiertas se evaluarán para determinar el impacto al sistema por los registros y acciones abiertas.

Se considera también la documentación que se genera como prerrequisitos de validación y aquella que se genera durante la validación del sistema computarizado, el estatus de la documentación y si esta se ha versionado se revisara los cambios y los motivos del cambio y si se realizó por medio de un registro de calidad.

Los procedimientos relacionados al sistema computarizado, así como al equipo asociado a este ya que los procedimientos deben dar alcance a la revisión de Audit Trail del sistema, ya sea para la liberación de un lote o para la revisión de Audit Trail por el dueño del sistema y dueño del proceso para buscar acciones no rutinarias. El cumplimiento a los respaldos del sistema es parte de la revisión documental, el dueño del sistema debe tener evidencia del cumplimiento de los respaldos.

La segunda parte de la revisión periódica de un sistema, son las pruebas del sistema en ambiente operativo las cuales son coincidentes con las realizadas en la validación del sistema computarizado, estas pueden ser pruebas de seguridad, pruebas operativas y de desempeño.

Las pruebas deben tener dictamen satisfactorio y deben documentarse las evidencias de las pruebas correspondientes.

El cierre de la actividad se realiza con el protocolo ejecutable completo, el ejecutor del protocolo debe asegurar que se cumplan los principios de ALCOA plus en las pruebas y en los resultados.

En caso de tener resultados no satisfactorios de las pruebas correspondientes, se debe documentar los hallazgos con su respectiva desviación la cual se evaluará entre el dueño del proceso, dueño del sistema, área de validación e integridad de

datos para evaluar el impacto a los datos generados y al estado validado del sistema.

Para la revisión anual de Audit Trail y revisión periódica de Audit Trail se ha mencionado que en caso de hallazgos que implique generar una desviación y que se impacte el estado validado, debe evaluarse si se requiere revalidar el sistema o sacarlo de ambiente operativo.

La desviación debe documentar, ¿Cuándo se detectó el hallazgo?, ¿Dónde se detectó el hallazgo?, ¿Quién detectó el hallazgo?, y el incumplimiento a los procesos estandarizados. En la desviación se documentará cronológicamente las acciones que se realizaron para que se generará el incumplimiento y son importantes pues de ellas se observara la causa raíz del incumplimiento.

Conclusiones.

La industria farmacéutica ha evolucionado en cuanto a los requerimientos normativos ya que por su segmento de negocio se exige que esta sea confiable, y la única forma de cumplir esa confiabilidad es con la Integridad de datos. Motivo por el cual en cada país existe un organismo que regula y dicta las normas jurídicas que la industria debe de cumplir para poder manufacturar y/o comercializar medicamentos. Ha ido evolucionado desde el punto en que existe registros de la manufactura en papel y lápiz, siguiendo una metodología en la cual se establece el cómo ejecutar las actividades, estos son los llamados procedimientos, instrucciones operativas, instrucción de trabajo, esto depende de cada industria. Y la evolución continua, ya que día a día se van integrando nuevos equipos para poder hacer más rápido el trabajo, sin embargo, estos equipos en la mayoría de los casos cuentan con un sistema computarizado el cual puede ser desde un firmware, un equipo sencillo que solo tiene funciones básicas con las que ejecuta una actividad, hasta un equipo computarizado con un software y equipo o instrumento con el cual en conjunto ejecutan una actividad analítica con cumplimiento a ALCOA plus y los criterios de CFR 21 parte 11. En su mayoría son configurados de acuerdo con los requerimientos del negocio, lo que implica que cada usuario que este entrenado en la actividad a desempeñar en el sistema computarizado debe tener una cuenta personalizada, y el sistema debe estar configurado de tal forma que la información que se genere debe de estar alineada a la integridad de datos. Antes de tener un sistema en ambiente operativo estos deben ser retados, es decir; tienen que ser validados, retar su funcionamiento y los cumplimientos regulatorios, con pruebas de configuración y operación, las cuales tienen que ser registradas con sus respectivas evidencias en los diferentes protocolos que una vez concluidos, estos deben pasar a flujo de firmas, el cual se cierra con la autoridad de calidad, que en ocasiones suele ser el responsable sanitario del sitio. Liberado el sistema en ambiente operativo las diferentes áreas deben trabajar en conjunto para asegurar la integridad de los datos ingresados, procesados y generados por los sistemas computarizados.

Los sistemas computarizados emiten registros electrónicos que reflejan la información, desde el ingreso al aplicativo, acciones operativas y administrativas

hasta respaldo y restauración del sistema en caso de desastre, es un gran reto el evidenciar las actividades GMP y no GMP que se realizan en un sistema operativo, ya que existen sistemas que no manejan Audit Trail desde su diseño, situaciones como la anterior deben manejarse un tanto a la antigua con papel y lápiz con el principio de revisión de cuatro ojos a los registros generados y el revisor/aprobador no debe ser el mismo que el ejecutor. Para sistemas que tiene un Audit Trail deben ser configurados para evidenciar mediante registros electrónicos todas y cada las actividades que se realice en el sistema, así como evitar eliminar y ocultar registros, adicional que estos puedan ser consultados por cualquier usuario.

Todo esto es un cumplimiento regulatorio, de más de una entidad, FDA, EMA, OFEPRIS, DIGEMID, INVIMA, ANVISA, etc. Cualquiera que sea la industria farmacéutica en la cual se encuentre un egresado de las ciencias químicas, debe estar manejando información de acuerdo con lo presentado en el trabajo o bien está en proceso de transición o proyecto con la firme intención de migrar al esquema que exigen los organismos regulatorios. No es un proceso fácil de implementar y estandarizar sin embargo la digitalización no es algo que este por llegar si no ya es parte de nuestro tiempo y espacio y si una industria maneja hoy en día registros electrónicos y firmas electrónicas en sus procesos estos ya deben de estar validados o en proceso de validación, por lo que es importante que cada área involucrada si bien no sea experta en la materia, tenga la habilidad de entender la necesidad de la implementación de la mejora, pues al final del día es eso una mejora, ya que una vez que se esté en cumplimiento y estandarizado el nuevo esquema, los hallazgos de los diferentes organismos regulatorios en procesos de auditoria serán los menos pues los procesos se vuelven más confiables y robustos ya que el error humano es menos en sus procesos,

Una vez validados los sistemas, los controles para el mantenimiento del estado validado de los sistemas computarizados deben de asegurar la integridad de los datos durante su periodo de vida operativo del sistema computarizado, y estos controles deben de identificar eventos que pongan en riesgo la integridad de datos del sistema y de la información generada, por lo que la configuración del sistema se

debe de mantener igual a la que se verifico en el proceso de validación, debe de existir un control para la gestión de usuarios, así como solo usuarios entrenados deben de poder ingresar al sistema, los respaldos realizados al sistema y a la información nos deben de proporcionar un punto de partida seguro y confiable en caso de que se corrompa el sistema.

El retiro de uso del sistema debe hacerse de una manera controlada, para que tengamos al final un sistema que ya no se use, que no genere datos, pero que permita ingresar a él para consultar los datos que se generaron durante de periodo de vida.

Toda la información generada en el sistema computarizado debe estar disponible para su consulta y el sistema debe de seguir asegurando la integridad de los datos, aunque ya no se encuentre en uso y este haya sido retirado.

REFERENCIAS BIBLIOGRAFICAS.

1. Prior-González, O.A., Garza-González E., Fuentes de la Fuente H.A., Rodríguez-Leal C., Maldonado-Garza H.J., Bosques-Padilla F.J. 2011. Farmacogenética y su importancia clínica: hacia una terapia personalizada segura y eficiente. *Medicina Universitaria*. 13(50):41-49
2. Gatti C.F. 2018. La talidomina y su tragedia. *Medigraphic*: 46 (3): 233-235.
3. News Google. Número de muertes en el mundo hoy, recuperado el 01 de Julio de 2021. <https://news.google.com/covid19>.
4. Figueras, A. (30 de Noviembre de 2020). La industria farmacéutica: impacto sanitario, social y económico. *OBS Business School*, 1-30. Obtenido de obsbusiness.school
5. Priede Bergamini, T. L.-C. (2009). SECTPR DE LA FABRICACIÓN DE PRODUCTOS FARMACÉUTICOS EN ESPAÑA, REPRESENTACIÓN DE LAS EMPRESAS DE PARTICIPACIÓN EN LA INDUSTRIA. *INVESTIGACIONES EUROPEAS DE DIRECCIÓN Y ECONOMÍA DE LAS EMPRESAS*, 137-147.
6. Godínez R.R. y Aceves P.P, 2014. El surgimiento de la industria farmacéutica en México (1917-1940). *Revista Mexicana de Ciencias Farmacéuticas*. 45 (2): 55-68.
7. Garcia M.P. 2009. La Industria Farmacéutica en México. *Sociedad Química en México*. 3(1): 30-31.
8. Bergamini P., T.; López-Cózar N.C y Hernández, S. B. 2009. Sector de la fabricación de productos farmacéuticos en España. Representación de las empresas de participación en la industria. *Investigaciones Europeas de Dirección y Economía de la Empresa*. 15 (1); 137-147.
9. Ramos-Martínez B., Alonso-Herreros J.M., Rosales-Cabrera A.M.M. 2020. La importancia del control de calidad de las materias primas empleadas en formulación magistral. *Farmacia Hospitalaria*. 44(1): 32 – 33.

10. FDA, U.S Food and Drug Administration, (abril 2016), Data Integrity and Compliance With CGMP Guidance for Industry, Wath is data integrity. <https://www.fda.gov/>
11. (Coro Pando & Blanco, 2000)
12. (Secretaria de Gobernación, 2016, 05 de febrero)
13. Code of Federal Regulations. (1 de April de 2004). Title 21 Food and Drugs. Washington DC., U.S.
14. Department of Health and Human Services Food and Drug Administration. (1 de Diciembre de 2018). Data Integrity and Compliance . U.S, U.S.
15. PHARMATECH. (2015). Integridad de datos "Paperless" agiliza y asegura el cumplimiento con las normas. *Pharmatech*, 52-55. Obtenido de Calidad.
16. SAP. (30 de noviembre de 2024). *SAP*. Obtenido de SAP Latinoamerica: <https://www.sap.com/latinamerica/industries/life-sciences-healthcare.html>
17. ambit. (Noviembre de 2024). *ambit*. Obtenido de ambit: <https://www.ambit-bst.com/blog/qu%C3%A9-es-gamp-5>