



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**  
PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA  
INGENIERÍA QUÍMICA – SISTEMAS DE CALIDAD

VALIDACIÓN DE SISTEMAS COMPUTARIZADOS EN INSUMOS PARA LA  
SALUD

TESIS  
QUE PARA OPTAR POR EL GRADO DE:  
MAESTRO EN INGENIERÍA QUÍMICA

PRESENTA:  
OCTAVIO VEGA GARCIA

TUTOR  
M.C. MARÍA DEL SOCORRO ALPIZAR RAMOS  
PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

Ciudad Universitaria, Cd. Mx.      Febrero 2020



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

**JURADO ASIGNADO:**

Presidente: Dr. Sámano Castillo José Sabino  
Secretario: M. en I. Sosa Zavala Elvia  
Vocal: Dr. Barragán Ocaña Alejandro  
1 er. Suplente: Dr. Del Moral Dávila Manuel  
2 d o. Suplente: M. C. Alpízar Ramos María del Socorro

Lugar o lugares donde se realizó la tesis: Ciudad Universitaria, CD. MX.

**TUTOR DE TESIS:**

M. C. Alpízar Ramos María del Socorro

-----  
**FIRMA**

## Contenido

|  |    |
|--|----|
| Resumen.....   | 6  |
| Abstract.....  | 7  |
| 1. Introducción.....   | 8  |
| 2. Objetivo.....   | 10 |
| 3. Hipótesis.....  | 10 |
| 4. Sistema Computarizado.....  | 11 |
| 4.1 Definición.....  | 11 |
| 4.2 Origen.....  | 11 |
| 4.3 Usos.....  | 12 |
| 5. Validación.....   | 12 |
| 5.1 Antecedentes.....  | 12 |
| 6. Validación de Sistemas Computarizados.....  | 13 |
| 6.1 Marco Normativo.....   | 13 |
| 6.2 Administración de Medicamentos y Alimentos (FDA).....  | 14 |
| 6.2.1 CFR 21 parte 11 Registros Electrónicos; Firmas Electrónicas.....   | 14 |
| 6.3 Agencia Europea de Medicamentos (EMA).....   | 15 |
| 6.3.1 EudraLex-Volumen 4 Directrices de las Buenas Prácticas de v Manufactura (GMP), Anexo 11 Sistemas Computarizados..... | 16 |
| 6.4 Comisión Federal para la Protección contra Registros Sanitarios (COFEPRIS).....  | 17 |
| 6.4.1 NOM-059-SSA1-2015, Buenas prácticas de fabricación de medicamentos.....  | 17 |
| 6.5 Análisis comparativo de los requerimientos regulatorios.....   | 21 |
| 6.5.1 Conclusiones.....  | 29 |
| 7. Metodología de Validación de Sistemas Computarizados.....   | 32 |
| 7.1 Ciclo de Vida de un Sistema Computarizado.....   | 32 |
| 7.2 Validación.....  | 32 |
| 7.2.1 Planear.....   | 32 |
| 7.2.2 Especificar y Diseñar.....   | 33 |
| 7.2.3 Construir y Probar.....  | 33 |

|   |    |
|---|----|
| 7.3 Entregables de Validación.....                                | 33 |
| 7.3.1 Evaluación de Impacto del Sistema .....                     | 35 |
| 7.3.2 Plan Maestro de Validación de Sistemas Computarizados ..... | 36 |
| 7.3.3 Plan de Validación.....                                     | 36 |
| 7.3.4 Evaluación de Riesgo del Sistema .....                      | 36 |
| 7.3.5 Requerimientos de Usuario .....                             | 37 |
| 7.3.5.1 Requerimientos de Usuario Críticos para el negocio .....  | 38 |
| 7.3.6 Evaluación del Proveedor .....                              | 38 |
| 7.3.7 Especificaciones Funcionales .....                          | 39 |
| 7.3.8 Especificaciones de Diseño .....                            | 39 |
| 7.3.9 Evaluación del Riesgo Funcional.....                        | 39 |
| 7.3.10 Matriz de Trazabilidad .....                               | 40 |
| 7.3.11 Línea Base de Configuración .....                          | 40 |
| 7.3.12 Plan de Pruebas .....                                      | 40 |
| 7.3.13 Protocolos.....  | 41 |
| 7.3.14 Calificación de Instalación .....                          | 41 |
| 7.3.15 Pruebas de Aceptación del Sistema .....                    | 42 |
| 7.3.16 Pruebas de Aceptación del Usuario .....                    | 43 |
| 7.3.17 Reporte de Validación .....                                | 44 |
| 7.4 Gestión de Cambios.....                                       | 45 |
| 7.5 Gestión de Riesgos .....                                      | 45 |
| 8. Operar y Mantener .....  | 45 |
| 8.1 Frecuencia .....  | 45 |
| 8.2 Revisión Periódica .....                                      | 46 |
| 8.3 Control de Cambios.....                                       | 47 |
| 8.4 Documentación del Ciclo de Vida del Sistema .....             | 47 |
| 8.5 Desviaciones .....  | 47 |
| 8.6 Elementos de Configuración .....                              | 47 |
| 8.7 Cuentas de usuario .....                                      | 48 |
| 8.8 Registro de Auditoría (Audit Trail).....                      | 48 |
| 8.9 Calificación del personal.....                                | 48 |

|  |    |
|--|----|
| 8.10 Resultados y Plan de Acción .....     | 48 |
| 8.10.1 Resultado 1. ....                   | 49 |
| 8.10.2 Resultado 2. ....                   | 49 |
| 8.10.3 Resultado 3. ....                   | 50 |
| 8.10.4 Reporte de Revisión Periódica.....  | 50 |
| 9. Retiro de un Sistema Computarizado..... | 51 |
| 9.1 Plan de Retiro.....                    | 51 |
| 9.2 Evaluación de Riesgo .....             | 51 |
| 9.3 Solicitud de Cambio.....               | 51 |
| 9.4 Actividades de Retiro .....            | 52 |
| 9.4.1 Desactivación del Sistema .....      | 52 |
| 9.4.2 Migración de Datos .....             | 52 |
| 9.4.3 Desmantelamiento.....                | 52 |
| 9.4.4 Eliminación .....                    | 53 |
| 10. Conclusiones .....                     | 54 |
| 11. Bibliografía .....                     | 55 |

## Resumen

La validación de sistemas computarizados es un proceso utilizado en la industria farmacéutica para comprobar la efectividad y la eficiencia con la que un sistema cumple el propósito para el que fue diseñado. Dependiendo el país o la región geográfica existen diferentes requerimientos regulatorios para este proceso.

En este trabajo se presenta una propuesta de metodología de validación de sistemas computarizados, para la industria farmacéutica establecida en México, alineada a los requerimientos regulatorios de las siguientes instituciones sanitarias: la Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS) de México, a la Administración de Alimentos y Medicamentos (FDA) de Estados Unidos y a la Agencia Europea de Medicamentos.

Se realizó un análisis comparativo de los requerimientos de validación de sistemas computarizados de la normas NOM-059-SSA1-2015 “Buenas prácticas de fabricación de medicamentos”; CFR 21 parte 11 “Registros Electrónicos y Firmas Electrónicas” y EudraLex-Volumen 4 “Directrices de las Buenas Prácticas de Manufactura (GMP)”, Anexo 11 “Sistemas Computarizados” con el propósito de identificar el enfoque, la equivalencia y complejidad de cada requerimiento y tomarlos como base para la metodología de validación propuesta.

La metodología se dividió en cinco fases: Planear; Especificar y Diseñar; Construir y Probar; Operar y Mantener y Retiro del sistema, en cada fase se describen las actividades de validación a desarrollar y los entregables que deben ser generados. Las tres primeras etapas describen las actividades que se deben realizar para la implementación de un sistema y su liberación en entorno productivo. La cuarta fase es una propuesta para mantener el estado validado y asegurar la integridad datos durante todo el ciclo de vida del sistema. Finalmente, la etapa de retiro se enfoca en las actividades que se deben de realizar para mantener disponible la información de acuerdo a las necesidades del negocio y a los requerimientos regulatorios una vez que un sistema se vuelve obsoleto.

**Palabras claves:** validación, sistemas computarizados, industria farmacéutica

## **Abstract**

The computerized system validation is a process used in the pharmaceutical industry to check the efficiency and effectiveness in which a system meets the purpose for which it was designed. According to the country or the geographical region there are different regulatory requirements for this process.

In this work is presented a computerized system validation proposal, for the pharmaceutical industry established in Mexico, aligned to the regulatory requirements of the following health institutions: the Federal Commission for the Protection against Sanitary Risk (COFEPRIS) of Mexico, the Food and Drug Administration (FDA) of United States and the European Medicines Agency (EMA).

A comparative analysis was performed on the computerized system validation requirements of the norms NOM-059-SSA1-2015 “Good Manufacturing practices of Drug Products”, CFR 21 part 11 “Electronic Records; Electronic Signatures” and EudraLex Volume 4 “Good manufacturing practice (GMP) Guidelines”, Annex 11 “Computerized System”, to identify the approach and the equivalence of every requirement and take them as a base for the validation methodology proposal.

The methodology was divided in five phases: Plan; Specify and Design; Built and Test, Operate and Maintain and System retirement, in every phase the validation activities are described for develop and the deliverables that must to be generated. The first three stages describe the activities that must be done for the correct implementation of a system and its release in productive environment. The fourth phase is a proposal to maintain the validation status and ensure integrity of data throughout the entire lifecycle of the system. Lastly, the stage of retirement focuses on the activities that must be completed in order to maintain availability of the information according to the needs of the business and the regulatory requirements once the system becomes obsolete.

**Key words:** validation, computerized systems, pharmaceutical industry



# 1. Introducción

La Industria Farmacéutica es uno de sectores empresariales más rentables e influyentes en el mundo, está dedicada al descubrimiento, desarrollo, fabricación y comercialización de medicamentos para salud humana y animal.

El mercado farmacéutico mexicano se ubica dentro de los 10 más importantes del mundo y es líder latinoamericano junto con Brasil. En México, representa el 4.5 % del Producto Interno Bruto manufacturero, con un valor aproximado de 200 mil millones de peso con un crecimiento anual entre el 3 % y 4 %, <sup>(1)</sup> 14 de las 15 empresas con presencia internacional se encuentran ubicadas en el país, por lo que México se ha posicionado como uno de los centros manufactureros más importantes a nivel internacional. <sup>(2)</sup>

En su conjunto, la industria farmacéutica de México contribuye al desarrollo y la seguridad nacional con la fabricación local de medicamentos. Además de generar más de 74 mil empleos directos y 310 mil indirectos y atraer inversiones <sup>(3)</sup>, la industria farmacéutica establecida en México invierte alrededor de 40 mil millones de pesos anualmente destinando el 1% de ese monto a investigación y desarrollo. <sup>(4)</sup>

La producción de 86% de los medicamentos con los cuales los mexicanos combatimos las enfermedades se lleva a cabo por la industria farmacéutica de nuestro país, mientras que sólo 14% son importados.

De acuerdo con los datos del Instituto Nacional de Estadística y Geografía (INEGI), en 2018 la Industria Farmacéutica mostró una tendencia de crecimiento en cuanto al número de establecimientos dedicados a esta actividad, teniendo un registro actual de 770 unidades económicas, por lo tanto, cada día existe una mayor competitividad entre las empresas farmacéuticas.

Esta industria es una de las más reguladas debido a su impacto en la salud humana, los fabricantes de medicamentos enfrentan el desafío de cumplir la regulación y legislaciones del país donde fabrican y comercializan sus productos, de esta manera una farmacéutica que produzca sus medicamentos en Estados Unidos y los comercialice en México, deberá cumplir con los requerimientos establecidos por FDA y COFEPRIS.

De acuerdo con la OMS, la legislación farmacéutica se orienta principalmente a garantizar que estén disponibles medicamentos eficaces e inocuos de buena calidad, y que se suministre información adecuada de ellas. <sup>(5)</sup>

Debido a la mejora continua por productos médicos de mayor eficiencia y confiables, la industria farmacéutica a nivel mundial ha tenido la necesidad de buscar alternativas tecnológicas para mejorar sus procesos y hacerlos más confiables. <sup>(5)</sup>

Los sistemas computarizados brindan ventajas a la industria farmacéutica para reducir o eliminar errores, aumentar el valor comercial y reducir el riesgo del paciente. Estas capacidades proporcionan beneficios significativos para mejorar la calidad y seguridad del producto. Sin embargo, la integración de éstos ha sido lenta en comparación con la evolución tecnológica. debido a los altos estándar de calidad de las agencias regulatorias quienes han vigilado muy de cerca todo el desarrollo tecnológico que la industria farmacéutica ha experimentado durante las pasadas dos décadas. <sup>(6)</sup>

En el pasado utilizar sistemas computarizados para aspectos relacionados con la calidad del producto era impensable debido a la desconfianza y negativa regulatoria, sin embargo, la FDA y la EMA han hecho avances importantes para regular estos sistemas, publicando de manera independiente, documentos que establecen los requerimientos para que un sistema computarizado se considere validado. La regulación mexicana no ha sido la excepción, desde 2016 la COFEPRIS se ha armonizado con las regulaciones internacionales y ha adoptado similares requerimientos indicados en la NOM-059-SSA1-2015, “Buenas prácticas de fabricación de medicamentos”.

Tanto los requerimientos de la FDA, la EMA y la COFEPRIS poseen el objetivo común de:

- asegurar el correcto diseño del sistema
- asegurar la funcionalidad del sistema
- asegurar la integridad de datos y seguridad de la información
- mantener el estado validado del sistema

Actualmente las agencias regulatorias respaldan, promueven y recomiendan altamente el uso de sistemas para garantizar el cumplimiento de las BPF, el reto para la industria es el entendimiento de los requerimientos para lograr cumplir con las expectativas regulatorias, ya que entre 2013 y 2015, la FDA emitió más de doscientas cartas de advertencia debido a problemas de software y sistemas computarizados, casi un tercio de estos fueron por problemas de validación. <sup>(7)</sup>

Para cumplir con los requerimientos regulatorios es muy importante que las empresas farmacéuticas cuenten con una metodología de validación de sistemas computarizados que contemple aspectos como:

- Requerimientos de usuario
- Análisis de impacto y de riesgos
- Selección de proveedor de software
- Manejo de cambios e incidentes
- Controles de seguridad
- Casos de pruebas para asegurar funcionalidad
- Capacitación de usuarios

Los aspectos anteriores son básicos para la implementación de un nuevo sistema, pero una vez que es liberado en ambiente productivo el reto es demostrar que el sistema mantiene su estado validado hasta su retiro, por lo que es importante que la metodología también contemple:

- Revisiones periódicas
- Manejo de cambios e incidentes durante la operación
- Respaldo y disponibilidad de la información
- Integridad de datos
- Plan de recuperación y desastre

Adicional a lo ya mencionado, la industria farmacéutica debe contar con una metodología para resguardar y asegurar la información electrónica generada por el sistema de acuerdo con los tiempos establecidos por la regulación (cinco años de acuerdo con la NOM-059-SSA1-2015) una vez que un sistema computarizado termine su ciclo de vida o sea vuelva una tecnología obsoleta.

## **2. Objetivo**

Proponer una metodología alineada los requerimientos regulatorios nacionales, estadounidenses y europeos que facilite a la industria farmacéutica establecida en México la validación de sistemas computarizados.

## **3. Hipótesis**

Una metodología que agrupe los requerimientos de COFEPRIS, FDA y EMA y que describa las actividades de validación, facilitará a la industria farmacéutica nacional a entender las expectativas regulatorias relacionada con la validación de sistemas computarizados.

## 4. Sistema Computarizado

### 4.1 Definición

El concepto de sistema computarizado está altamente asociado con la industria farmacéutica, el cual tiene diferentes variantes según la agencia regulatoria, por ejemplo:

#### **COFEPRIS**

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. <sup>(9)</sup>

#### **FDA**

Sistema que incluye hardware, software, dispositivos periféricos, personal y documentación; por ejemplo, manuales y Procedimientos Estándar de Operación. <sup>(20)</sup>

#### **EMA**

Conjunto de componentes de software y hardware los cuales en conjunto cumplen ciertas funcionalidades. <sup>(19)</sup>

De acuerdo con las agencias regulatorias podemos definir a un sistema computarizados como:

***“Conjunto de elementos de hardware, software, personal y documentación que realizan una función o funciones específicas dentro de un proceso”***

### 4.2 Origen

El concepto de sistemas computarizados en la industria farmacéutica surge en la década de los 70's, su uso se contempló desde tempranas publicaciones en las Serie de Informes Técnicos de la Organización Mundial de la Salud relativas a Especificaciones para las Preparaciones Farmacéuticas.

Es en la década de los 80', este concepto se vuelve más conocido, debido a un suceso. Entre 1985 y 1987, los sistemas de dispositivos médicos canadienses, Therac 25, se habían vendido y utilizado en toda América del Norte para ayudar a los pacientes a tratar el cáncer sin embargo la falta de capacitación del usuario combinado con la nula validación dio como resultado que los pacientes recibieran tratamiento de Rayos X, 125 veces más de las dosis prescritas. Seis pacientes fueron expuestos y trágicamente tres pacientes murieron como consecuencia directa. <sup>(8)</sup>

El accidente de los dispositivos médicos y la falta de controles de seguridad, incrementaron el riesgo en los sistemas computarizados durante los años 90's,

época en la que su uso no fue tan solicitado. Es en el año 2000 con el apogeo de la era digital donde el uso de los sistemas computarizados en la industria farmacéutica se intensifica hasta la era actual.

### **4.3 Usos**

Actualmente los sistemas computarizados son utilizados en la producción, comercialización, embalaje, distribución y almacenamiento de medicamentos algunos sistemas populares en la industria farmacéutica son los siguientes:

- SAP ERP – Sistema utilizado para la planificación de recursos
- LIMS – Sistema utilizado en la gestión de información en el laboratorio
- MES – Sistema utilizado en el control y monitoreo de la producción
- Empower y OpenLab– Sistema utilizado en la gestión de datos de cromatografía

## **5. Validación**

La validación es la evidencia documentada generada a través de la recopilación y evaluación de datos obtenidos que aseguran que un proceso, método o sistema específico se desempeña acorde a su propósito de uso y produce consistentemente un resultado que cumple con los criterios de aceptación predeterminados. <sup>(9)</sup>

### **5.1 Antecedentes**

En 1906 se editó en los Estados Unidos (EU) un libro llamado “La Jungla” del autor Upton Sinclair, en el cual se describía cuán malas y “turbias” eran las condiciones del empaque de la carne comercializada en la industria cárnica de Chicago, los norteamericanos redujeron el consumo de carne a la mitad. La respuesta del entonces presidente Teddy Roosevelt fue persuadir al Congreso a la creación de la Food and Drug Administration (FDA). Esta legislación comunicaba un mensaje: prevenir adulteraciones.

Treinta y un años después un farmacéutico en Tennessee cometió el error de usar una sustancia altamente tóxica, el dietilen-glicol, en un nuevo elixir de sulfanilamida. Más de 100 muertes resultaron de esto. El Congreso de EU respondió con la Ley que creaba la Food, Drug and Cosmetic (FD&C). El próximo mensaje era: probar seguridad del producto.

Finalmente, en 1976, la FDA propuso un nuevo sistema regulatorio sobre las Buenas Prácticas de Fabricación (BPF) en la industria farmacéutica. Luego de tres años de audiencias públicas estas nuevas regulaciones se convirtieron en ley. Ya a finales de 1979 se postulaba que un incumplimiento de las BPF podía conllevar a

una demanda por un acto criminal. Las nuevas BPF daban a la FDA mucho más poder regulatorio.

El mensaje clave transmitido por estas nuevas regulaciones fue validar métodos analíticos; procesos de manufactura de medicamentos asépticos, estériles y no estériles; y sistemas de computarizados. <sup>(10)</sup> Por lo que la validación se convirtió en un requerimiento importante para la industria farmacéutica.

## **6. Validación de Sistemas Computarizados**

La validación de sistemas computarizados es parte del Sistema de Gestión de Calidad Farmacéutica. <sup>(11)</sup> Es la evidencia documental que asegura que los sistemas han sido diseñados apropiadamente, construidos y probados para cumplir los requerimientos de usuario, la validación también demuestra su funcionalidad, consistencia y robustez.

El objetivo principal de la validación es asegurar que los sistemas computarizados no impacten en la calidad de los productos, no pongan en riesgo la seguridad del paciente y no alteren la integridad de datos.

### **6.1 Marco Normativo**

La validación de sistemas computarizados es un requerimiento regulatorio para la industria farmacéutica, toda empresa que tenga como propósito la elaboración, distribución y comercialización de medicamentos tendrá que demostrar que los sistemas computarizados utilizados operan y se mantienen en un estado validado.

Para este trabajo se tomaron como referencia la regulación mexicana y la de Estados Unidos y Europa por las siguientes razones:

#### **Estados Unido**

La FDA se caracteriza por ser una de las agencias regulatorias más importantes en el mundo, sus altos estándares de calidad y sus minuciosas inspecciones la convierten en una referencia mundial, han sido pioneros en la regulación de varios procesos en la industria farmacéutica, incluyendo la validación de sistemas computarizados. Adicionalmente la relación comercial más estrecha para la industria farmacéutica nacional es con los Estados Unidos, de este país se importa poco más del 20% de los productos que se comercializan en México y se exporta poco más del 26% de la producción nacional. <sup>(12)</sup> Además existe una fuerte presencia de farmacéuticas estadounidenses en México. <sup>(27)</sup>

## Europa

La EMA regula los 28 países que forman parte de la unión europea, así como Islandia, Noruega y Liechtestein, la cual impacta alrededor de 500 millones de personas, es el equivalente de la FDA en Europa. <sup>(13)</sup> Sus estándares son reconocidos internacionalmente lo que permite que los laboratorios europeos sean uno de los mayores exportadores de medicamentos en el mundo. <sup>(28)</sup> Después de estados unidos la mayor presencia de farmacéuticas extranjeras en México proviene de Europa. <sup>(27)</sup>

### 6.2 Administración de Medicamentos y Alimentos (FDA)

En los estados unidos, la validación de sistemas computarizados ha sido un requerimiento de la Administración de Medicamentos y Alimentos (FDA) para la manufactura de medicamentos desde 1978. En 1983 la FDA publicó una guía para la inspección de los sistemas computarizados en procesos farmacéuticos, también conocido como el "Libro Azul". <sup>(8)</sup>

En 1997 la FDA presentó el Código de Regulaciones Federal CFR 21 Parte 11 para el uso y manejo de registros electrónicos y firmas electrónicas en la industria farmacéutica. La entrada en vigor de la norma de regulación federal 21CFR parte 11 en Estados Unidos desencadenó un proceso de cambio sustancial en la forma en que venía manejándose el tema de los sistemas computarizados en la industria de insumos para la salud sin embargo su importancia llegó a considerarse en toda su magnitud a principios del año 2000. <sup>(12)</sup>

El CFR 21 parte 11 generó confusión y dudas en la industria farmacéutica sobre su alcance real lo que dio como resultado que la FDA generará en 2003 la "Orientación para la industria Parte 11, Registros electrónicos; Firmas electrónicas - Alcance y aplicación", con la intención de aclarar cómo debe implementar y hacer cumplir la parte 11.

El CFR 21 parte 11 se convirtió en una pauta de referencia frente a las demás agencias sanitarias, ejerciendo una notable influencia en la misma EMA, la cual publicó una normativa similar cuatro años después. <sup>(13)</sup>

#### 6.2.1 CFR 21 parte 11 Registros Electrónicos; Firmas Electrónicas

La Parte 11, aplica a los fabricantes de medicamentos, de dispositivos médicos, empresas de biotecnología, desarrolladores de productos biológicos, organizaciones de investigación por contrato (CRO), y otras industrias reguladas por la FDA. <sup>(14)</sup>, define los criterios bajo los cuales los registros electrónicos y firmas electrónicas se consideran dignos de confianza, fiables y equivalentes a los registros en papel.

El CFR 21 Parte 11 está estructurado de la siguiente manera: <sup>(15)</sup>

## **Subparte A – Provisiones Generales**

Alcance  
Implementación  
Definiciones

## **Subparte B – Registros Electrónicos**

Controles para sistemas cerrados  
Controles para sistemas abiertos  
Manifestaciones de firma  
Firma/vinculación de registro

## **Subparte C – Registros Electrónicas**

Requerimientos generales  
Controles y componentes de la firma electrónica  
Controles para la identificación de códigos/contraseñas  
Y se enfocan específicamente en los siguientes requerimientos:

1. Validación
2. Registro de auditoría
3. Sistemas heredados
4. Copia de registros
5. Retención de registros

El CFR 21 parte 11 aplica a todos las empresas farmacéuticas que quieran comercializar sus productos en los estados unidos

## **6.3 Agencia Europea de Medicamentos (EMA)**

En Europa, en 1991 los grupos de la industria farmacéutica se unieron junto con la Comisión de los Comités Europeos para adoptar 2 nuevas directivas. Estas directivas establecerían los principios y directrices para las buenas prácticas de fabricación para producción y distribución de medicamentos en Europa.

En 1991, el Convenio de Inspección Farmacéutica y Esquema de Cooperación de Inspección Farmacéutica (PICs, por sus siglas en inglés) creó un documento que define los requerimientos para los sistemas computarizados, que luego recibirían el nombre de Anexo 5, y que más tarde se renombraría como Anexo 11 para formar parte de las Directrices de la UE GMP. En 1992 se convirtió en parte de los requisitos GLP y GCP para Europa, unificando los requisitos para la gestión de registros electrónicos y firmas electrónicas en compañías farmacéuticas. <sup>(16)</sup>

A medida que los sistemas computarizados aumentaron en complejidad y sofisticación, los requerimientos del Anexo 11 original dejaron de ser adecuados



para satisfacer las necesidades de las organizaciones farmacéuticas europeas. Lo que llevó a una nueva versión del Anexo 11 que entró en vigor en junio de 2011.

### **6.3.1 EudraLex-Volumen 4 Directrices de las Buenas Prácticas de v Manufactura (GMP), Anexo 11 Sistemas Computarizados**

EudraLex es una serie de normas y regulaciones que regulan los productos médicos en la unión europea, en específico para el sector farmacéutico debe cumplir con los volúmenes 1 al 5.

Dentro del Volumen 4 “Buenas Prácticas de Manufactura” encontramos el Anexo 11 el cual describe los requerimientos que deben cumplir los sistemas computarizados utilizados en la fabricación, incluyendo almacenaje, distribución y control de calidad en donde un sistema computarizado reemplace la operación manual.

Esta norma es pionera por establecer que la administración de riesgo debe estar presente durante todo el ciclo de vida de un sistema computarizados también establece que cuando un sistema computarizado reemplace una operación manual, no debería haber disminución de la calidad del producto, control de proceso o garantía de calidad y no debería haber un incremento en el riesgo general del proceso.

La norma se enfoca en los siguientes temas:

1. Administración del Riesgo
2. Personal
3. Proveedores de servicio
4. Validación
5. Datos
6. Comprobaciones de precisión
7. Almacenamiento de Datos
8. Impresiones
9. Registro de Auditorías
10. Administración de configuración y cambios
11. Evaluación periódica
12. Seguridad
13. Administración de incidentes
14. Firmas Electrónicas
15. Liberación de Lotes
16. Continuidad del Negocio
17. Archivo

El Anexo 11 aplica a todos las empresas farmacéuticas que quieran comercializar sus productos en la unión europea.

## **6.4 Comisión Federal para la Protección contra Registros Sanitarios (COFEPRIS)**

En México la validación de sistemas computarizados es un requerimiento que la Comisión Federal para la Protección contra Registros Sanitarios (COFEPRIS) solicita a las empresas dedicadas a la fabricación de medicamentos y dispositivos médicos.

En México, el 31 de Julio de 1998 fue publicada la Norma Oficial Mexicana NOM-059-SSA1-1993, Buenas prácticas de fabricación para establecimientos de la industria químico farmacéutica dedicados a la fabricación de medicamentos, en esté norma la validación era solicitada solo para los procesos de fabricación y métodos analíticos, el concepto de sistemas computarizados no existía.

En 2008 la norma fue modificada y sustituida por la Norma Oficial Mexicana NOM-059-SSA1-2006, Buenas prácticas de fabricación para establecimientos de la industria químico farmacéutica dedicados a la fabricación de medicamentos, en esta versión el concepto de sistema computarizado fue incorporado y por primera vez se menciona que los fabricantes de medicamentos deben validar los sistemas computarizados que impacten en la calidad del producto.

Esta norma se caracterizó por la cantidad de requerimientos que se especificaron para el cumplimiento del uso de Registros y firmas electrónicas.

Con el objetivo de elevar los estándares de calidad en la manufactura de medicamentos, la COFEPRIS, en conjunto con la Secretaría de Salud, la Cámara Nacional de Industria Farmacéutica (Canifarma), y otras autoridades del sector, elaboraron una norma única que integrará los lineamientos de las buenas prácticas de Fabricación, la cual se publicó el de Junio de 2014 como Norma Oficial Mexicana NOM-059-SSA1-2013 Buenas Prácticas de fabricación de medicamentos. Esta actualización no tuvo impacto sustancial en el tema de Validación de Sistemas Computarizados. <sup>(17)</sup>

### **6.4.1 NOM-059-SSA1-2015, Buenas prácticas de fabricación de medicamentos**

En 2015 la COFEPRIS buscaba actualizar y armonizar la norma mexicana con las mejores prácticas internacionales, por lo que inició un proceso de reconocimiento por parte de la Organización Mundial de Salud (OMS) y solicito formar parte del Convenio de Inspección Farmacéutica y Esquema de Cooperación de Inspección Farmacéutica (PIC/S). PIC/S son dos instrumentos internacionales utilizados entre las agencias reguladoras del sector farmacéutico de diversos países para fomentar la cooperación activa y constructiva de los esquemas de buenas prácticas de fabricación en el campo de los productos medicinales. En esta directriz participan activamente las autoridades sanitarias de 46 países entre las que destacan la

Organización Mundial de Salud (OMS), la Agencia Europa de Medicinas (EMA), la Administración de Alimentos y Medicamentos (FDA), la Agencia Suiza para Productos Terapéuticos (Swissmedic), el Ministerio de Salud de Alemania, entre muchos otros. <sup>(18)</sup>

La auditoría realizada por la OMS para otorgar el reconocimiento encontró brechas entre las guías de la OMS y la NOM mexicana, también se detectaron brechas entre las normas mexicanas y las guías PIC/S, lo que llevó a la COFEPRIS a revisar y modificar la NOM-059-SSA1-2013. Como resultado, el 5 de febrero de 2016 entró en vigor la norma NOM-059-SSA1-2015, Buenas prácticas de fabricación de medicamentos. <sup>(17)</sup>

Una de las secciones que más cambios tuvo corresponden al punto 9.13 Validación de Sistemas Computarizados, la cual se armonizó con la Guía para las buenas prácticas de fabricación para productos medicinales PE 009-11 (anexo 11) Sistemas Computarizados, del Esquema de Cooperación de Inspección Farmacéutica.

Para mostrar el resultado de esta modificación se creó el siguiente cuadro comparativo entre los requerimientos de validación de sistemas computarizados de la NOM-059-SSA-2013 y la NOM-059-SSA-2015. (Tabla No. 1)

**Nota:** Los requerimientos sombreados en gris son los que se mantuvieron de la NOM-059-SSA-2013.

| <b>Tabla No. 1 comparativo de requerimientos NOM-059-SSA1-2013 y NOM-059-SSA1-2015</b> |  |  |
|--|--|--|
| <b>Numeral</b>   | <b>NOM-059-SSA1-2013</b>   | <b>NOM-059-SSA1-2015</b>   |
| 9.13   | <b>Validación de Sistemas Computarizados</b>                             | <b>Validación de Sistemas Computarizados</b>   |
| 9.13.1   | Los sistemas que impactan en la calidad del producto deben ser validados | Los sistemas que impactan en la calidad del producto e <b>integridad de datos</b> deben ser validados  |
| 9.13.2   | Protección, integridad y respaldo de la información                      | Inventario de todos los sistemas computarizados  |
| 9.13.3   | Acceso controlado  | Considerar en la validación componentes de software, instrumentos, equipos e infraestructura de tecnología de la información   |
| 9.13.3.1   |  | Protección, integridad y respaldo de la información basada en una <b>evaluación de riesgo</b>  |
| 9.13.3.2   |  | Acceso controlado  |
| 9.13.3.2.1   |  | Controles de seguridad físico y/o lógicos para restringir el acceso a usuarios (modificados periódicamente)  |
| 9.13.3.2.2   |  | Bloqueo de usuarios después de cierta cantidad de intentos   |
| 9.13.3.3   |  | Considerar en la validación registros electrónicos y firmas electrónicas   |
| 9.13.3.3.1   |  | Definición de registros electrónicos   |
| 9.13.3.3.2   |  | Para datos electrónicos regulados debe existir evidencia documental para asegurar trazabilidad, fácil acceso e integridad a los mismos   |
| 9.13.3.4   |  | Los datos críticos capturados manualmente deben ser revisados por una segunda persona o por un medio electrónico validado  |
| 9.13.3.5   |  | Protección de datos por herramientas como copias de seguridad periódicas   |
| 9.13.3.6   |  | La capacidad de restaurar los datos, así como la integridad y la exactitud para su respaldo, deberá ser verificada en la validación y monitoreados periódicamente  |
| 9.13.3.7   |  | Basado en la valoración de riesgos determinar la necesidad de incluir un sistema de auditoría de datos, para registrar fecha y hora de ingreso de usuarios, así como acciones de crear, modificar o eliminar registros                                   |
| 9.13.3.7.1   |  | La auditoría de los datos (Audit trail) deberá prevenir su alteración y deberá estar disponible y convertible en un modo entendible, durante su periodo de retención, para permitir evidencia en la cadena de eventos.                                   |
| 9.13.4   | Considerar en la validación registros electrónicos y firmas electrónicas | El proceso de validación debe abarcar todas las fases relevantes del ciclo de vida de acuerdo con la categoría y arquitectura del sistema, para asegurar la exactitud, integridad y consistencia en el desempeño previsto de los Sistemas Computarizados |
| 9.13.4.1   | Definición de registros electrónicos                                     | La gestión de riesgos debe aplicarse al ciclo de validación completo, incluyendo las fases de planeación, especificaciones, pruebas, liberación del Sistema, mantenimiento y retiro del sistema.   |
| 9.13.4.2   | Para firmas electrónicas:  | Los componentes de la infraestructura de tecnología de la información y cualquier instrumento o equipo relevante deben ser calificados.  |
| 9.13.4.2.1   | Únicas e intransferibles   |  |

|            |  |   |
|------------|--|---|
| 9.13.4.2.2 | Establecer fecha de vigencia y equivalencia      |   |
| 9.13.4.2.3 | Contar con código de identificación y contraseña |   |
| 9.13.4.3   |  | Para la validación, se pueden emplear pruebas ejecutadas por el proveedor, sin embargo, no deben sustituir las pruebas de validación efectuadas en sus instalaciones  |
| 9.13.4.4   |  | Si se emplea un Sistema centralizado en múltiples sitios, el proceso de validación debe incluir la verificación de los procesos ejecutados a través del Sistema en cada sitio individual                              |
| 9.13.4.5   |  | Deben contar con una matriz de trazabilidad donde se documenten las múltiples etapas de especificaciones (incluyendo las revisiones) y las pruebas una vez que se han cumplido de manera satisfactoria.               |
| 9.13.5.1   |  | Todo cambio a un sistema computarizado debe realizarse de acuerdo con el sistema de control de cambios  |
| 9.13.5.2   |  | Deberán implementarse procedimientos de control, que aseguren la revisión de la auditoría de datos de forma regular; la frecuencia y el método serán determinados, de acuerdo con el riesgo.                          |
| 9.13.5.3   |  | Los sistemas con la funcionalidad de auditoría de datos deben emitir información que permita verificar si algún dato ha sido alterado desde su ingreso original.  |
| 9.13.5.4   |  | Si los datos son transferidos a otro formato de datos o sistema, la validación debe incluir la revisión de que los datos no sean alterados en valor y/o definición durante el proceso de migración                    |
| 9.13.6     |  | Para firmas electrónicas:   |
| 9.13.6.1   |  | Únicas e intransferibles  |
| 9.13.6.2   |  | Establecer fecha de vigencia y equivalencia   |
| 9.13.6.3   |  | Contar con código de identificación y contraseña  |
|            |  | 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 |
| 9.13.6.5   |  | 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  |

Fuente: Elaboración propia, 2019

## Análisis

En comparación con la NOM-059-SSA1-2013 la NOM-059-SSA1-2015 agregó requerimientos para:

- Asegurar la protección, recuperación en integridad de la información
- Gestionar las actividades mediante análisis de riesgo
- Demostrar trazabilidad de los cambios realizados en el sistema
- Asegurar el correcto uso de las firmas electrónicas

- Delimitar el alcance los proveedores
- Demostrar la validación de sistemas globales

Estos requerimientos fortalecen el proceso de validación de sistemas computarizados y se asemejan mucho a los requerimientos del Anexo 11.

### **6.5 Análisis comparativo de los requerimientos regulatorios**

Existen similitudes y diferencias en los requerimientos de cada agencia regulatoria, para identificarlas se realizó un cuadro comparativo, ver Tabla No.2 y Tabla No.3, donde se agruparon los requerimientos de la siguiente manera para facilitar el análisis:

- Administración de Riesgos
- Proveedores de Servicio
- Validación
- Firmas Electrónicas/Registros Electrónicos
- Registro de Auditoría/Audit Trail
- Transferencia de Datos
- Almacenamiento de datos
- Controles de seguridad
- Mantenimiento del estado validado
- Administración de incidentes
- Capacitación del personal
- Administración de cambios
- Continuidad del negocio
- Retiro de un sistema computarizado

**Tabla No. 2 comparativo general EudraLex-Volumen 4-Anexo 11, CFR 21 Parte 11 y NOM-059-SSA1-2015**

|                 | <b>EudraLex-Volumen 4-Anexo 11</b>  | <b>CFR 21 parte 11</b>  | <b>NOM-059-SSA1-2015</b>  |
|-----------------|---|---|---|
| <b>Alcance</b>  | Sistemas computarizados utilizados en las actividades reguladas por las Buenas Prácticas de Fabricación.  | Sistemas computarizados utilizados para todas las actividades reguladas por la FDA.   | Sistemas Computarizados que impactan en la calidad del producto e integridad de datos |
| <b>Enfoque</b>  | Administración de actividades basadas en el riesgo del sistema  | Uso de registros electrónicos y firmas electrónicas en sistemas computarizados  | Controles de seguridad y recuperación de la información basadas en análisis de riesgo |
| <b>Objetivo</b> | Demostrar que el uso de sistemas computarizados no impacta en la calidad del producto y asegura la misma calidad que un sistema manual sin que se incremente el riesgo. | Demostrar que los registros electrónicos y firmas electrónicas son confiables y seguros como los registros en papel y la firma manuscrita | Demostrar funcionalidad, consistencia y robustez de los sistemas computarizados       |

**Tabla No. 3 comparativo de requerimientos Anexo 11, Parte 11 y NOM-059-SSA1-2015**

| EudraLex-Volumen 4-Anexo 11 Título  | CFR 21 parte 11  | NOM-059-SSA1-2015   |
|---|--|---|
| <b>Administración de Riesgos</b>  |  |   |
| 1 Aplicar la evaluación de riesgo en todo el ciclo de vida del sistema  | Sin alcance  | 9.13.4.1 Aplicar la gestión del riesgo aplicado en el ciclo de validación completo  |
| <b>Proveedores de Servicio</b>  |  |   |
| <p>3.1 Establecer acuerdos formales para establecer responsabilidades</p> <p>3.2 Realizar auditoría definida por un análisis de riesgo</p> <p>-Revisar la documentación de productos comerciales</p> <p>-La información de auditoría debe estar disponible para los inspectores cuando se requiera</p>  | Sin alcance  | <p>5.3.2.2 Auditoría a proveedores</p> <p>5.3.2.1. Determinar mediante una evaluación de riesgo los proveedores que tenga un impacto en la calidad, seguridad y eficacia del medicamento</p> <p>5.3.2.2 Debe existir un procedimiento para la ejecución de auditoría</p> <p>5.3.2.3 Debe existir un programa de auditorías periódicas</p> <p>5.3.2.4 Los reportes de auditoría deben formar parte del expediente de calificación del proveedor</p> <p>9.13.4.3 Para la validación, se pueden emplear pruebas ejecutadas por el proveedor, sin embargo, no deben sustituir las pruebas de validación efectuadas en sus instalaciones</p>   |
| <b>Validación</b>   |  |   |
| <p>4.1 La validación debe cubrir todos los pasos relevantes del ciclo de vida. Justificar mediante un análisis de riesgo lo estándares protocolos, criterios de aceptación procedimiento y registros</p> <p>4.2 Debe incluir registros de control de cambios y reportes de desviación identificados durante el proceso de validación</p> <p>4.3 Inventario de todos los sistemas computarizados BPF con información relevante, para sistemas críticos una descripción detallada</p> <p>4.4 Especificación de requerimientos de usuario que describan las funciones requeridas por el sistema basado en una evaluación de impacto BPF. Estos requerimientos deben ser trazables durante todo el ciclo de vida</p> <p>4.5 Asegurar que el sistema ha sido diseñado acorde a los requerimientos de usuario</p> | <p>11.10 (a) Validación del sistema para asegurar precisión, fiabilidad, consistencia para realizar su propósito de uso, y la habilidad de discernir registros inválidos o alterados</p> <p>11.10 (k)(1) Controles adecuados sobre la distribución, acceso y uso de la documentación para la operación y mantenimiento del sistema</p> | <p>9.13.4 El proceso de validación debe abarcar todas las fases relevantes del ciclo de vida de acuerdo con la categoría y arquitectura del sistema, para asegurar la exactitud, integridad y consistencia en el desempeño previsto de los Sistemas Computarizados</p> <p>9.13.2 Inventario de todos los sistemas computarizados</p> <p>9.13.4.2 Los componentes de la infraestructura de tecnología de la información y cualquier instrumento o equipo relevante deben ser calificados</p> <p>9.13.4.4 Si se emplea un Sistema centralizado en múltiples sitios, el proceso de validación debe incluir la verificación de los procesos ejecutados a través del Sistema en cada sitio individual</p> <p>9.13.5 Deben contar con una matriz de trazabilidad donde se documenten las múltiples etapas de especificaciones (incluyendo las revisiones) y las</p> |



**Tabla No. 3 comparativo de requerimientos Anexo 11, Parte 11 y NOM-059-SSA1-2015**

| EudraLex-Volumen 4-Anexo 11 Título   | CFR 21 parte 11  | NOM-059-SSA1-2015  |
|--|--|--|
| <p>4.6 Para la validación de sistemas computarizados personalizados debe haber un proceso que asegure la calidad y desempeño del sistema</p> <p>4.7 Evidencia de los métodos de pruebas y escenarios de pruebas deben ser demostrados. Específicamente considerar parámetros límites del sistema, límite de datos y manejo de errores.</p>   |  | <p>pruebas una vez que se han cumplido de manera satisfactoria</p>   |
| <b>Firmas Electrónicas / Registros Electrónicos</b>  |  |  |
| <p>14 Deben tener el mismo impacto que las firmas manuales, estar permanentemente ligado a un registro electrónico e incluir la fecha y hora</p> <p>15 Cuando un sistema computarizado se usado para certificación de registros y liberación de lotes, el sistema debe permitir solo a personas calificadas realizar la certificación y liberación de lotes mediante el uso de firmas electrónicas</p> | <p>11.5 (a) Las firmas electrónicas deben contener la siguiente información asociada</p> <ol style="list-style-type: none"> <li>1. Nombre impreso del firmante</li> <li>2. Fecha y hora cuando la fecha fue realizada y</li> <li>3. El significado (revisión, aprobación, responsabilidad o autorización)</li> </ol> <p>11.70 Las firmas electrónicas deben estar ligadas a su respectivo registro electrónico para asegurar que no pueden ser eliminadas, copiadas, o falsificadas.</p> <p>11.10 (j) Establecimiento y adherencia a políticas escritas que establecen las responsabilidades del personal sobre las acciones realizadas bajo su firma electrónica</p> <p>11.100 (a) Cada firma electrónica debe ser única para cada individuo y no debe ser reusada o reasignada a alguien más</p> <p>11.100 (b) Antes de que una organización establezca, asigne y/o certifique una firma electrónica se deberá verificar la identidad del individuo.</p> <p>11.100 (c) La equivalencia de las firmas electrónicas con las firmas manuales y la validez legal debe ser certificada ante la agencia</p> <p>11.200 (a) Las firmas electrónicas que no estén basadas en biometría deberán:</p> | <p>9.13.3.3 Cuando un sistema computarizado emplee firmas electrónicas éstos deben ser considerados en la validación</p> <p>9.13.6.1 Únicas e intransferibles</p> <p>9.13.6.2 Establecer fecha de vigencia y equivalencia</p> <p>9.13.6.3 Contar con código de identificación y contraseña</p> <p>9.13.6.4 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</p> <p>9.13.6.5 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</p> <p>9.13.3.3 Cuando un sistema computarizado genere registros electrónicos éstos deben ser considerados en la validación</p> <p>9.13.3.3.1 Son considerados registros electrónicos los documentos y registros que son creados, modificados, mantenidos, archivados, recuperados y/o transmitidos a través de sistemas electrónico.</p> <p>9.13.3.3.2 Debe existir evidencia documental para asegurar trazabilidad, fácil acceso e integridad a los mismos</p> |

**Tabla No. 3 comparativo de requerimientos Anexo 11, Parte 11 y NOM-059-SSA1-2015**

| EudraLex-Volumen 4-Anexo 11 Título  | CFR 21 parte 11   | NOM-059-SSA1-2015  |
|---|---|--|
|   | (1) Emplear al menos dos identificaciones distintas como código de identificación y contraseña<br>(2) Ser utilizados por el dueño de la firma<br>11.100 (b) Las firmas electrónica basadas en biometría deben ser diseñadas para asegurar que no pueden ser utilizadas por nadie más aparte de su dueño   |  |
| <b>Registro de Auditoría / Audit Trail</b>  |   |  |
| 8.2 Para registros que respaldan la liberación de lotes debe ser posible generar impresiones indicando cualquier cambio de datos.<br>9 Basado en un análisis de riesgo el sistema debe contar con un registro de auditoría para identificar cambios y eliminación de información BPF.<br>-Para cambios y eliminación de información debe haber una razón documentada<br>El registro de auditoria debe estar disponible para las agencias regulatorias<br>12.3 Debe haber registro de la creación, cambios y cancelación de autorización de accesos<br>12.4 El sistema debe tener la capacidad de registrar la identidad del operador, cambios, confirmación o eliminación de datos incluyendo fecha y tiempo. | 11.10 (e) Uso seguro de registro de auditoría, generado por computadora, con marca de tiempo para registrar fecha y hora de entrada de operadores, modificaciones o eliminación de registros electrónicos debe retenerse por un periodo al menos tan largo que el requerido para registros electrónicos y deben estar disponibles para revisión de agencias y copias. | 9.13.3.7 Basado en la valoración de riesgos determinar la necesidad de incluir un sistema de auditoría de datos, para registrar fecha y hora de ingreso de usuarios, así como acciones de crear, modificar o eliminar registros<br>9.13.3.7 .1 La auditoría de los datos (Audit trail) deberá prevenir su alteración y deberá estar disponible y convertible en un modo entendible, durante su periodo de retención, para permitir evidencia en la cadena de eventos.<br>9.13.5.2 Deberán implementarse procedimientos de control, que aseguren la revisión de la auditoría de datos de forma regular; la frecuencia y el método serán determinados, de acuerdo con el riesgo.<br>9.13.5.3 Los sistemas con la funcionalidad de auditoría de datos deben emitir información que permita verificar si algún dato ha sido alterado desde su ingreso original |
| <b>Transferencia de Datos</b>   |   |  |
| 4.8 Si existe transferencia de datos a otros formato o sistema, la validación debe verificar que no hay alteración de datos, valor o significado durante la migración de datos<br>5 para sistemas que intercambien datos electrónicamente con otros sistemas deben incluir verificaciones para el correcto y seguro ingreso y proceso de datos con el objetivo de minimizar el riesgo   | 11.10 h Usar dispositivos para determinar la validez de la fuente de entrada de datos o instrucciones operacionales   | 9.13.3.4 Los datos críticos capturados manualmente deben ser revisados por una segunda persona o por un medio electrónico validado<br>9.13.5.4 Si los datos son transferidos a otro formato de datos o sistema, la validación debe incluir la revisión de que los datos no sean alterados en valor y/o definición durante el proceso de migración  |

**Tabla No. 3 comparativo de requerimientos Anexo 11, Parte 11 y NOM-059-SSA1-2015**

| EudraLex-Volumen 4-Anexo 11 Título   | CFR 21 parte 11  | NOM-059-SSA1-2015   |
|--|--|---|
| 6 Para ingreso manual de datos, debe haber una verificación adicional de la precisión de los datos. Debe existir un análisis de riesgo para identificar los riesgos asociados a un proceso de ingreso de datos manual.   |  |   |
| <b>Almacenamiento de Datos</b>   |  |   |
| 7.1 Los datos deben ser protegidos por medio físico y electrónicos contra daños. Verificar accesibilidad, legibilidad y precisión durante el periodo de retención<br>7.2 Verificar durante la validación la capacidad de restaurar la información, se deben realizar respaldos de la información periódicamente<br>8.1 Debe ser posible obtener impresiones claras de la información electrónica almacenada<br>17 Los datos deben ser archivados. Verificar accesibilidad, legibilidad, confiabilidad e integridad de datos. Asegurar y probar la recuperación de datos cuando se realizan cambios relevantes (por ejemplo, equipo o programas de cómputo) | 11.10 b Capacidad de generar copias electrónicas precisas y completas y legibles de los registros para su adecuada inspección, revisión<br>11.10 (c) Protección de los registros para asegurar precisión y recuperación a través de periodo de retención de registros  | 9.13.3.1 Sistema de protección, integridad y respaldo de la información basada en una evaluación de riesgo. Asegurar accesos y legibilidad durante todo el tiempo de retención<br>9.13.3.5 Protección de datos por herramientas como copias de seguridad periódicas<br>9.13.3.6 La capacidad de restaurar los datos, así como la integridad y la exactitud para su respaldo, deberá ser verificada en la validación y monitoreados periódicamente |
| <b>Controles de seguridad</b>  |  |   |
| 12.1 Se deben tener Controles físicos y/o lógicos para restringir el acceso al sistema a personas no autorizadas por ejemplo claves, contraseñas, pase de tarjetas, códigos personas con contraseña, acceso biométrico, acceso restringido a equipo de cómputo y área de almacenamiento de datos<br>12.2 El grado de seguridad depende de la criticada del sistema   | 11.10 (f) Uso de verificaciones del sistema operativo para hacer cumplir la secuencia permitida de pasos y eventos<br>11.10 (g) Verificar que solo el personal autorizado puede usar el sistema, firmar electrónicamente, acceder a dispositivos de entrada y salida, alterar un registro o realizar una actividad a mano. | 9.13.3.2 Acceso controlado<br>9.13.3.2.1 Controles de seguridad físico y/o lógicos para restringir el acceso a usuarios (modificados periódicamente)<br>9.13.3.2.2. Bloqueo de usuarios después de cierta cantidad de intentos  |
| <b>Mantenimiento del estado validado</b>   |  |   |
| 11 Se debe realizar una evaluación periódica para confirmar que el estado validado se mantiene; debería incluir, cuando aplique: funcionalidades, registro de desviaciones, incidentes, problemas,   | Sin alcance  | 9.14.2 Debe efectuarse una revisión periódica a fin de determinar si es necesario una nueva validación<br>9.14.2.1 Si los sistemas no han tenido cambios significativos, la evidencia documental de que éstos cumplen los requisitos predefinidos es suficiente   |

**Tabla No. 3 comparativo de requerimientos Anexo 11, Parte 11 y NOM-059-SSA1-2015**

| EudraLex-Volumen 4-Anexo 11 Título  | CFR 21 parte 11   | NOM-059-SSA1-2015   |
|---|---|---|
| actualizaciones, historia, desempeño, fidelidad, seguridad y reportes del estatus de validación   |   | evidencia para demostrar el mantenimiento del estado validado<br>9.14.3 Cuando un cambio afecte la calidad o características del producto, o sus componentes y/o proceso debe llevarse a cabo una nueva validación  |
| <b>Administración de Incidentes</b>   |   |   |
| 13 Todos los incidentes, incluyendo fallas y error de datos deben ser reportados y evaluados. Para incidentes críticos Identificar causa raíz y realizar acciones preventivas y correctivas | Sin alcance   | Sin alcance   |
| <b>Capacitación del Personal</b>  |   |   |
| 2 Todo el personal debe tener las apropiadas calificaciones, niveles de acceso y definir responsabilidades para llevar a cabo sus actividades   | 11.10 Las personas que usan sistemas para modificar, mantener o transmitir registro electrónico deberá emplear procedimientos y usar controles diseñados para asegurar autenticidad, integridad y confidencialidad de los registros electrónicos<br>11.10 (i) Determinar que las personas que desarrollan mantienen o usan registros electrónicos/ firmas electrónicas en el sistema tienen la educación, capacitación y experiencia para desarrollar sus actividades.7 | 7.1.1 Con el número suficiente de personal calificado para llevar a cabo todas las actividades requeridas para la fabricación de medicamentos. El personal debe recibir inducción en BPF desde su contratación, entrenamiento en las actividades que va a realizar y capacitación continua.<br>7.1.2 El personal que participa en cualquier aspecto de la fabricación con impacto en la calidad del producto debe contar con el perfil requerido y ser continuamente capacitado y calificado.<br>7.1.2.1 El personal de reciente contratación debe recibir una capacitación adecuada previa a la ejecución de las tareas que le sean asignadas. |
| <b>Administración de Cambios</b>  |   |   |
| 10 cualquier cambio a un sistema computarizado, incluyendo la configuración debe ser realizado de una manera controlada de acuerdo a un procedimiento definido                              | 11-10 (k) (2) Procedimiento para control y revisión de cambios para mantener un registro de auditoría que documente tiempos de secuencia y modificaciones de la documentación del sistema   | 9.13.5.1 Todo cambio a un sistema computarizado debe realizarse de acuerdo con el sistema de control de cambios   |
| <b>Continuidad del negocio</b>  |   |   |
| 16 Para los sistemas computarizados que se utilizan en proceso críticos deben tomarse medidas   | Sin alcance   | Sin alcance   |

| <b>Tabla No. 3 comparativo de requerimientos Anexo 11, Parte 11 y NOM-059-SSA1-2015</b>                                |                        |                          |
|--|------------------------|--------------------------|
| <b>EudraLex-Volumen 4-Anexo 11 Título</b>  | <b>CFR 21 parte 11</b> | <b>NOM-059-SSA1-2015</b> |
| para garantizar la continuidad del proceso en caso de falla del sistema (por ejemplo, un sistema manual o alternativo) |                        |                          |

**Fuente:** Elaboración propia, 2018

### **6.5.1 Conclusiones**

Con base al análisis realizado podemos concluir que requerimientos de cada normativa serán tomados como referencia para la propuesta de validación de éste trabajo.

#### **Administración de Riesgo**

El Anexo 11 es muy específico en que la evaluación de riesgo debe este aplicada en todo el ciclo de vida del sistema a diferencia que la NOM 059 la cual es establece que sólo en el ciclo de validación, adicional a esto el Anexo 11 es muy específico sobre en qué puntos es necesario realizar una evaluación de riesgo

- Para identificar si una auditoría a un proveedor es necesaria
- Para determinar el alcance de la validación
- Para establecer un registro de Auditoría (Audi Trail)
- Para Transferencia de datos electrónica y manual

Se tomarán como referencia los requerimientos del Anexo 11.

#### **Proveedores de servicio**

Asegurar que los proveedores de servicio de software estén alineados a las políticas y estándares de la industria farmacéutica es crítico para la implementación de un nuevo sistema, en este contexto la Norma 059 es más rigurosa que el anexo 11 incorporando 2 requerimientos que dan valor agregado lo cuales:

- Programa de auditorías y
- Alcance de las pruebas realizadas por el proveedor

Se tomarán como referencia los requerimientos de la NOM 059.

#### **Validación**

Al revisar los requerimientos, se identifica que los requerimientos del Anexo 11 y los de la NOM 059 abarcan los requerimientos del CFR 21 parte 11 que se enfocan en asegurar la precisión, fiabilidad, consistencia y seguridad del sistema, sin embargo, el Anexo 11 y la NOM 059 solo coinciden que la validación debe aplicarse en todo el ciclo de vida y en contar con inventario de sistemas computarizados.

Se tomará como referencia los requerimientos del Anexo 11 y los de la NOM 059.

## **Firmas Electrónicas / Registro Electrónicos**

La NOM 059 y la parte 11, ambas se enfocan en la seguridad, autenticidad, y trazabilidad de las Firmas electrónicas y registros electrónicos adicional el CFR 21 parte solicita que las firmas electrónicas muestren si la firma es para revisión, aprobación, responsabilidad o autorización lo que representa un valor agregado para la trazabilidad de las acciones realizadas en el sistema

Se tomará como referencia el CFR 21 parte 11.

## **Registro de Auditoría (Audit Trail)**

Las tres regulaciones solicitan que los sistemas computarizados deben tener un registro de auditoría para registrar cambios y/o modificaciones en el sistema y para identificar la fecha y hora en los que se hicieron, al ser una función crítica del sistema, la NOM 059 solicita que se realice una revisión periódica del mismo.

Se tomarán como referencia los requerimientos NOM 059.

## **Transferencia de Datos**

Los requerimientos del Anexo 11 integran los requerimientos del la NOM 059 y del CFR 21 parte 11, para asegurar que la transferencia de datos electrónicos y manuales es precisa y confiable

Se tomará como referencia los requerimientos de la NOM 059.

## **Controles de seguridad**

La información y los datos electrónicos que se resguardan en un sistema computarizado está relacionada con las BPF, es información crítica para el negocio por lo que las tres regulaciones solicitan que el sistema tenga accesos controlados a usuarios autorizados mediante dispositivos físico y/o lógicos sin embargo en el CFR 21 parte 11 existen requerimientos para la gestión de contraseñas que si se cumplen pueden elevar la seguridad del sistema.

Se tomará como referencia los requerimientos del CFR 21 parte 11

## **Mantenimiento del estado validado**

Asegurar que el sistema mantiene su estado validado durante todo su ciclo de vida garantiza que mientras el sistema este en operación no hay un impacto a la calidad del producto, seguridad del paciente e integridad de la información. El Anexo 11 ya que establece los puntos a revisar (cambios, incidentes, funcionalidades, problemas, actualizaciones/cambios, seguridad, reportes de validación, entre otros)

para asegurar el mantenimiento el estado validado, El CFR 21 parte 11 no cuenta con requerimientos para este proceso y la NOM 059 solo establece que se debe realizar una revisión periódica, sin establecer que elementos revisar y hacer un análisis de los cambios realizados en el sistema.

Se tomará como referencia los requerimientos del Anexo 11.

### **Retiro del sistema**

Ninguna de las regulaciones específica las actividades que se deben realizar para el retiro de un sistema, sin embargo, al ser sistemas con impacto a las BPF se debe tener un proceso que asegure que una vez que el sistema se vuelva obsoleto, la información puede ser recuperada al menos en el tiempo establecido por la regulación (5 años de acuerdo a la NOM-059-SSA1-2015)

Con base al análisis comparativo realizado de las diferentes instancias regulatorias se propone una metodología de validación de sistemas computarizados que integre los requerimientos más completos de la normatividad mexicana, europea, estadounidenses y que adicionalmente describa los requerimientos para el retiro de un sistema computarizado.

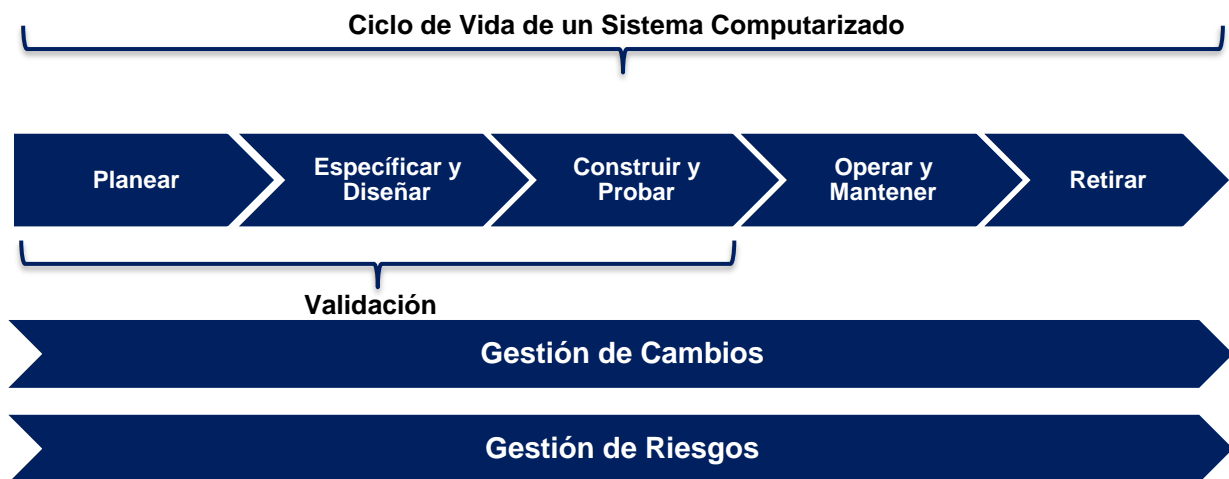


## 7. Metodología de Validación de Sistemas Computarizados

### 7.1 Ciclo de Vida de un Sistema Computarizado

El ciclo de vida de un sistema computarizado debe ser definido para asegurar que el mismo es diseñado, construido y probado adecuadamente para cumplir los requerimientos de usuario, requerimientos regulatorios, y que operan en un estado validado. En todo el ciclo de vida la gestión del riesgo y la gestión de cambios deben estar presentes. <sup>(9)</sup>

El ciclo de vida de un sistema computarizado se muestra en la Figura No. 1:



**Figura No. 1** ciclo de Vida de un Sistema Computarizado  
Fuente: Elaboración propia 2018

### 7.2 Validación

La validación incluye tres etapas del ciclo de vida de un sistema computarizado: Planear; Especificar y Diseñar; Construir y Probar, una vez que se realicen y se documenten cada una de las actividades, el sistema se considera validado.

#### 7.2.1 Planear

En esta primera etapa se debe describir la estrategia general de validación, el alcance del proyecto, las funciones y responsabilidades, las actividades de validación, incluyendo el análisis de riesgo, entregables de validación y procedimientos necesarios para la instalación adecuada del sistema.

### **7.2.2 Especificar y Diseñar**

Etapa en la que los usuarios deben definir los requerimientos específicos necesarios para que el sistema desempeñe sus funciones, satisfaga las necesidades de negocio, así como establecer las restricciones del sistema.

El sistema se debe adecuar para que cada una de sus funciones cumpla con los requerimientos de usuario.

### **7.2.3 Construir y Probar**

Una vez diseñado el sistema cada una de sus funciones debe ser probada, por lo que se debe definir una estrategia de pruebas, el ambiente de pruebas, los pre-requisitos necesarios, la secuencia de actividades y los criterios de aceptación.

Una vez que el sistema haya cumplido los criterios de aceptación definidos puede ser puesto en operación y considerado como validado.

## **7.3 Entregables de Validación**

Todas las actividades de validación realizadas deben estar documentadas, en la Tabla no. 4 Entregables de Validación, se muestra la propuesta de los diferentes entregables a realizar en cada etapa del ciclo de vida de un sistema computarizado y los requerimientos regulatorios en los que se basan.

| <b>Tabla No. 4 Entregables de Validación</b> |  |
|--|--|
| <b>FASE</b>                                  | <b>ENTREGABLES</b>   |
| Planear                                      | Evaluación de Impacto del Sistema  |
|  | Plan Maestro de Validación de Sistemas Computarizados  |
|  | Plan de Validación   |
| Especificar y Diseñar                        | Requerimientos de Usuario  |
|  | Evaluación del Proveedor   |
|  | Especificaciones de Diseño   |
|  | Especificaciones Funcionales   |
|  | Evaluación del Riesgo Funcional  |
|  | Matriz de Trazabilidad   |
|  | Reporte de la Administración de Riesgo   |
| Construir y Probar                           | Línea Base de Configuración  |
|  | Plan de Pruebas/ Reporte de Pruebas <ul style="list-style-type: none"> <li>• Calificación de Instalación</li> <li>• Pruebas de Aceptación de Usuario</li> <li>• Pruebas de Aceptación del Sistema</li> </ul> |
|  | Plan y Reporte de Migración de Datos   |
|  | Reporte de Validación  |
|  | Registro de Validación   |
|  |  |
| Operar y Mantener                            | Administración de Cambios Técnicos   |
|  | Revisión Periódica   |
|  | Administración de Discrepancias  |
| Retirar                                      | Plan/Reporte de Retiro   |

### 7.3.1 Evaluación de Impacto del Sistema

Antes de iniciar con la validación es importante identificar el impacto del sistema en las Buenas Prácticas de Fabricación (BPF) considerando la seguridad del paciente, calidad del producto e integridad de datos. Para realizar esta evaluación se propone utilizar las siguientes preguntas de actividades comunes relacionadas con las BPF:

- ¿El sistema es utilizado en la fabricación de medicamentos?
- ¿El sistema es utilizado en la administración de materiales, por ejemplo, en la inspección, almacenaje e inventarios?
- ¿El sistema es utilizado en actividades de control de calidad como pruebas de materia prima, controles en proceso, estabilidad o monitoreo ambiental?
- ¿El sistema es utilizado en el transporte y distribución de productos farmacéuticos o muestras de medicamentos?
- ¿El sistema, transfiere o reporta datos utilizados como fuente primaria para determinar la calidad del producto?
- ¿El sistema proporciona información para la identificación del producto (ejemplo: ¿número de lote, fecha de caducidad, ect)?
- ¿El sistema genera, transfiere o reporta datos los cuales no son usados como fuente de datos primaria para determinar la calidad del producto, pero se confían en ellos para tomar decisiones BPF?
- ¿El sistema es utilizado en la revisión de lotes, disposición de lotes y liberación de sustancias a granel, medicamentos o ingredientes activos farmacéuticos?
- ¿El sistema es utilizado para el registro, análisis y seguimiento de quejas de producto?
- ¿El sistema es utilizado para administrar y controlar procedimientos de operación, protocolos, especificaciones, etc.?
- ¿El sistema calcula y almacena datos para pruebas de control de calidad?
- ¿El sistema verifica, produce o modifica datos que pueden ser solicitados por autoridades regulatorias?
- ¿El sistema influye en la calidad del medicamento o seguridad del producto?

La validación debe ser realizada si el sistema tiene como propósito de uso alguno de los identificados en las preguntas anteriores.

### **7.3.2 Plan Maestro de Validación de Sistemas Computarizados**

El Plan Maestro de Validación de Sistemas Computarizados describe la estrategia general de validación y documenta el Programa de Revisión Periódica de los Sistemas Computarizados del Sitio. Es un documento vivo y debe ser actualizado cuando haya un cambio relevante en la estrategia general de validación.

La revisión debe asegurar que la estrategia de validación, los entregables, responsabilidades y referencias están vigentes. Se deberá realizar una revisión con mayor frecuencia cuando se realizan cambios significativos.

El Plan Maestro de Validación de Sistemas Computarizados debe contener la siguiente información <sup>(4)</sup>:

- Título, versión, autor, fecha de aprobación, firma y nombre de él/los responsables de autorizar el documento
- Propósito del plan
- Alcance
- Política de Validación
- Estrategia de Validación de Sistemas Computarizados
- Responsables de Validación de Sistemas Computarizados
- Inventario de Sistemas Computarizados con una breve descripción de cada sistema
- Mantenimiento del Estado Validado-Programa de Revisión Periódica
- Referencia a documentos aplicables (procedimientos de desviaciones, controles de cambios, administración de riesgos entre otros)

### **7.3.3 Plan de Validación**

Cuando un nuevo sistema computarizado sea implementado y no esté dentro del alcance del Plan Maestro se debe crear un Plan de Validación que debe contener información sobre el alcance del proyecto, estrategia de validación, funciones y responsabilidades, descripción del sistema que será validado, requisitos previos, secuencia de actividades y criterios de aceptación.

### **7.3.4 Evaluación de Riesgo del Sistema**

La Evaluación de Riesgo del Sistema determina el impacto BPF del sistema y el que pueda tener en la seguridad del paciente, calidad del producto e integridad de datos.

. La Evaluación de Riesgo del Sistema al menos debe considerar:

- El nombre y descripción del propósito de uso del sistema
- Evaluación de la relevancia BPF y determinar si se requiere una validación y si las firmas electrónicas y datos electrónicos estarán dentro del alcance.
- Una evaluación general del sistema computarizado para riesgos del negocio y riesgos tecnológicos para orientar los requerimientos del sistema (por ejemplo requerimientos para: procesar datos críticos/confidenciales del sistema, para asegurar el cumplimiento regulatorio, disponibilidad del sistema, entre otros) y para determinar si se requieren evaluaciones necesarias (por ejemplo Evaluación Funcional de Riesgo) o si se requieren algún entregable adicional (por ejemplo Evaluación/Auditoría del proveedor)
- Sección para la clasificación de Datos (se consideran datos confidenciales aquellos que están relacionados con la información del paciente).

La evaluación de riesgo de sistema ayudará para la estrategia general de validación y debe ser revisado y actualizado si es necesario cuando se presente algún cambio en el propósito de uso del sistema durante el ciclo de vida del mismo.

### **7.3.5 Requerimientos de Usuario**

Los requerimientos de usuarios deben estar relacionados con el negocio, ser relevantes, necesarios, priorizados y deben cumplir con las siguientes características:

- Específicos: Precisos y detallados, sin ambigüedad usando una terminología coherente
- Medibles: comprobables y/o verificables
- Alcanzables: técnicamente factibles
- Realizables: realista, considerando los recursos
- Rastreables: vinculado a requerimientos subsecuentes.

Cada requerimiento del sistema debe estar identificado con un ID único, deben redactarse en un lenguaje claro y preciso tanto para el usuario como para el proveedor y no deben ser contradictorios o estar duplicados.

Los requerimientos deben ser clasificado de acuerdo a su prioridad como:

- Críticos para el negocio: indican que los requerimientos deben ser parte de la solución. No implementar este tipo de requerimientos traerá problemas al negocio.
- Importantes: indican que es una característica necesaria para mejorar el negocio, productividad o rendimiento.
- Deseables: proporcionan características confortables adicionales, pero no son críticos para el negocio.

Los Requerimientos de usuario, son la base para la realización de las pruebas del sistema, por lo tanto, deben ser concluidos, revisados y aprobados antes de iniciar con la etapa de Diseño.

En caso de que existan nuevos requerimientos de usuario o tuvieran que ser eliminados y/o corregidos, el entregable tendrá que ser actualizado, re-aprobado y dejar documentados los cambios en el histórico correspondiente.

### **7.3.5.1 Requerimientos de Usuario Críticos para el negocio**

- El sistema debe contar con controles lógicos (ID único de usuario y contraseña y/o acceso biométrico) para restringir el acceso a personas autorizadas y proteger la información que almacena, procesa y trasmite.
- Si el sistema no es capaz de manejar cuentas únicas o con controles lógicos estos pueden ser sustituidos por controles de acceso físico y/o por procedimientos
- La contraseña aceptada por el sistema debe tener cierto grado de seguridad y caducidad.
- Las firmas electrónicas deben contar con un registro electrónico vinculado al nombre completo del firmante, fecha y hora de cuando fue ejecutada la firma, y el significado de la firma (como revisor, aprobador o autor).
- La firma electrónica debe ser visible tanto en la pantalla y copias impresas.
- Los registros electrónicos deben contener registro de auditoría de datos no modificable que incluya:
  - ID único de usuario.
  - Fecha y hora del evento (por ejemplo, creación, modificación, o eliminación del registro).
  - Valores antiguos y nuevos para modificaciones y eliminaciones.
  - Razón del cambio de registros

### **7.3.6 Evaluación del Proveedor**

Los potenciales proveedores de un sistema computarizado deben cubrir cada uno de los requerimientos de usuario definidos previamente; pero esto no basta como criterio de selección, pues también es importante determinar si el proveedor es capaz de proveer un sistema que se desempeñe de manera consistente y confiable y que pueda dar un servicio y soporte adecuado durante el tiempo de vida útil del sistema.

La selección y evaluación del proveedor puede ser realizada de las siguientes formas:

- Documentando la experiencia previa con el proveedor de sistemas existentes en la empresa o evaluando la documentación proporcionada por el proveedor de otros proyectos que ha desarrollado para otros clientes.

- Aplicando cuestionarios para evaluar el sistema de calidad y los estándares de desarrollo de software del proveedor.
- Realizando una auditoría al proveedor para evaluar su sistema de gestión de la calidad.

### **7.3.7 Especificaciones Funcionales**

Describen la propuesta de solución para la implementación de los requerimientos de usuario previamente aprobados, incluyen descripciones técnicas y detalles específicos, pero deben ser claros para que personas no expertas en el tema puedan entender.

En ocasiones, las mejores soluciones seleccionadas pueden obligar a reducir o cambiar algunos requerimientos, documentados en la Especificación de Requerimientos de Usuario, por lo que, al terminar y aprobar el documento de especificaciones funcionales, los requerimientos de usuario tendrán que ser revisados, actualizados y aprobados de nuevo en caso de que sea necesario.

Las especificaciones funcionales del sistema sólo son requeridas para aplicaciones personalizadas o productos configurados y define la funcionalidad del sistema, tomando como referencia los requerimientos de usuario.

### **7.3.8 Especificaciones de Diseño**

Documentan los detalles del diseño requerido para construir el sistema y deben ser basadas en las especificaciones funcionales.

Las especificaciones funcionales y de diseño deben ser aprobadas antes de pasar a la etapa de Construcción (programación y/o configuración del software).

Es importante mencionar que, en el caso de sistemas personalizados, el proveedor debe entregar toda la documentación del software, la entrega debe estar documentada. (de ser posible incluir el código fuente). La documentación debe ser almacenada en un lugar seguro de acceso controlado.

### **7.3.9 Evaluación del Riesgo Funcional**

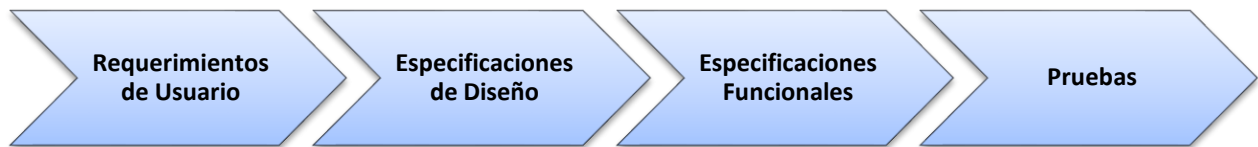
La evaluación del riesgo funcional nos permite definir los controles de seguridad para, eliminar, reducir y/ o mitigar los riesgos con impacto en la seguridad del paciente, calidad del producto e integridad de datos que se derivan debido a la implementación de un nuevo sistema computarizado o cambios en los mismos.

La evaluación del riesgo funcional también ayudará a determinar el nivel de riesgo de cada función del sistema y la profundidad con que será verificada durante la etapa de pruebas.



### 7.3.10 Matriz de Trazabilidad

Este documento se crea con el propósito de proporcionar evidencia suficiente de que todos los requerimientos de usuario han sido cubiertos, son trazables con las especificaciones del sistema y han sido verificados durante la etapa de pruebas. Ver Figura No. 2.



**Figura No. 2** Matriz de Trazabilidad  
**Fuente:** Elaboración propia 2018

La Matriz de trazabilidad es considerado como un documento “vivo” durante la validación y es creado en la etapa de Diseño y es actualizado durante la etapa de Pruebas.

### 7.3.11 Línea Base de Configuración

Previo a la calificación de instalación se debe tener un establecimiento formal de la lista de elementos de configuración que son parte del sistema computarizado (hardware, software y documentación) con sus respectivas versiones.

Este documento debe ser aprobado antes de realizarse la calificación de instalación con el objetivo de asegurar que se tienen los elementos necesarios para que el sistema pueda funcionar, en caso de que se requiera el cambio de un elemento durante la etapa de pruebas o durante el ciclo de vida del sistema este documento debe ser actualizado y se debe tener un cambio debidamente documentado.

### 7.3.12 Plan de Pruebas

El Plan de Pruebas debe incluir la estrategia de pruebas, criterios de aceptación y estar descrito con suficiente detalle.

Las pruebas son realizadas para asegurar que el sistema computarizado cumple con su propósito, requerimientos de usuario y especificaciones, previamente a la liberación del sistema.

La estrategia de pruebas consiste en:

1. Calificación de Instalación
2. Pruebas de Aceptación del Sistema
3. Pruebas de Aceptación del Usuario

### 7.3.13 Protocolos

Se debe contar con protocolos que documentan los casos de pruebas, los pasos, instrucciones, así como los criterios de aceptación para la ejecución de la Calificación de Instalación, Pruebas de Aceptación del Sistema y Pruebas de Aceptación del Usuario.

Un protocolo debe contar con la siguiente información básica:

**Título:** Incluye el título de la prueba, nombre del sistema, la ubicación (si aplica), versión y nombre/firma/fecha/departamento del autor y del aprobador.

**Alcance:** Define el objetivo y el alcance general de las pruebas, incluyendo una descripción del sistema a ser validado

**Registro de firmas:** Se debe contar con un registro de firmas para documentar firmas, nombres impresos, iniciales, así como compañías o contratistas que participaron en la ejecución de las pruebas

**Requisitos previos:** Establece los requerimientos que deben ser contemplados antes de iniciar las pruebas por ejemplo PNOs aprobados, controles de cambios abiertos/cerrados, capacitación del personal, etc.

**Pruebas:** Se definen las pruebas que deben realizarse, técnicas o procedimientos, número de corridas, la trazabilidad a las especificaciones funcionales y documentación de soporte requerida (fotos, copia de pantallas, ect.)

**Criterios de Aceptación:** Se documentan los resultados esperados de cada prueba con base a las especificaciones del sistema y requerimientos del usuario.

**Documentos de Referencia:** Referencia a los documentos de soporte utilizados durante la ejecución del protocolo

### 7.3.14 Calificación de Instalación

La calificación de instalación documenta que las instalaciones y equipos están instalados acorde a las especificaciones de diseño del sistema computarizado, dependiendo de los requerimientos del sistema se verifican: <sup>(13)</sup>

#### 7.3.14.1 Verificación de Línea Base de Configuración

Verificar que el Hardware del sistema se ajuste al especificado previamente en la línea base de configuración.

#### **7.3.14.2 Pruebas Analógicas de entradas y salidas**

Verificar la señal de entrada de los dispositivos de campo hacia el sistema computarizado y verificar la señal de respuesta del sistema hacia los dispositivos de campo y que estén de acuerdo a lo visualizado en las pantallas del sistema. Las señales de entrada analógicas deben ser verificadas en diferentes puntos para verificar la configuración del rango correcto del instrumento.

#### **7.3.14.3 Requisitos ambientales**

Verificar que se cumplen con las especificaciones para el buen funcionamiento del hardware, como temperatura, humedad, voltaje, frecuencia y verificar que se tenga suministro de energía **interrumpible** para proteger el hardware de un corte de energía inesperado.

#### **7.3.14.4 Configuración del Software**

Instalar el software y versión requerida en el hardware especificado en la línea base de configuración

Verificar que exista un duplicado del software instalado y que esté disponible (incluyendo cualquier configuración).

Registrar el procedimiento utilizado para la instalación del software y controlar la ubicación del procedimiento de instalación, registrar el medio físico y la ubicación donde este sea almacenado.

#### **7.3.14.5 Manuales de Operación y Mantenimiento**

Documentar los manuales de operación y mantenimiento para el sistema que ha sido adquirido y deben estar disponibles en forma impresa y en archivo electrónico para los usuarios finales.

#### **7.3.15 Pruebas de Aceptación del Sistema**

Son la verificación documental que aseguran que el sistema funciona de acuerdo a su propósito de uso a través de los rangos de operación predefinidos, las pruebas y criterios de aceptación del sistema deben estar basadas en las especificaciones funcionales y de diseño.

Para ejecutar las pruebas de aceptación del sistema la calificación de instalación debe estar concluida y en caso de tener desviaciones están deben estar cerradas.

Los siguientes elementos deben ser contemplados en las pruebas de aceptación del sistema que está siendo validado:

#### **7.3.15.1 Pruebas de lazo de control.**

Verificar que los lazos de control han sido configurados y documentar los parámetros de lazo ajustado

#### **7.3.15.2 Integridad de los datos**

Verificar la integridad de los datos relevantes a las BPF. Verificar que el sistema tenga la capacidad para identificar registros invalidos o alterados. Verificar los registros de audit trail del sistema, fecha y hora de los ingresos del operador y las acciones que genera, modifica y elimina información

#### **7.3.15.3 Fallas de comunicación**

Verificar la respuesta del sistema ante la pérdida de comunicación de alguno de los dispositivos

#### **7.3.15.4 Pérdida y restauración de energía**

Verificar la recuperación del sistema ante la pérdida y restauración de la energía eléctrica y que satisfaga las especificaciones funcionales

#### **7.3.15.5 Acceso y seguridad**

Verificar que la seguridad es la adecuada para evitar entradas no autorizadas al sistema. Verificar que los controles de seguridad del sistema funciones como están especificados.

#### **7.3.16 Pruebas de Aceptación del Usuario**

Son la verificación documentada de que el sistema se desempeña efectiva y confiablemente y cumple con los criterios de aceptación definidos por las especificaciones de requerimientos de usuario.

Antes de realizar las pruebas de aceptación de usuario se debe tener en consideración lo siguiente:

- Todas las pruebas de aceptación del sistema deben estar concluidas y todas las desviaciones deben estar documentadas y cerradas.
- Los procedimientos de operación y uso deben estar disponibles y aprobados.
- Los instrumentos que serán utilizados para coleccionar información durante las

pruebas, deben estar debidamente calibrados.

- Para la ejecución de éstas pruebas se puede requerir el uso de material de prueba o material de uso productivo, lo cual se debe especificar en el protocolo correspondiente.

Las siguientes pruebas deben ser incluidas ya que son consideradas como críticas para el sistema que está siendo validado:

#### **7.3.16.1 Pruebas positivas**

Pruebas destinadas para demostrar que, al ingresar valores válidos, el sistema funciona y cumple con un flujo de trabajo establecido por el usuario.

#### **7.3.16.2 Pruebas negativas**

Pruebas destinadas para demostrar que, al ingresar valores inválidos o excepciones el sistema no funciona.

#### **7.3.16.3 Pruebas usando múltiples escenarios**

Tienen como objetivo demostrar que, ante una serie de combinaciones de valores válidos, inválidos e intentos de violar la seguridad del sistema, el sistema responde de acuerdo a las expectativas del usuario

#### **7.3.16.4 Pruebas de facilidad de uso**

Este tipo de pruebas ayudan a que el usuario identifique tiempos de respuesta del sistema, interface usuario-software, contenidos de menús, gráficos entre otros.

#### **7.3.17 Reporte de Validación**

Documenta los resultados de las pruebas ejecutadas, las desviaciones y cambios en el sistema, en este reporte se concluye si el sistema se considera validado y se libera para uso productivo. El reporte de validación debe incluir:

- Título y versión del documento
- Nombre del sistema
- Número de páginas
- Nombre, firma y fecha del autor del documento
- Fecha de elaboración
- Nombre, firma y fecha del aprobador
- Fecha de aprobación
- Descripción del sistema

- Resumen y análisis de los resultados de las pruebas realizadas
- Resumen de todas las desviaciones de validación, resolución e impacto en el estado validado
- Referencia a los controles de cambio realizados para la implementación del sistema
- Listado con referencia a todos los entregables de validación
- Conclusión que establezca el cumplimiento de los criterios de aceptación de la validación, y el estado validado del sistema

#### **7.4 Gestión de Cambios**

Los cambios a un sistema computarizado BPF deben ser de una manera controlada durante todo el ciclo de vida del sistema.

Los cambios deben seguir un procedimiento y debe evaluarse el impacto y el riesgo que tienen en el sistema, así como las pruebas necesarias que deben realizarse para asegurar el estado validado.

#### **7.5 Gestión de Riesgos**

La gestión de riesgos debe ser aplicada en todo el ciclo de vida. Un enfoque basado en el riesgo es utilizado para determinar el grado de actividades de validación y controles de sistemas computarizados. Los controles de sistemas computarizados deben ser implementados en un nivel de formalidad y complejidad apropiado para el riesgo del sistema y del negocio. <sup>(9)</sup>

### **8. Operar y Mantener**

Una vez que el sistema computarizado haya sido validado, se deben establecer controles que aseguren que el estado validado se mantiene a través de su vida operacional.

El estado validado debe asegurarse mediante revisiones periódicas realizadas frecuentemente basadas en los riesgos del sistema.

#### **8.1 Frecuencia**

La frecuencia de revisión del sistema no está definida en ninguna de las regulaciones que han sido evaluadas, sin embargo, el Anexo 11 y la NOM 059-

SSA1-2015 mencionan que el enfoque basado en riesgo debe estar presente durante todo el ciclo de vida de un sistema computarizado, por lo que el riesgo del sistema puede ser el parámetro para determinar la frecuencia de revisión:

Frecuencia de revisión periódica de un sistema con base en su riesgo:

| <b>Tabla No. 5 Frecuencia de Revisión</b> |                   |
|---|-------------------|
| <b>Riesgo del Sistema</b>                 | <b>Frecuencia</b> |
| Alto                                      | 1 año             |
| Medio                                     | 2 años            |
| Bajo                                      | 3 años            |

Fuente: Elaboración propia 2018

Es importante mencionar que existen otros parámetros que pueden tomarse en cuenta para para reducir la revisión periódica, ejemplo:

1. Cambios relevantes en el sistema que redefinan el riesgo del sistema, ejemplo que el alcance de un sistema local cambie a u un alcance regional o global donde haya una gran cantidad de usuarios
2. Desviaciones en el proceso del cual el sistema éste siendo parte
3. Alguna instrucción o declaratoria establecida por parte del proveedor del software

Una vez definida la frecuencia de revisión periódica del sistema, esta debe ser documentada en algún procedimiento que sea parte del sistema de gestión de calidad, e incumplir con la revisión periódica en el tiempo especificado se considera una desviación que pone en riesgo la validación del sistema.

## **8.2 Revisión Periódica**

La revisión periódica se realiza con el fin de verificar que el sistema se ha mantenido bajo control durante su uso productivo y que no existen cambios no autorizados o desviaciones que comprometan su estado de validación:

Los elementos a considerar en la revisión periódica son los siguientes:

- Control de Cambios
- Documentación del Ciclo de Vida del Sistema
- Discrepancias
- Elementos de configuración
- Cuentas de usuario
- Registro de Auditoría (Audit Trail)

- Capacitación

### **8.3 Control de Cambios**

La revisión de que se realizaron y documentaron todas las actividades enlistadas en cada solicitud de cambio tiene como objetivo asegurar que en la implementación de uno o varios cambios no se comprometió la validación del sistema computarizado.

La revisión periódica no se puede concluir si existen controles de cambios abiertos y/o actividades abiertas relacionadas con el sistema.

### **8.4 Documentación del Ciclo de Vida del Sistema**

En la revisión periódica, la documentación es un elemento sumamente importante, ya que es el soporte ante cualquier instancia regulatoria que el sistema ha sido validado. Para asegurar que se cuenta con toda la documentación de validación del sistema, se debe hacer una verificación física y/o electrónica de las versiones aprobadas de todos los documentos relacionados en el Registro de Validación.

### **8.5 Desviaciones**

Las desviaciones presentadas por el sistema durante el periodo que comprende la revisión deben estar cerradas y deben ser evaluadas para descartar recurrencia y el impacto que tengan o hayan tenido en la validación del sistema.

En la revisión periódica sí se detecta alguna desviación abierta, no se puede concluir que el sistema mantiene el estado validado, y sí se detecta la recurrencia de una misma desviación es el momento justo para proponer actividades de validación (pruebas, cambios, etc.) que eliminen la causa raíz.

### **8.6 Elementos de Configuración**

Todos los elementos de la Línea Base de Configuración deben ser revisados periódicamente, el objetivo es asegurar que el hardware y software verificados en la calificación de instalación se mantienen, toda modificación en la línea base de configuración debe estar documentada en una solicitud de cambio.

Si en la revisión se detecta que uno de los elementos de configuración no está presente y no se cuenta con una solicitud de cambio, se debe abrir una desviación y evaluar el impacto en el estado validado del sistema.



## **8.7 Cuentas de usuario**

Es normal que durante el tiempo de vida del sistema computarizado haya cambios organizacionales que promuevan la creación o bajas de usuarios.

El propósito en la revisión periódica es asegurar que los permisos y roles de los usuarios activos en el sistema continúan vigentes, y que la baja y desactivación de los usuarios del personal que ya no laboré en la compañía se haya realizado conforme al procedimiento de Altas y Bajas de Usuarios.

El contar con una lista de usuarios no actualizada, no pone en riesgo la validación del sistema, pero se requiere de una desviación para realizar actividades de remediación y evitar recurrencia.

## **8.8 Registro de Auditoría (Audit Trail)**

Debido a que los cambios realizados por los usuarios que tienen acceso al sistema no se pueden controlar mediante solicitudes de cambios, se debe revisar el registro de auditoría (Audit Trail) para asegurar que la integridad de datos en el sistema se mantiene y que los usuarios han realizado un buen uso de la información.

En esta revisión el dueño del sistema y del proceso debe ser muy objetivo para determinar qué cambios realizados por el usuario son aprobados y que cambios son cuestionables, en caso de que se detecté que algún cambio realizado puso en riesgo la integridad de la información, el sistema pierde su estado validado.

## **8.9 Calificación del personal**

Todos los usuarios que tienen acceso al sistema deben contar con una capacitación formal de manejo y uso del sistema, así como deben conocer a detalle los permisos con los que cuenta su perfil de acceso.

La falta de capacitación de un usuario que tiene acceso al sistema pone en riesgo la validación del mismo, si en la revisión periódica se identifica que existe uno o algunos usuarios sin el entrenamiento adecuado para utilizar el sistema, se deben desactivar inmediatamente sus accesos y abrir una desviación del proceso.

## **8.10 Resultados y Plan de Acción**

Con la información obtenida de cada uno de los elementos revisados, se puede tener los siguientes resultados

- **Resultado 1:** El sistema mantiene el estado validado y no se requiere de acciones correctivas
- **Resultado 2:** Se mantiene el estado validado, pero se requiere de acciones correctivas
- **Resultado 3:** Existe un impacto potencial al estado validado y se requiere de acciones correctivas

#### **8.10.1 Resultado 1.**

##### **El sistema mantiene el estado validado y no se requiere de acciones correctivas**

Esta conclusión se obtiene cuando:

1. Todos los cambios realizados al sistema se encuentran documentados y con la evidencia suficiente de haber sido implementados sin afectar el estatus validado del sistema
2. Toda la documentación del ciclo de vida del sistema se encuentra disponible, vigente y actualizada.
3. No existen desviaciones relacionadas con el sistema o las desviaciones existentes se encuentran documentadas, analizadas y con acciones correctivas que eliminaron la reincidencia
4. Todos los elementos de Hardware y Software se encuentran física y lógicamente actualizados de acuerdo a la línea base de configuración
5. Los usuarios activos en el sistema están actualizados de acuerdo a sus funciones y responsabilidades del personal que tiene acceso.
6. No se han realizado cambios en el sistema por parte de los usuarios que pongan en riesgo la integridad de los datos
7. Todo el personal que tiene acceso al sistema se encuentra activo en la compañía y cuenta con la apropiada calificación en el sistema, así como los permisos en el mismo.

#### **8.10.2 Resultado 2.**

##### **Se mantiene el estado validado, pero se requiere de acciones correctivas**

Esta conclusión se obtiene cuando hay elementos que no cumplen el resultado esperado de la revisión periódica pero no pone en riesgo la validación del sistema, por lo que se deben proponer acciones y establecer fechas para lograr el cumplimiento, por ejemplo:

1. Desactivar usuarios que no necesitan más acceso al sistema o asignar el rol/permisos que le correspondan

2. Capacitar a los usuarios que cuentan con acceso al sistema y no cuentan con una capacitación del manejo y uso del sistema

### **8.10.3 Resultado 3.**

#### **Existe un impacto potencial al estado validado y se requiere de acciones correctivas**

Cuando se concluye éste resultado, se debe detener el uso del sistema ya que hay un alto riesgo de comprometer la integridad de datos y calidad del producto.

Esta conclusión se puede obtener cuando:

1. Hay cambios en el sistema inconclusos o sin la evidencia necesaria de que el estado validado del sistema no se haya afectado
2. Hay desviaciones relacionadas con el sistema sin analizar, con reincidencia y sin acciones de mejora
3. Hay cambio de hardware o actualización de software sin documentación de respaldo
4. En la revisión de audit trail se detecta manipulación o alteración de datos por parte de los usuarios.

El sistema podrá utilizarse hasta que se tengan acciones implementadas que aseguren que el uso del sistema no pone en riesgo la integridad de datos y calidad el producto.

### **8.10.4 Reporte de Revisión Periódica**

Para finalizar con la revisión periódica se debe contar con un reporte de revisión periódica donde se describa brevemente el objetivo de la revisión y el propósito de uso de sistema, también se debe documentar, anexar y/o hacer referencia a toda la evidencia revisada para facilitar la trazabilidad.

El reporte debe concluir alguno de los posibles resultados propuestos en el punto 4.3, y en caso de que se requiera abrir alguna desviación, solicitud de cambio y/o capa se debe referenciar el código o número de registro con el que se dará seguimiento dentro del sistema de calidad.

El reporte debe ser aprobado por el dueño del sistema y por la unidad de calidad.

## **9. Retiro de un Sistema Computarizado**

Cuando un sistema computarizado validado ya no se requiere para cumplir las funciones para las cuales fue diseñado, ya sea porque es una tecnología obsoleta o por la implementación de un nuevo sistema, comienza el proceso de retiro.

El retiro de un sistema computarizado validado debe ser de forma gradual y controlado para no tener un impacto negativo en la operación y mantener la integridad de los datos.

### **9.1 Plan de Retiro**

Se debe desarrollar un plan donde se establezca y se describa cada una de las actividades que se realizarán para el retiro del sistema, los sistemas e interfaces que estarán dentro del alcance y el cronograma de actividades

El plan de retiro debe estar aprobado por el dueño del sistema, dueño del proceso y el por la unidad de calidad.

### **9.2 Evaluación de Riesgo**

La gestión de riesgo debe estar presente hasta el retiro de un sistema, y la integridad de la información debe garantizarse aun cuando un sistema haya sido retirado por lo que es importante evaluar todos los riesgos asociados con las siguientes actividades de retiro:

- Transferencia de Datos
- Interfaz con otros sistemas
- Respaldo y recuperación de la información

Cada normativa tiene requerimientos específicos para la retención de la información, en el caso de COFEPRIS la información debe estar disponible al menos 5 años después de la producción de un medicamento <sup>(5)</sup>, la evaluación de riesgo ayudará a implementar controles que reduzcan el riesgo de pérdida de información.

### **9.3 Solicitud de Cambio**

Al igual que la gestión de riesgos, la administración de cambios debe estar presente durante todo el ciclo de vida de un sistema, por lo que las actividades de retiro deben estar documentadas en una solicitud de cambio y aprobada por el área de calidad.

## **9.4 Actividades de Retiro**

### **9.4.1 Desactivación del Sistema**

Es la primera etapa del retiro donde el sistema se remueve de la operación y deja de ser productivo, las cuentas de usuario son desactivadas o configuradas con acceso de sólo lectura, las interfaces con otros sistemas son deshabilitadas y ningún dato o información puede ser ingresado al sistema. También todos los procedimientos relacionados con el sistema deben ser dados de baja y/o actualizados.

### **9.4.2 Migración de Datos**

Es la actividad donde se transfieren datos electrónicos de un sistema a otro, o simplemente la transición de datos de un estado a otro. Esta actividad puede ser realizada durante las diferentes etapas del ciclo de vida de un sistema computarizado, por ejemplo:

- Durante el desarrollo e implementación de un sistema
- Durante la actualización de un sistema
- Durante el retiro de un sistema

En el retiro se debe determinar los datos que están dentro del alcance y como mínimo, evaluar los posibles riesgos y proporcionar estrategias de mitigación con lo relacionado a:

- Pérdida de integridad de datos
- Capacidad para proteger confidencialidad, incluyendo la información del paciente
- Conservación de la integridad y contenido de los datos
- Conservación del vínculo de Registros electrónicos/Firmas electrónicas, cuando aplique
- Capacidad para recuperar/reconstruir los datos para facilitar la lectura
- Capacidad para satisfacer los requerimientos de retención
- Retiro y retención de procedimientos/procesos existentes
- Retiro y retención de documentación asociada al sistema

### **9.4.3 Desmantelamiento**

Una vez que se asegure que los datos del sistema han sido transferidos en su totalidad al nuevo sistema y/o formato es posible continuar con las actividades de desmantelamiento.

En esta etapa el software es desinstalado y los componentes de hardware se remueven físicamente de las instalaciones, para asegurar el desmantelamiento completo del sistema se recomienda hacer una verificación de lo desinstalado con la Línea Base de Configuración del Sistema.

#### **9.4.4 Eliminación**

Esta última etapa del retiro sucede cuando los requerimientos de retención hayan sido concluidos y cualquier información y documentación relacionada con el sistema puede ser destruida.

El tiempo de retención está definido por la regulación y por los lineamientos corporativos de cada compañía.

## 10. Conclusiones

La validación de sistemas computarizados es crucial para las empresas farmacéuticas, actualmente tiene una gran importancia para las agencias regulatorias y es un punto importante en auditorías e inspecciones, para lograr una validación fructífera es necesario contar con una metodología lo suficientemente descriptiva de las actividades a realizar para cumplir con los requerimientos regulatorios, cualquier empresa que no logró demostrar ante las agencias regulatorias que sus sistemas han sido validados, inmediatamente pone en riesgo la seguridad del paciente, calidad del producto e integridad de datos, las consecuencias pueden ir desde una observación en una auditoría hasta el retiro comercial de productos, dependiendo de la criticada del sistema.

Las farmacéuticas nacionales que producen y comercializan sus productos en México, no están obligadas a cumplir con los requerimientos de la FDA o la EMA, se pueden limitar a cumplir con lo establecido en la NOM-050-SSA1-2015, sin embargo a medida que la tecnología avanza, los sistemas computarizados se vuelen más complejos, por lo cual se debe tener un proceso de validación directamente proporcional a la complejidad del sistema para disminuir el riesgo, la FDA, la EMA y la COFEPRIS por separado han realizado esfuerzos para actualizar sus requerimientos con diferentes enfoques, la FDA se esfuerza más por la integridad de datos y seguridad de la información, la EMA busca que cualquier actividad realizada sea basado en un análisis de riesgo y la última actualización de la COFEPRIS tiene un poco de ambas, unificar los requerimientos de las tres regulaciones fortalece el proceso de validación y aumenta el control para las nuevas tecnologías.

Las farmacéuticas que produce sus medicamentos en México y que los comercializa en Estados Unidos y Europa, además de cumplir con los requerimientos de la regulación nacional, están obligados a cumplir con lo establecido por la FDA y la EMA, por lo que esta propuesta de metodología puede ser adoptada como guía para el cumplimiento de los requerimientos regulatorios de las tres regulaciones, ya que se tomaron los criterios más rigurosos de cada regulación.

Las regulaciones mencionan que el estado validado se debe mantener hasta el retiro del sistema mediante la ejecución de revisiones periódicas, sin embargo, no especifican la frecuencia en que debe realizarse, en esta metodología se propone una estrategia de revisión basado en el riesgo del sistema y los controles críticos, así como los posibles resultados que se pueden obtener una vez ejecutada la revisión periódica.

Ante las nuevas soluciones que la tecnología ofrece, los sistemas cada vez tienen un menor tiempo de vida, por lo que las farmacéuticas se están enfrentando más frecuentemente a retiros de sistemas que se vuelven obsoletos. Para la fase de retiro del sistema las regulaciones disponibles no ofrecen mucho, se limitan a solicitar la recuperación y disponibilidad de la información en los tiempos establecidos. Por lo anterior esta propuesta ofrece una estrategia de las actividades que se deben realizar para un retiro controlado, documentado y con el menor riesgo a los procesos donde el sistema está involucrado.

## 11. Bibliografía

1. Asociación Nacional de Fabricantes de Medicamentos. A.C. (2016). La industria Farmacéutica, recuperado el 20 de octubre de 2016 de <http://www.anafam.org.mx/industria.htm>
2. Mesa editorial Merca2.0 (2018). Industria farmacéutica en México, recuperado el 24 de septiembre de 2019 de <https://www.merca20.com/industria-farmaceutica-mexico/>
3. Ruy Alonso Rebolledo(10 Junio 2017), ¿Cómo le va a la industria farmacéutica en México?, recuperado el 24 de Octubre de 2019 de <https://www.economista.com.mx/empresas/Como-le-va-a-la-industria-farmaceutica-en-Mexico-20170610-0010.html>
4. Código F, La revista de la CANIFARMA., 22 Mar 2017, Entrevista al Ing. Rafael Gual Cosío, Director General de CANIFARMA.
5. Organización Mundial de Salud Ginebra (2002). Cómo desarrollar y aplica una política farmacéutica, pp 25 3.2 Marco de la legislación farmacéutica
6. Daniel Yañez Flores, (19 septiembre 2018), Requerimientos regulatorios para sistemas computarizados validables, recuperado el 20 de agosto de 2019 de <https://www.linkedin.com/pulse/requerimientos-regulatorios-para-sistema-validables-cnqfb/>
7. Rodrigo Perez (5 DE Abril 2018) Why is Computer System Validation Required and What Happens if you Don't Comply?, recuperado el 5 de septiembre de 2019 de <https://validationcenter.com/why-computer-system-validation-required/>



8. Diamonn Ivan, (2004), Computer System Validation, pp. 3-3, recuperado el 30 de junio de 2016 de [https://embed.topra.org/sites/default/files/regrapart/1/923/2004N09\\_Focus.pdf](https://embed.topra.org/sites/default/files/regrapart/1/923/2004N09_Focus.pdf)
9. Norma Oficial Mexicana NOM-059-SSA1-2015, Buenas prácticas de fabricación de medicamentos.
10. Mosquera Sierra, José Javier; Cabrera Rabí, Leila, (2005), Validación y las buenas prácticas de fabricación en la producción de ingredientes farmacéuticos activos no estériles de origen natural, pp. 2-2, recuperado el 05 de noviembre de 2016 de <http://www.redalyc.org/pdf/1812/181220525046.pdf>.
11. International Conference on Harmonization (ICH), Q10 Pharmaceutical Quality Systems
12. KPMG, (22 mayo 2017), Industria farmacéutica en México se fortalece, recuperado el 29 Oct 2019 de <https://home.kpmg/mx/es/home/tendencias/2017/05/industria-farmaceutica-en-mexico-se-fortalece.html>
13. Julia Kagan, (13 Octubre 2019), European Medicines Agency (EMA), recuperado el 20 de Octubre de 2019 de <https://www.investopedia.com/terms/e/european-medicines-agency-ema.asp>
14. Microsoft, Food and Drug Administration CFR Title 21 Part 11, recuperado el 20 de octubre de 2016 de <https://www.microsoft.com/en-us/TrustCenter/Compliance/FDA>
15. Pharmaceutical CGMPs (Agosto 2013), Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application, recuperado el 30 Noviembre de 2018, de <https://www.fda.gov/media/75414/download>
16. Oliver Pearce, The Beginner´s Guide to Eudralex Vol. 4 Annex 11, recuperado el 15 de Octubre de 2019 de <https://blog.montrium.com/blog/the-beginners-guide-to-eudralex-vol-4-annex-11>
17. Valentina González, Marzo 2013, Norma para elevar calidad en medicinas, recuperado el 20 de Octubre de 2019 de

<https://manufactura.mx/industria/2013/03/24/norma-para-elevar-calidad-en-medicinas>

18. Julio César Roche López, Julio 2015, Dictamen Total, con efectos de final, respecto del anteproyecto denominado Proyecto de Norma Oficial Mexicana PROY-NOM-059-SSA1-2015, Buenas Prácticas de Fabricación de Medicamentos
19. EudraLex - Volume 4 Good manufacturing practice (GMP) Guidelines, Annex 11 Computerized Systems
20. Code of federal regulations (CFR) Title 21 Part 11 Electronic Records, Electronic Signatures
21. International Society for Pharmaceutical Engineering (ISPE), 2008, GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems
22. LeonResearch, Qué es una CRO y cómo puede ayudarte en tu estudio clínico, recuperado el 19 de noviembre de 2018 de <https://leonresearch.com/es/que-es-una-cro-y-como-puede-ayudarte-en-tu-estudio-clinico/>
23. FDA, U.S. Food and Drug Administration, Part 11, Electronic Records; Electronic Signatures — Scope and Application, recuperado el 30 de octubre de 2016 de <https://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm>
24. Japanese guideline “Guideline on Management of Computerized Systems for Marketing Authorization Holders and Manufactures of Drugs and Quasi-Drugs”
25. Pharmaceutical Inspection Convention (PIC/S) Guidance, Good Practices for Computerised Systems in Regulated “GXP” Environments
26. Menes Leonardo, Castillo Mayra, COFEPRIS en la vanguardia de cooperación internacional, 2016, Revista electrónica COFEPRIS Protección y Salud, recuperado el 20 de noviembre de 2017 de <http://revistacofepris.salud.gob.mx/n/no3/acciones.html>
27. Giselle Pérez Zazueta, 2013, Industria Farmacéutica, recuperado el 30 Octubre de 2019 de [https://www.gob.mx/cms/uploads/attachment/file/62881/130820\\_DS\\_Farmaceutica\\_ESP.pdf](https://www.gob.mx/cms/uploads/attachment/file/62881/130820_DS_Farmaceutica_ESP.pdf)
28. Reviste electrónica Dinero, (19 octubre 2019) Los mayores exportadores de medicamentos en el mundo, recuperado el 30 de octubre de 2019.