UNIVERSIDAD PERUANA
CAYETANO HEREDIA

Facultad de
Ciencias e Ingeniería

IMPLEMENTACIÓN DE UN PLAN MAESTRO DE VALIDACIÓN PARA SOFTWARE DE EQUIPOS ANALÍTICOS DE CONTROL DE CALIDAD EN UN LABORATORIO FARMACÉUTICO CON ENFOQUE EN CFR 21 PARTE 11

TRABAJO DE SUFICIENCIA PROFESIONAL PARA OPTAR POR EL TÍTULO PROFESIONAL DE QUÍMICO FARMACÉUTICO

AUTOR(ES)
LOÏC GABRIEL FERREYROS ARCINIEGA

ASESOR(ES)
ROBERTO MICHAEL ORIHUELA ECHAVIGURIN

LIMA - PERÚ
2026

Revisores

Revisor 1: Mg. Carlos Enrique Cabrera Garcia

Revisor 2: Mg. Humberto Ricardo Laserna Zubiaga

UNIVERSIDAD PERUANA
CAYETANO HEREDIA

DECLARACIÓN DE ORIGINALIDAD

Los egresados:

Nº	APELLIDOS Y NOMBRES
1.	FERREYROS ARCINIEGA LOÏC GABRIEL

Pertenecientes al programa de la **CARRERA PROFESIONAL DE FARMACIA Y BIOQUÍMICA**, autores del trabajo titulado: **IMPLEMENTACIÓN DE UN PLAN MAESTRO DE VALIDACIÓN PARA SOFTWARE DE EQUIPOS ANALÍTICOS DE CONTROL DE CALIDAD EN UN LABORATORIO FARMACÉUTICO CON ENFOQUE EN CFR 21 PARTE 11**, el cual ha sido elaborado, sustentado y aprobado, según corresponda, para optar por el **TÍTULO PROFESIONAL DE QUÍMICO FARMACÉUTICO** bajo la modalidad de **TRABAJO DE SUFICIENCIA PROFESIONAL.**

En calidad de docentes asesores de la Universidad Peruana Cayetano Heredia:

Nº	APELLIDOS Y NOMBRES DEL DOCENTE	FACULTAD	NIVEL DE ASESORÍA
1.	ORIHUELA ECHAVIGURIN ROBERTO MICHAEL	FACI	ASESOR

Declaramos que el contenido del presente documento es original y que las citas y referencias a otros autores cumplen con las normas académicas establecidas. En ese sentido, hacemos constar que:

- El documento presenta un porcentaje de similitud de **14%**, según el reporte emitido por el software **Turnitin®** (identificador de entrega: **3614618959;** fecha de entrega: **20/07/2026**).
- Tras una revisión detallada del reporte y del contenido del trabajo en cuestión, no se han identificado indicios de plagio.
- Se certifica que el documento respeta los principios de integridad académica y cumple con los requisitos institucionales de originalidad.

Lugar y fecha: **Lima, 20 de julio de 2026.**

Firma del asesor

Nº DNI: 40432215

ORCID: 0000-0003-4232-0419

TABLA DE CONTENIDO

RESUMEN

El presente trabajo de suficiencia profesional tiene como objetivo demostrar la experiencia adquirida en el proceso de implementación de un Plan Maestro de Validación en el área de Control de Calidad en un laboratorio farmacéutico de una transnacional ubicado en Lima Perú laborando como Analista de Control de Calidad.

A lo largo de los años la evolución de la tecnología significó la mejora de todos los aspectos relacionados a garantizar la eficacia y seguridad de los medicamentos. Uno de esos aspectos es la aplicación de registros electrónicos en softwares de equipos analíticos que revolucionan la forma de afianzar la trazabilidad de los datos y resultados de los procesos analíticos que permiten ser resguardados de una forma más segura. Por tal motivo la FDA implementó la normativa CFR 21 parte 11. Esto con la finalidad de asegurar la integridad datos al definir los criterios bajo los cuales los registros electrónicos y las firmas electrónicas sean fiables, confiables y equivalentes a los registros en papel. En el Perú este requisito es obligatorio desde el 2019, no obstante, muchas farmacéuticas nacionales recién lo están comenzando a implementar. El Plan Maestro de Validación (PMV) es un documento estratégico que define y guía las actividades de validación dentro de una organización farmacéutica. Fue necesario implementar un PMV enfocado en los softwares de equipos analíticos que cumpla la función de mostrar en forma de procedimiento el proceso de validación de software que culmina con la evidencia de la validación de un software de equipo analítico que permite grabar datos seguros, no alterables y con registro de fecha y hora del personal que realizó un rol y acción específico. Además de cumplir con el CFR 21 parte 11 consolida GAMP 5 e integra las actualizaciones nacionales dictaminadas en el Manual BPM de DIGEMID 2018 dándole

robustez al PMV implementado. El presente trabajo aborda el proceso de implementación de un PMV que cumple con la normativa mencionada y con la aprobación del comité de validaciones de la empresa.

Palabras Clave: Validación de Sistemas, Calidad, Integridad de Datos, PMV, CFR 21 Parte 11

ABSTRACT

The purpose of this professional proficiency project is to demonstrate the experience gained during the implementation of a Validation Master Plan in the Quality Control department of a multinational pharmaceutical laboratory located in Lima, Peru, where I worked as a Quality Control Analyst.

Over the years, technological advancements have led to improvements in all aspects related to ensuring the efficacy and safety of medications. One such aspect is the use of electronic records in analytical equipment software, which revolutionizes the way data traceability and results from analytical processes are secured, allowing them to be safeguarded more securely. For this reason, the FDA implemented the CFR 21 Part 11 regulation. This was done to ensure data integrity by defining the criteria under which electronic records and electronic signatures are reliable, trustworthy, and equivalent to paper records. In Peru, this requirement has been mandatory since 2019; however, many domestic pharmaceutical companies are only now beginning to implement it. The Validation Master Plan (VMP) is a strategic document that defines and guides validation activities within a pharmaceutical organization. It was necessary to implement a VMP focused on analytical equipment software that serves to outline, in the form of a procedure, the software validation process, culminating in evidence of the validation of analytical equipment software that allows for the recording of secure, tamper-proof data, along with a time and date stamp indicating the personnel who performed a specific role and action. In addition to complying with CFR 21 Part 11, it consolidates GAMP 5 and incorporates the national updates mandated in the 2018 DIGEMID BPM Manual, thereby strengthening the implemented VMP. This paper addresses the process of implementing

a VMP that complies with the aforementioned regulations and has been approved by the company's validation committee.

Keywords: Systems Validation, Quality, Data Integrity, VMP, CFR 21 Part 11

I. INTRODUCCIÓN

La industria farmacéutica es un área vital en el sector de salud, ya que, se encarga de la manufactura, análisis, almacenamiento y transporte de productos farmacéuticos esenciales para la salud de la población. El objetivo principal de la industria farmacéutica es entregar un producto de la más alta calidad, seguridad y eficacia que cumpla con las normas y requisitos dictaminados por la entidad reguladora del país como también con normas internacionales.

No cumplir con una política de integridad de datos puede generar una gran cantidad de resultados no validados y resultar en problemas que afecten la salud de los pacientes, problemas de post venta y el retorno de productos fallidos que a su vez resultan en problemas financieros y de imagen de la compañía.(1)

En las últimas décadas el sector farmacéutico ha visto grandes avances tecnológicos. Esto ha significado el desarrollo de softwares que cuentan con historial de actividades (audit trail), roles de usuario, permisos especiales para realizar distintas actividades, entre otras características. A la vez estos softwares están conectados a los distintos equipos analíticos que son utilizados para el análisis de materia prima, estabilidades y productos terminados en los laboratorios de control de calidad de industrias farmacéuticas. De esta forma, los antiguos registros físicos en papel que pueden ser modificados, eliminados y perdidos comienzan a ser reemplazados por los registros electrónicos.

Estos cambios ocasionan que se deba comprobar que dichos softwares garanticen la integridad de datos. En 1997 la FDA comenzó a implementar la CFR 21 Parte 11 que es una regulación que impone los criterios para que los registros electrónicos, firmas electrónicas y firmas a mano ejecutadas para registros electrónicos sean fiables, dignos

de confianza y, en general equivalentes a los documentos en papel y a las firmas manuscritas en papel. Además, hace hincapié en que el alcance de esta normativa incluye a sistemas computarizados como software y hardware. (2)

En el 2002 la FDA publicó un documento respecto a los principios generales para la validación de software como guía para las industrias farmacéuticas. Poniendo énfasis en que la validación del software es la verificación mediante análisis y aporte de pruebas objetivas que las especificaciones del software se ajustan a las necesidades y el uso previsto por el usuario y que estos requisitos implementados a través del software puedan cumplirse de manera sistemática. Con esto se tienen dos documentos de normativa de referencia para utilizarlos como guía para validar softwares que garanticen integridad de datos y el adecuado manejo de firmas electrónicas. (3)

Se podría pensar que con los documentos mencionados anteriormente que provienen de una entidad que es utilizada como referencia internacional (FDA) es suficiente para validar softwares, pero, no es así. Si se quiere tener una validación completa es necesario incluir la guía de referencia técnica GAMP 5 elaborada por la ISPE (International Society of Pharmaceutical Engineering). Dicha guía es vital para asegurar las buenas prácticas de fabricación automatizada que, al ser implementadas correctamente, aseguran la validación y mantenimiento de sistemas automatizados para fabricar productos de alta calidad. Se basa en cinco conceptos que son el conocimiento del producto y el proceso, el enfoque basado en el ciclo de vida dentro de un sistema de gestión de la calidad, actividades escalables del ciclo de vida, gestión de riesgos de calidad y potenciar la participación de proveedores. (4,5)

Con respecto a la realidad nacional, las normativas y guías mencionadas anteriormente se vienen implementado gradualmente en los últimos años. Tanto el usuario como el auditor vienen ganando experiencia y conocimiento en estos temas.

En el Manual de Buenas Prácticas de Manufactura de Productos Farmacéuticos 021-2018-SA de la DIGEMID ya se contemplan las consideraciones que se deben tomar cuando se usan firmas electrónicas y también cuando el sistema computarizado genera registros electrónicos.(6) Todo esto en base a el CFR 21 parte 11 de la FDA.

En la actualidad es un requisito indispensable la validación de sistemas electrónicos y softwares cumpliendo los lineamientos de CFR 21 parte 11 y que la evidencia este documentado apropiadamente.

Para poder garantizar la calidad y fiabilidad de los productos farmacéuticos se deben seguir diversas actividades a lo largo de toda la cadena de producción, calidad y aseguramiento. Estos procesos deben estar documentados y validados con el fin de poder analizar cada paso y etapa de los procesos que se llevan a cabo. Esto es primordial para de esta forma analizar paso a paso los procesos lo cual permite detectar fallas de una forma más precisa, comprobar que los procesos se estén realizando de acorde a las regulaciones estipuladas, minimizar riesgos al poder observar todos los procesos paso a paso e identificar las partes críticas, entre otras cosas. El primer paso para lograr que se lleven a cabo estas actividades que finalicen en la validación es un PMV. (7)

Se ha tomado como referencia ANVISA (Agencia Nacional de Vigilancia Sanitaria) ente regulatorio de Brasil. Esto debido a que Brasil forma parte de PIC/S (Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme) un convenio de carácter internacional del cual los países que forman parte cooperan en el

tema de BPM entre las entidades reguladoras y la industria farmacéutica. Este convenio tiene como principal objetivo validar y dar reconocimiento a las auditorias e inspecciones llevadas a cabo en un país miembro como válidas para también los demás países miembros.

Se tuvo como guía el documento PE009-17, Anexo 11 de PIC/S que está contemplado en la normativa de ANVISA.(8) Utilizando de forma referencial requisitos necesarios por un convenio internacional que con miras al futuro podría significar la validez de carácter internacional de prestigio de dicho PMV. Con miras a un futuro cercano, ya que, Perú en la actualidad es miembro observador de PIC/S y dentro de poco podría ser miembro.

El PMV es parte fundamental del sistema de gestión de la calidad de un laboratorio farmacéutico que documenta la información referente a las actividades de validación que la organización debe realizar, donde se definen detalles y escalas de tiempo para cada trabajo de validación a ejecutar. Es primordial que las responsabilidades con dicho plan estén establecidas en dicho documento.(6)

El PMV es un documento que contiene un cronograma con la lista de actividades que se deben realizar para poder validar un proceso además de detallar quienes serán los responsables de cada actividad (asignación de roles).

Es crucial tener un PMV que tenga integrado el CFR 21 parte 11, principalmente vinculado a los softwares integrados a los equipos analíticos de control de calidad.

El PMV debe ser una guía detallada y precisa que permita que las validaciones de software de equipos analíticos que se lleven a cabo garanticen la integridad de datos cumpliendo CFR 21 Parte 11 en un laboratorio farmacéutico en Lima, Perú.

Identificar y clasificar los equipos analíticos en el área de control de calidad según la criticidad de validarlos según el software que utilizan y el riesgo que conlleva fue crítico para tener un PMV estructurado de tal forma que los equipos de mayor riesgo sean validados primeros.

Fue indispensable establecer requisitos regulatorios según CFR 21 parte 11, el Manual de BPM 2018 y GAMP 5. De esta forma se garantizó que el PMV esté alineado tanto a la normativa nacional como la internacional. También así asegurando que los registros y firmas electrónicas sean equivalentes a la data primaria.

Para definir una estrategia que logre que el PMV sirva como una guía eficiente en la validación de softwares de equipos analíticos se utilizó un diagrama de Gantt y matrices para trazar el cumplimiento de CFR 21 Parte 11, BPM DIGEMID y GAMP 5. Permitiendo monitorear el cumplimiento de las actividades de forma minuciosa y a la vez realizarlo de forma ordenada, cronológica y dentro de los tiempos estimados.

El presente trabajo se justifica debido a que aporta al constructo del proceso de validaciones de softwares, también como referencia para implementación de PMV en otras compañías farmacéuticas que requieran regularizar la documentación y de aporte a la comunidad científica cuyo enfoque sea la validación de sistemas informáticos.

II. OBJETIVOS

Objetivo General

Implementar un PMV para software de equipos analíticos garantizando la integridad de datos cumpliendo CFR 21 Parte 11 en un laboratorio farmacéutico en Lima, Perú.

Objetivos Específicos

1. Establecer requisitos regulatorios según CFR 21 parte 11, el Manual de BPM 2018 y GAMP 5 que estén incluidos en el PMV.
2. Identificar y clasificar los equipos analíticos en el área de control de calidad de una forma que permita tener una estrategia para realizar las validaciones dentro de un rango de tiempo deseado.
3. Definir una estrategia para validar los softwares de los equipos analíticos.

III. METODOLOGÍA

Previo a la redacción del PMV se revisaron PMV de similar índole como referencia y guía estructural para la PMV actual.

Se hizo una revisión documental de r CFR 21 parte 11 y GAMP 5 y la última versión del manual BPM DIGEMID 2018.

Se inició el documento explicando el propósito del PMV donde, se resalta la importancia de validar los softwares con CFR 21 parte 11 y la estrategia que se va a realizar para poder lograr eso.

Se incluyó un glosario con todas las palabras claves que se mencionan a lo largo del documento con sus respectivas abreviaciones.

Se menciona al comité de validación que va formar parte en todo el proceso de la validación. Incluyendo además los roles y funciones que cada una va cumplir en el proceso de validación (Ver Anexo 5 y Anexo 6).

Se deben establecer los requisitos que el software debe cumplir según las necesidades del laboratorio. Para ello en el PMV se establecen las pautas para redactar y elaborar el documento de especificaciones de requisitos del usuario (URS) (Ver Anexo 3).

Se incluyó un inventario de los equipos analíticos del área de control de calidad donde están catalogados según el tipo de software que utilizan o que utilizarán según lo descrito en GAMP 5 y USP <1058> y la criticidad de cada uno. (Ver Anexo 2).

Se evaluó la criticidad de cada equipo y su software utilizando como herramienta el análisis de riesgo (AR) usando el NPR (Número de Prioridad de Riesgo) similarmente a lo mostrado en el trabajo de PORTIER (11). Se usó una escala de riesgos que muestra la

forma de calcular y clasificar el puntaje de NPR obtenido. (Ver Anexo 7). Con este análisis de riesgo se establecen acciones necesarias para mitigar impactos que puedan afectar el cumplimiento de CFR 21 parte 11.

Se incluyó en tablas los requisitos de cumplimiento de CFR 21 Parte 11 y los criterios de aceptación necesarios para el cumplimiento de URS, AR, IQ, OQ y PQ. (Ver Anexo 4 y Anexo 9)

Se incluyó en el PMV un diagrama de Gantt para tener ordenado en base a tiempos y fechas cada actividad que se va a desarrollar según la criticidad del equipo analítico según lo mostrado en el AR. (Ver Anexo 1).

Como parte final del PMV se incluyó un ciclo de vida con información respecto a controles de cambios, POEs, entrenamiento constante a personal, políticas de buenas prácticas de documentación, mantenimiento preventivo de equipos analíticos y software. (Ver Anexo 8)

IV. RESULTADOS Y DISCUSIÓN

Como resultado de la implementación exitosa del PMV se logró tener una estrategia adecuada para poder validar los softwares de los equipos analíticos.

Parte fundamental de tener una estrategia adecuada fue realizar un diagrama de Gantt (ver Anexo 1) que muestre de forma gráfica y comprensiva las diversas actividades que se deben llevar a cabo. Además de delimitar las actividades, el diagrama muestra la duración aproximada que debe tomar cada actividad.

Se tomó en cuenta el mantenimiento del estado validado. Para poder mantener el estado validado de los softwares de equipos analíticos se deben realizar monitoreos y el respaldo de la información almacenada en el software para ver que cumpla con los requisitos mencionados en el URS, IQ, OQ y PQ. Estas actividades se mencionan en el diagrama de Gantt como mantenimiento preventivo de software. Teniendo un PMV que toma en cuenta el ciclo de vida de la validación al hacer un seguimiento post aprobación y validación de los softwares. Garantizando así cumplir con normativa local mencionada en BPM DIGEMID 2018. (6)

Sin embargo, solamente con el diagrama de Gantt que muestra un cronograma claro de las actividades no es posible llevar de forma adecuada las validaciones de software. El diagrama muestra que los softwares de equipos analíticos han sido divididos en tres grupos según su prioridad: Baja, Mediana y Alta prioridad.

Según esta prioridad se establece que tan urgente y por ende en que parte del cronograma se colocará la realización del URS, Análisis de Riesgo, IQ, OQ, PQ y finalmente la aprobación.

Para poder establecer la prioridad se generó una tabla (ver Anexo 2) con los equipos analíticos del área de control de calidad y su clasificación. Esta clasificación es en base a GAMP 5 y la USP. La clasificación de los equipos es en base a si es que cuentan o no cuentan con software, la complejidad del software, si el equipo analítico está vinculado a un sistema computarizado complejo como LIMS y si es que se requiere realizar una calibración y/o verificación del equipo analítico cuando se vaya a utilizar. (5,12)

Tanto lo mostrado en la Tabla 1 y el Anexo 2 permitieron identificar y clasificar de forma adecuada los equipos analíticos y sus softwares dentro del área de control de calidad del laboratorio.

Tabla 1: Clasificación de Equipos según USP <1058> y GAMP 5

Grupo General	Descripción	Grupo Específico	Descripción
A	El grupo A contiene a los instrumentos y equipos simples que no miden parámetros físicos.	A1	Equipos que no tienen capacidad de medición.
		A2	Equipos que si tienen capacidad de medición pero sin necesidad de calibrar.
B	El grupo B contiene a los instrumentos de medición que si miden parámetros físicos y requieren una calibración o verificación	B1	Instrumentos con firmware básico y que no son programables.
		B2	Son equipos que contienen cálculos.
		B3	Similar al B2 pero pueden ser configurados.
		C1	Contiene software que

C	Equipos con sistemas computarizados que tienen tanto hardware como software.		no puede ser personalizado.
		C2	Contiene software que permite configurar parámetros.
		C3	Contiene un software muy personalizado. Hecho a la "medida" del usuario.

Si hacemos una comparación de la forma de clasificar los equipos analíticos de este PMV versus el PMV de Shiv Kumar. Notaremos que por más que su clasificación es bastante sólida al usar GAMP 5 como referencia, no menciona el capítulo <1058> de la USP. Carece de una integración de diversas fuentes normativas para poder agregar robustez y confiabilidad a su trabajo. (13)

Para poder tener una estrategia efectiva no solo es necesario tener un cronograma bien definido y una tabla que muestre de forma clara que softwares de que equipos analíticos van a tomarse en cuenta en el PMV, también, es necesario delimitar de forma clara y concisa los cargos y las funciones que cada persona que forma parte del comité de validación contemplado en este PMV va a tener y realizar.

El trabajo de suficiencia profesional de SUAREZ VILLAR donde se realizó un PMV contó con un organigrama donde se muestra las distintas áreas de la empresa y los empleados de cada área que forman parte en el PMV.(9) Sumado a ello, se describen detalladamente los roles y las actividades que cada uno cumple en el PMV.

Con la información contemplada en los Anexos 5 y 6 se tiene una idea clara de los cargos que van a participar del PMV como también sus roles en cada actividad. Esto resulta en

una forma organizada, concisa y bien dirigida de llevar a cabo el PMV pudiendo entonces lograr de forma eficiente y dentro del cronograma estipulado todas las actividades propuestas.

La elaboración de una guía pertinente para elaborar un URS y un análisis de riesgo que a su vez permitan luego la implementación de protocolos y reportes de IQ, OQ y PQ sólidos en contenido y confiabilidad se logró al tomar en cuenta las consideraciones de CFR 21 Parte 11, GAMP 5 y BPM DIGEMID 2018.

Esto, sumado a la revisión de trabajos de suficiencia previos que incluían dichos documentos, permitió la generación de una guía competente y concisa para elaborar un URS adecuado (ver Anexo 3).

La fase que sigue luego de la redacción, revisión y aprobación del URS es entonces el análisis de riesgo. En esta etapa se evalúa el riesgo que supone cada software ligado al equipo utilizando el NPR (Número de Prioridad de Riesgo). La forma calcular el NPR y la criticidad del riesgo está explicada en el Anexo 7.

PARDO FIERRO describe de forma breve una matriz de trazabilidad en su documento de "Validación de Sistemas Computarizados".(10) Sin embargo, se necesita algo más conciso ara el cumplimiento tanto de CFR 21 Parte 11. Se tomaron en cuenta los artículos 11.10 (controles para sistemas cerrados), 11.50 (manifestaciones de firmas), 11.70 (vinculación firma/registro), 11.100 (requisitos generales para firmas electrónicas), 11.200 (componentes y controles de la firma electrónica) y 11.300 (controles para códigos de identificación/contraseñas). Para poder hacer seguimiento y trazabilidad del cumplimiento de estos parámetros se implementó una matriz (ver Anexo 4) el cual debe ser revisado y verificado para poder corroborar que todos los ítems estén completos de

forma satisfactoria. Está especificado que para poder aprobar IQ, OQ y PQ dicha matriz debe estar completa y conforme en todos los ítems.

Adicionalmente a la matriz de CFR 21 Parte 11 se establecieron los criterios de aceptación para cada uno de los documentos a elaborar en la validación. Estos criterios de aceptación se muestran en el Anexo 9.

Para poder tener un entendimiento de todo el proceso de validación desde el URS hasta la baja del sistema es necesario establecer un ciclo de vida del sistema que contemple cambios que se requieren hacer conforme las normativas cambien o se modifiquen y el sistema deba ser configurado para cumplir con ellas. El Anexo 8 muestra un ciclo de vida que incluye el flujo para realizar controles de cambio y la baja de un sistema que queda obsoleto frente a nuevos requerimientos normativos.

Dicho PMV tiene componentes similares a otras validaciones investigadas como parte de la literatura de este trabajo ya que, esos trabajos de validación también están enfocados fuertemente en el cumplimiento de CFR 21 Parte 11. Sin embargo, la implementación del checklist que contempla tanto CFR 21 Parte 11 hacen que el presente trabajo sea más completo y robusto al abarcar normativas adicionales que permiten que el PMV a futuro pueda tener una validez que abarca una mayor cantidad de países y entes regulatorios a través del mundo. (11,14)

Para las guías generalizadas de los Protocolos y Reportes de IQ, OQ, PQ se señalaron puntos similares a otros trabajos que contemplan CFR 21 Parte 11. Sobre todo, que al finalizar cada etapa se cuenten con pruebas tangibles del cumplimiento de cada punto a cumplir. Este PMV solicita que las pruebas se presenten en un documento PDF con capturas de pantalla y/o vídeos que muestren de forma conclusiva que el software que

está siendo validado permita realizar las acciones deseadas y a su vez cumplan con las normas de los entes regulatorios contemplados en este trabajo de suficiencia. Los criterios de aceptación del Anexo 9 mencionados anteriormente sirven como una guía primordial para confirmar que URS, Análisis de Riesgo, IQ, OQ y PQ estén conformes y sean aprobados.

Todo lo deliberado anteriormente resulta entonces en un PMV sólido, robusto, confiable y en cumplimiento de CFR 21 Parte 11, BPM DIGEMID 2017 y GAMP 5.

V. CONCLUSIONES

1. Se realizó la satisfactoriamente la implementación de un PMV para Software de Equipos Analíticos de Control de Calidad en un laboratorio Farmacéutico con enfoque en CFR 21 Parte 11.

2. Se establecieron requisitos regulatorios según CFR 21 Parte 11, Manual de BPM DIGEMID 2018 y GAMP 5.

3. Se identificaron y clasificaron los equipos analíticos con sus softwares según su criticidad de una forma que permita tener una estrategia efectiva para realizar las validaciones dentro de un rango de tiempo deseado.

4. Se pudo definir una estrategia para validar los softwares de equipos analíticos.

5. Es necesario tener un monitoreo constante de los softwares porque no son infalibles y los principios de CFR 21 Parte 11 están en evolución constante.

6. Revisar de forma periódica el audit trail de los softwares para asegurar que los controles de acceso y acciones por rol de usuario estén funcionando adecuadamente.

7. Es vital capacitar de forma adecuada al personal que usará los softwares para que no se tengan problemas de integridad de datos por el uso inadecuado de los softwares.

VI. BIBLIOGRAFÍA

1. Charoo NA, Khan MA, Rahman Z. Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. Int J Pharm. enero de 2023;631:122503. doi:10.1016/j.ijpharm.2022.122503

2. FDA. Part 11 Electronic Records, Electronic Signatures [Internet]. 2026. Disponible en: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11#11.30

3. FDA. General Principles of Software Validation [Internet]. 2002. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.fda.gov/media/73141/download

4. Pedro F, Veiga F, Mascarenhas-Melo F. Impact of GAMP 5, data integrity and QbD on quality assurance in the pharmaceutical industry: How obvious is it? Drug Discov Today. noviembre de 2023;28(11):103759. doi:10.1016/j.drudis.2023.103759

5. ISPE. GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems [Internet]. 2a ed. 2022. Disponible en: https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition

6. DIGEMID. Manual de Buenas Prácticas de Manufactura de Productos Farmacéuticos. 2018.

7. Raja JR, Kella A, Narayanasamy D. The Essential Guide to Computer System Validation in the Pharmaceutical Industry. Cureus. 23 de agosto de 2024. doi:10.7759/cureus.67555

8. PIC/S Secretariat. GUIDE TO GOOD MANUFACTURING PRACTICE FOR MEDICINAL PRODUCTS ANNEXES [Internet]. Ginebra; 2023 [citado 29 de abril de 2026]. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://picscheme.org/docview/8881

9. Marco Alberto Suarez Villar. Plan maestro de validación para los procesos críticos de las buenas prácticas de almacenamiento, distribución y transporte. Universidad Nacional Mayor de San Marcos; 2025.

10. William Pardo Fierro. Validación de Sistemas Computarizados [Internet]. Ecuador: Empresa Expercontri S.A.; 2021 [citado 29 de abril de 2026]. Disponible en: https://es.scribd.com/document/499841484/QPD8-Plan-Maestro-de-Validacion-de-Sistemas-V2-Expercontri123

11. Portier Noriega SG. Validación del software LabX integrado a un espectrofotómetro UV-Vis para asegurar la integridad de datos en un laboratorio farmacéutico en Lima, Perú. 2025.

12. USP. USP-NF 2026 Chapter <1058> Analytical Instrument Qualification. Estados Unidos; 2025.

13. Shiv Kumar. Computer System Validation Master Plan. 2020.

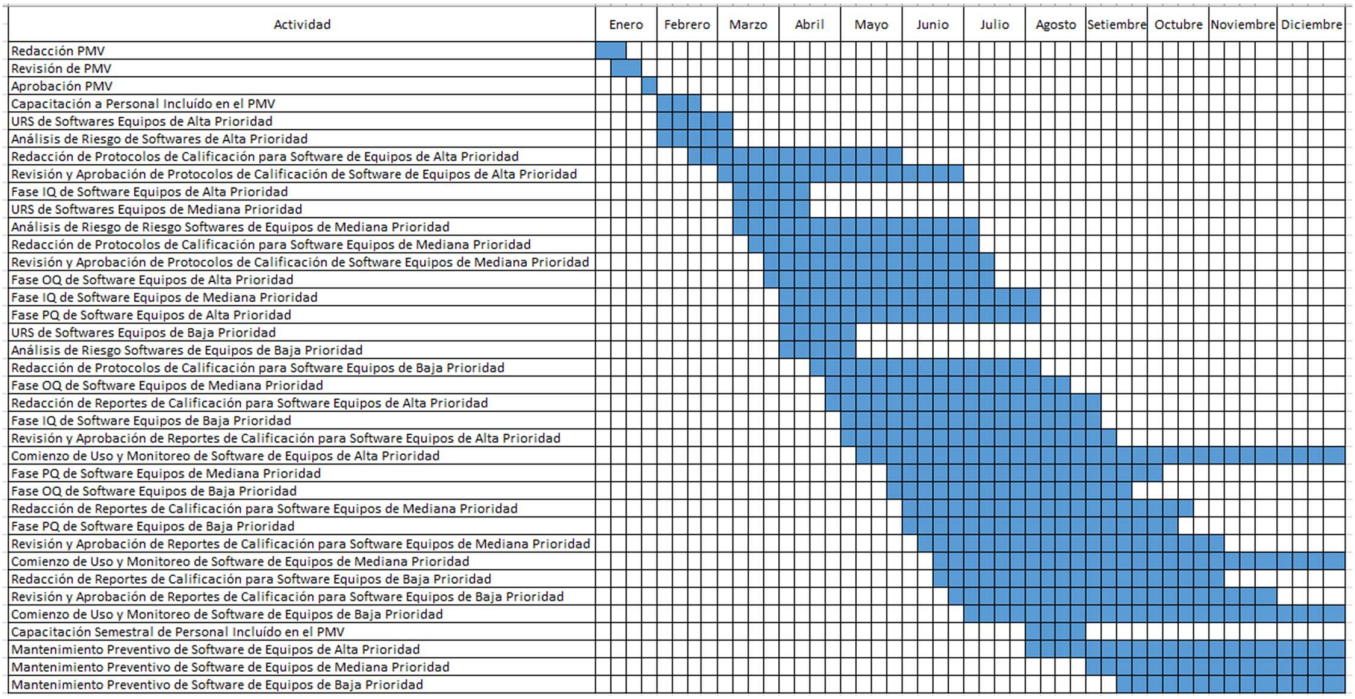
14. Fuenzalida Leal PA. Implementación de validación de sistema computarizado en software de control de espectrofotómetro UV para cumplimiento con normativa CFR21 en laboratorio de desarrollo analítico para Synthon Chile Ltda. [Internet]. Universidad de Chile; [citado 11 de marzo de 2026]. Disponible en: https://repositorio.uchile.cl/handle/2250/185544 doi:10.58011/6FGV-V358

15. Elser C, Richmond FJ. Validation Master Plans: Progress of Implementation in the Pharmaceutical Industry. Ther Innov Regul Sci. mayo de 2019;53(3):354-63. doi:10.1177/2168479018784910

16. EMA. Guideline on computerised systems and electronic data in clinical trials [Internet]. 2023 [citado 14 de mayo de 2026]. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf

ANEXOS

Anexo 1: Diagrama de Gantt para PMV



Anexo 2: Tabla de Inventario de Equipos Analíticos

Equipo	Modelo	Marca	Código	Ubicación	Software y Versión	Proveedor	Clasificación	Requiere CFR 21 Parte 11		Criticidad	Validado (SI/NO)
								SI	NO		
Titulador Karl Fischer	899 Coulemeter	Metrohm	QC-014	FQ-3	TiamoTM 3.0	QSI	C1	X		Mediana	SI
Estufa al Vacío	Memmert	VO200	QC-015	FQ-3	AtmoCONTROL FDA Edition 3.7	Kossodo	C1	X		Mediana	SI
Polarímetro	MCP 150	Anton Paar	QC-017	FQ-3	AP Connect 2.5	QSI	C1	X		Mediana	SI
Espectrofotómetro IR	Spectrum Two FT-IR	PerkinElmer	QC-018	FQ-3	Spectrum ES IR 10.7	Científica Andina	C1	X		Mediana	SI
Microbalanza	XPR2U	Mettler Toledo	QC-019	Sala de Balanzas	LabX Balance 2022.1	Científica Andina	B2	X		Baja	SI
Balanza	XPR205DR	Mettler Toledo	QC-020	Sala de Balanzas	LabX Balance 2022.1	Científica Andina	B2	X		Baja	SI
Balanza	XPR205DR	Mettler Toledo	QC-021	Sala de Balanzas	LabX Balance 2022.1	Científica Andina	B2	X		Baja	SI
Balanza	XPR205DR	Mettler Toledo	QC-022	Sala de Balanzas	LabX Balance 2022.1	Científica Andina	B2	X		Baja	SI
Balanza	XPR205DR	Mettler Toledo	QC-023	Sala de Balanzas	LabX Balance 2022.1	Científica Andina	B2	X		Baja	SI
Balanza	XPR205DR	Mettler Toledo	QC-024	Sala de Balanzas	LabX Balance 2022.1	Científica Andina	B2	X		Baja	SI
HPLC	Alliance e2695	Waters	QC-025	Sala de HPLCs	Empower 3 FR5 2022	Científica Andina	C2	X		Alta	SI
HPLC	Arc HPLC	Waters	QC-026	Sala de HPLCs	Empower 3 FR5 2022	Científica Andina	C2	X		Alta	SI
HPLC	1260 Infinity II	Agilent	QC-027	Sala de HPLCs	Empower 3 FR5 2022	Científica Andina	C2	X		Alta	SI
HPLC	Nexera X2	Shimadzu	QC-028	Sala de HPLCs	Empower 3 FR5 2022	Científica Andina	C2	X		Alta	SI
GC	8890 GC	Agilent	QC-029	Sala de HPLCs	OpenLab CDS 2.7	QSI	C2	X		Alta	SI
Titulador Automático	905 Titrando	Metrohm	QC-030	FQ-2	TiamoTM 3.0	Científica Andina	C1	X		Mediana	SI
Potenciómetro	SevenExcellence S500	Mettler Toledo	QC-031	FQ-2	LabX pH	QSI	B2	X		Baja	SI
Potenciómetro	SevenExcellence S500	Mettler Toledo	QC-032	FQ-3	LabX pH	QSI	B2	X		Baja	SI
Espectrofotómetro UV/VIS	Cary 3500	Agilent	QC-033	FQ-2	Cary UV Workstation 2.1	EQUANTI	C1	X		Mediana	SI

Anexo 3: URS

URS

El URS es una actividad crítica en el proceso de la validación del software del equipo analítico, ya que, se definen los requisitos que deben tener tanto el software como el equipo analítico al cual estará integrado. Se debe tomar el URS como la base de todo. Si el URS se realiza de forma errónea entonces, los siguientes pasos posteriores al URS serán incorrectos y por ende la validación no será aprobada.

Entonces es importante que el URS cuente con lo siguiente para que sea redactado de forma coherente:

Los requisitos del Equipo Analítico, tales como:

- Especificaciones de Equipo: Modelo deseado con sus dimensiones y peso exacto, voltaje y amperaje necesario para funcionamiento, rango de lectura (si es necesario), precisión del equipo e interfaz con software Todos justificados debidamente.
- Especificaciones del Software: Nombre y versión deseada, firmas electrónicas, control de firmas, roles de usuarios, audit trail, generación de reportes con fecha, hora y firma, impresión de datos con fecha, hora y firma, sistema de backup, registro de datos, cálculos (si es necesario), ecuaciones (si es necesario) e interfaz con el equipo analítico.
  Todos justificados debidamente.

Anexo 4: Matriz de Cumplimiento de CFR 21 Parte 11

Requisito	SI	N.A	Control Implementado	Evidencia Documentaria	Estado (Cumple/ N.A)
La data está encriptada			Software que permita tener datos encriptados almacenados en la PC vinculada al software y al equipo analítico	En especificaciones técnicas del software y evidencia en IQ.	
Es posible discernir entre registros inválidos o alterados			Software que cuenta con audit trail que permite ver todas las actividades realizadas por cada usuario que ingresó al software	Secuencia de capturas de pantalla que muestran a un usuario modificando algo y luego secuencia de capturas de pantalla que muestran ingreso al audit trail donde se evidencia las actividades que realizó dicho usuario y si datos ingresados son inválidos o están fuera del rango. Toda esta evidencia adjunta al OQ. POE de Integridad de Datos.	
El acceso al sistema está limitado a personal autorizado			Software que cuenta con usuarios con propia cuenta y contraseña y roles designados	Evidencia en OQ con capturas de pantalla donde se muestran los usuarios y sus roles en el software. Además, una	

				tabla donde se muestre los permisos que cada rol tiene. POE de Gestión de Usuarios.	
Se usan firmas digitales			Software que permita habilitar el uso de firmas digitales para cada actividad que realice un usuario dentro de este	Evidencia en OQ y PQ de un usuario requerido de poner firma digital para realizar una actividad y que luego la firma se pueda visualizar en el audit trail. POE de firmas digitales.	
Hay capacitación para el personal			Contemplado en el Diagrama de Gantt de PMV.	Registros de capacitaciones y registros de evaluaciones dadas como prueba para evaluar competencia del personal	
Se tiene un tiempo máximo determinado para la duración de las contraseñas			Configurar duración de clave en software.	Evidencia con captura de pantalla donde se ingresa duración predeterminada de clave y adjuntar a OQ. POE de Gestión de Contraseñas.	
Existe un sistema seguro, generado por computadora, con fecha y hora de audit trail que registra la fecha, hora, usuario y actividad realizada			Software con opción de habilitar audit trail.	Evidencia con captura de pantalla de historial de audit trail donde se muestra registro de firmas por usuarios. Adjuntar a OQ.	

Si se realiza un cambio a una información previamente registrada se permite ver la información original			Software que cuenta con audit trail que permite ver las todas las actividades realizadas por cada usuario que ingresó al software.	Evidencia con captura de pantalla que muestra ingreso de usuario que modifica información original y luego con rol de administrador se visualiza el historial de audit trail donde se evidencia con usuario, su firma, fecha y hora y modificación realizada. Adjuntar evidencia al OQ.	
El audit trail permite visualizar toda las actividades del usuario incluyendo cambio de clave y/o rol de usuario			Configurar audit trail para que historial permita ver cambio de clave y/o rol de usuario.	Capturas de pantalla evidenciando esas actividades y luego revisión en historial de audit trail donde se muestra que la actividad se realizó. Adjuntar evidencia al OQ. POE de Revisión de Audit Trail.	
Los registros electrónicos firmados deberán contener información relacionada con la firma que indique claramente todos los siguientes elementos: El nombre completo del firmante; La fecha y la hora en que se realizó la firma; y			El software genera registros electrónicos que contiene nombre completo del usuario y su rol, fecha y hora que se realizó firma y actividad que se realizó.	Captura de pantalla que evidencia pedida de firma electrónica por cada acción realizada y su posterior visualización en el registro de audit trail. Evidencia	

El significado (como revisión, aprobación, responsabilidad o autoría) asociado a la firma.				adjunta al OQ y PQ.	
Si se imprime algo se visualiza también el flujo de firmas con los nombres de usuarios, fecha y hora			Configurar en software que a la hora de generar reportes e imprimirlos se pida firma electrónica.	Reportes impresos y archivo PDF con historial de firmas al final. Esto adjunto como evidencia para PQ.	
Las firmas electrónicas y las firmas manuscritas que se apliquen a registros electrónicos deben vincularse a sus respectivos registros electrónicos para garantizar que las firmas no puedan ser eliminadas, copiadas ni transferidas de ningún otro modo con el fin de falsificar un registro electrónico por medios ordinarios.			Vinculación de forma permanente entre firma y registro electrónico.	Evidencia en OQ y PQ y documentación de proveedor.	
El software no permite que se puedan editar las firmas, fechas y horas			Software restringe las modificaciones de firmas, fechas y horas.	Evidencia en OQ al mostrar configuración de software que niega la alteración de firmas, fechas y horas.	
La identidad del usuario es verificada antes de realizar una firma			Software pide identificación del usuario y su contraseña antes de firmar.	Evidencia de esto mediante captura de pantalla que pide usuario y contraseña antes de firmar por realizar alguna actividad en el software. Adjuntar en OQ y PQ. POE de	

				Firmas Electrónicas.	
El sistema usa un sistema establecido automático de conversión o métodos de exportación como Excel o PDF			Software cuenta con función de exportación para tipo Excel y PDF. PC que usa el software cuenta con ambos programas.	Evidencia de archivos generados al exportar datos. Uso de secuencia de capturas de pantalla como evidencia para OQ y PQ.	
El sistema no permite borrar data			Software cuenta con restricción de eliminación de datos y registros.	Evidencia en OQ al mostrar configuración de permisos que no permita eliminación de datos y registros.	
El sistema no permite modificar parámetros de un ensayo durante el mismo			La configuración del software bloquea la modificación de parámetros durante la ejecución de un ensayo.	Evidencia en OQ y PQ al mostrar configuración de permisos que no permita modificar parámetros de un ensayo durante su ejecución.	
Hay sistemas de validación para garantizar la precisión, confiabilidad y consistencia de la performance esperada y además la capacidad para discernir registros inválidos o alterados			Ejecución del ciclo de vida del software con los documentos relevante (URS, RA, IQ, OQ, PQ).	Documentos de PMV, URS, RA, IQ, OQ y PQ como evidencia.	
Se puede generar copias de registros precisas y completas tanto en forma física legible y electrónica adecuado para ser inspeccionado, revisado y copiado por la entidad			Software con función de impresión validada para generar copias precisas y completas en papel de los	Evidenciar en PQ mediante un reporte impreso y compararlo con capturas de pantallas de documento PDF que se imprimió para corroborar	

			registros electrónicos.	precisión. POE de Exportación de Registros.	
Existe protección de los registros que permite su recuperación precisa y rápida durante el periodo de conservación de los mismos			Sistemas de backup automatizados y recuperación de información.	Mostrar carpeta y registros de backup como evidencia para OQ. POE de Backup y Recuperación.	
Uso de comprobaciones del sistema operativo para garantizar la secuencia permitida de pasos y eventos según corresponda			Flujos de trabajo controlados mediante permisos y secuencias configuradas.	Flujos de trabajo controlados mediante permisos y secuencias configuradas.	
Uso de dispositivos que permite comprobar, según corresponda, la validez de la fuente de datos introducidos o de las instrucciones operativas			Validaciones automáticas de entrada de datos y control de dispositivos autorizados.	Validaciones automáticas de entrada de datos y control de dispositivos autorizados.	
Se determinará que las personas que desarrollan, mantienen o utilizan sistemas de registros electrónicos y firmas electrónicas cuenten con la formación, la capacitación y la experiencia necesarias para desempeñar las			Programa de capacitación contemplado en diagrama de Gantt y evaluación después de cada capacitación para medir conocimiento de personal.	Registro de asistencia a capacitaciones, registro de toma de evaluación de capacitación y registro de notas del personal para evaluar que personal	

tareas que se les asignen.				cumple con el perfil deseado.	
El establecimiento y el cumplimiento de políticas escritas que exijan a las personas rendir cuentas y asumir la responsabilidad de las acciones realizadas mediante sus firmas electrónicas, con el fin de disuadir la falsificación de registros y firmas.			Política corporativa instaurada para las firmas y las responsabilidades que consigna tener una.	Evidencia de documento corporativo respecto a la política de firmas electrónicas. POE de Seguridad Informática.	
Uso de controles adecuados sobre la documentación de los sistemas, lo que incluye: 1) Controles adecuados sobre la distribución, el acceso y el uso de la documentación para el funcionamiento y el mantenimiento de los sistemas.			Gestión de control de documentos con el uso de software donde se guardan los documentos con el código, versión, fecha de la última versión, y finalmente con acceso restringido que varía según usuario y sus roles.	Documento corporativo sobre control documentario. POE de Control Documental.	
2) Procedimientos de control de revisiones y cambios para mantener un registro de auditoría que documente, en orden cronológico, el desarrollo y la modificación de la documentación de los sistemas.			Gestión de control de documentos con software que muestra flujo de usuarios que modifican, revisan y aprueban documentos con registro de hora y fecha de cada acción realizada por casa usuario.	Documento corporativo sobre control documentario e historial de revisiones.	
Cada firma electrónica es exclusiva de una persona y no podrá ser			Asignación individual de	Documento corporativo	

reutilizada ni reasignada a ninguna otra persona.			credenciales y prohibición de compartir usuarios.	sobre gestión de usuarios y documento con matriz de usuarios autorizados. POE de Gestión de Usuarios.	
Antes de que la organización establezca, asigne, certifique o apruebe de cualquier otra forma la firma electrónica de una persona, o cualquier elemento de dicha firma electrónica, la organización deberá verificar la identidad de dicha persona.			Procedimiento para verificar y autorizar usuarios a personal.	Documento que contiene registro con nombre de personal, su usuario, su rol, fecha de aprobación de firma y firma de supervisor que autoriza que obtenga firma. POE de Gestión de Usuarios.	
Las personas que utilicen firmas electrónicas deberán certificar ante el organismo, antes o en el momento de dicho uso, que las firmas electrónicas de su sistema, utilizadas a partir del 20 de agosto de 1997, tienen por objeto ser el equivalente legalmente vinculante de las firmas manuscritas tradicionales.			Declaración formal de aceptación de firma electrónica.	Declaración firmada por el personal que acepta la firma electrónica.	

La certificación deberá firmarse con una firma manuscrita tradicional y presentarse en formato electrónico o en papel.			Procedimiento documentado para emisión y archivo de certificaciones.	Certificación archivada.	
Las personas que utilicen firmas electrónicas deberán, a petición de la autoridad competente, presentar una certificación o un testimonio adicional que acredite que una firma electrónica concreta tiene el mismo valor legal que la firma manuscrita del firmante.			Procedimiento que acredite firma electrónica tiene mismo valor legal que la firma manuscrita del firmante.	Documento corporativo para generar certificado que acredite la firma electrónica de forma competente para auditorías e inspecciones. POE de Inspecciones y Auditorías.	
Las firmas electrónicas que no se basen en datos biométricos deberán: 1) Utilizar al menos dos elementos de identificación distintos, como un código de identificación y una contraseña.			Autenticación mediante usuario único y contraseña única.	Configuración del sistema. Adjuntar evidencia en OQ.	
2) Cuando una persona realice una serie de firmas durante un único período continuo de acceso controlado al sistema, la primera firma deberá realizarse utilizando todos los componentes			Configuración de firma electrónica conforme al flujo del sistema.	Adjuntar capturas de pantalla que muestran que el inicio de sesión y las firmas posteriores requieren tanto usuario como contraseña como evidencia para OQ y PQ.	

de la firma electrónica; las firmas posteriores deberán realizarse utilizando al menos un componente de la firma electrónica que solo pueda ser ejecutado por dicha persona y que esté diseñado para ser utilizado exclusivamente por ella.					
3) Cuando una persona realice una o más firmas que no se hayan efectuado durante un único período continuo de acceso controlado al sistema, cada firma deberá realizarse utilizando todos los componentes de la firma electrónica.			Re autenticación obligatoria para cada firma fuera de sesión activa.	Evidencia con capturas de pantalla para OQ y PQ mostrando que sistema vuelve a pedir firma electrónica para poder reiniciar sesión y continuar.	
4) Ser utilizadas únicamente por sus legítimos propietarios			Política corporativa que exige uso individual de usuarios y contraseñas.	Documento corporativo sobre política de seguridad informática, usuarios y contraseñas y auditorías.	
5) Se aplicará y ejecutará de manera que cualquier intento de utilizar la firma electrónica			Controles de autenticación y segregación de funciones que previenen el uso	Procedimientos de seguridad, configuración del sistema.	

de una persona por parte de alguien que no sea su verdadero titular requiera la colaboración de dos o más personas.			indebido de credenciales.		
Las firmas electrónicas basadas en datos biométricos deberán diseñarse de tal manera que se garantice que solo puedan ser utilizadas por sus legítimos titulares.			Implementación de autenticación biométrica exclusiva para el usuario autorizado.	Especificación técnica del sistema biométrico, evidencia OQ.	
Las personas que utilicen firmas electrónicas basadas en el uso de códigos de identificación combinados con contraseñas deberán aplicar controles para garantizar su seguridad e integridad. Dichos controles deberán incluir: 1) Garantizar la unicidad de cada combinación de código de identificación y contraseña, de modo que no haya dos personas con la misma combinación de código de identificación y contraseña.			Generación y administración de usuarios únicos.	POE de Gestión de Usuarios adjuntar evidencia a OQ.	
2) Asegurarse de que la asignación de códigos de identificación y contraseñas se compruebe, se			Política corporativa sobre expiración y renovación periódica de contraseñas.	POE de contraseñas y usuarios.	

	revise o se actualice periódicamente (por ejemplo, para tener en cuenta situaciones como la caducidad de las contraseñas).					
3)	Seguir los procedimientos de gestión de pérdidas para desactivar electrónicamente los tokens, tarjetas y otros dispositivos que contengan o generen códigos de identificación o contraseñas, y que hayan sido objeto de pérdida, robo, extravío o cualquier otra situación que pueda comprometer su seguridad, así como para emitir sustitutos temporales o permanentes mediante controles adecuados y rigurosos.			Proceso para el bloqueo y reemplazo de credenciales comprometidas.	POE de Gestión de Incidentes donde se incluya registro de bloqueos.	
4)	Utilización de medidas de seguridad en las transacciones para evitar el uso no autorizado de contraseñas y/o códigos de			Bloqueo por intentos fallidos, monitoreo de accesos y alertas de seguridad.	Configuración del sistema, registros de eventos de seguridad. Adjuntar capturas de pantalla que muestran	

identificación, así como para detectar y notificar de manera inmediata y urgente cualquier intento de uso no autorizado a la unidad de seguridad del sistema y, según corresponda, a la dirección de la organización.				bloqueo por intentos fallidos en OQ.	
5) Pruebas iniciales y periódicas de dispositivos, como tokens o tarjetas, que contienen o generan códigos de identificación o contraseñas, con el fin de garantizar que funcionan correctamente y que no han sido modificados de forma no autorizada.			Verificación periódica del correcto funcionamiento de los mecanismos de autenticación.	Registros de mantenimiento y pruebas.	

Anexo 5: Comité de Validación

Funciones en Base al Cargo

Cargo	Funciones	Responsabilidad Documental
Gerente de Control de Calidad	Asegurar que el personal adecuado asuma cada rol delimitado en el PMV. Asegurar la disponibilidad de los recursos requeridos. Aprobación definitiva de Documentos de Validación y responsable final de todo el proceso de validación.	Encargado de dar la aprobación final del PMV y luego la aprobación del Reporte Final que engloba los documentos de IQ, OQ y PQ.
Supervisor de Control de Calidad	Revisión y supervisión de Documentos de Validación Aprobación de Documentos de Validación Supervisar la labor de los analistas de validación. Realizar un seguimiento constante que asegure que las técnicas de ejecución, redacción, documentación, requisitos regulatorios, gestión de desvíos, controles de cambios e implementación de acciones correctivas y preventivas sean las adecuadas. Coordinar la capacitación y evaluación del personal involucrado en todo el proceso de validación.	PMV, URS, Análisis de Riesgos, IQ, OQ, PQ, Matriz CFR 21 Part 11, Reporte Final
Analista de Control de Calidad	Redacción de Documentos de Validación Realizar las actividades y pruebas y registrar la evidencia de forma adecuada. Implementar controles de cambio	PMV, URS, Análisis de Riesgos, IQ, OQ, PQ, Matriz CFR 21 Part 11, Reporte Final

Gerente de Ingeniería y Mantenimiento	Seleccionar al personal adecuado para realizar las mediciones Supervisar y aprobar las mediciones realizadas por los ingenieros de su área.	URS, IQ
Analista de Ingeniería y Mantenimiento	Realizar las mediciones pertinentes que indica el reporte de validación de software (IQ principalmente).	IQ
Aseguramiento de la Calidad	Verificar el cumplimiento regulatorio de todos los documentos y consecuentemente aprobarlos.	Todos los documentos relacionados a validación
Usuario Propietario (System Owner)	Definir los requerimientos y verificar que el software cumpla con las necesidades de la empresa/negocio.	Da soporte funcional en elaboración de URS en base a los requerimientos de la empresa/negocio
Proveedor	Suministrar documentación técnica y brindar soporte especializado.	Dependiendo del apoyo y documentación requerida pueden estar involucrados en todos los documentos pero solo en el ámbito de enviar documentos y evidencia y más adelante en los mantenimientos preventivos y las verificaciones operacionales.
Analista de IT	Revisar que el software esté instalado de forma adecuada. Revisar que los permisos de la PC estén conformes Aprobar los ítems relacionados a IT Verificar que los permisos de la PC y el sistema operativo estén actualizados y en línea para el correcto funcionamiento del software.	Da soporte funcional en elaboración de URS en temas de sistema operativo óptimo y marca y modelo de PC. Apoya en temas técnicos de IT que están en su mayoría en el IQ.

Anexo 6: Matriz de Ejecución, Elaboración, Revisión y Aprobación

Ítem	Analista QC	Supervisor QC	Gerente QC	Gerente de Ingeniería y Mantenimiento	Analista de Ingeniería y Mantenimiento	Gerente QA	Analista IT
PMV	E, R	RV	A	RV	-	RV, A	RV
URS	E, R	RV	A	RV	-	RV, A	RV
AR	E, R	RV	A	-	-	RV, A	-
IQ	E, R	RV	A	RV	E	RV, A	E
OQ	E, R	RV	A	RV	E	RV, A	E
PQ	E, R	RV	A	-	E	RV, A	E
Matriz CFR 21 Parte 11	E, R	RV	A	-	-	RV, A	-
Reporte Final	E, R	RV	A	RV	-	RV, A	RV

E: Ejecución de pruebas y/o mediciones

R: Redacción

RV: Revisión

A: Aprobación

Anexo 7: Análisis de Riesgo Y Escala de Riesgos por Equipo y Sistema

Es vital tener un análisis de riesgo que se haga anteriormente a la implementación de un software vinculado a un equipo analítico. Esto para poder identificar los posibles riesgos, el posible daño que puede causar y la forma en la que pueden ser reducidos o mitigados. Al tener un conocimiento más profundo de estos riesgos hay una mayor probabilidad de poder prevenirlos o, en todo caso, saber cómo lidiar con dichos riesgos si es que llegan a suceder.

El cálculo del riesgo se basa en tres factores: Severidad (S), Ocurrencia (O) y Detectabilidad (D).

Severidad es la gravedad e impacto que tiene el riesgo si es que llega a suceder en la calidad, integridad, confiabilidad del producto farmacéutico y en BPx.

Ocurrencia es la probabilidad que el riesgo pueda ocurrir. A mayor ocurrencia mayor probabilidad que suceda el riesgo.

Detectabilidad se refiere a la capacidad para poder detectar este riesgo antes que cause un impacto. Normalmente va depender de las herramientas y metodologías que se tienen para gestionar la trazabilidad de los procesos. Si se tienen buenas herramientas de trazabilidad hay una mayor probabilidad de poder detectar cuando y en que parte del proceso sucedió el riesgo.

A continuación, se presenta la categorización en forma numérica de cada uno de los tres factores. Siendo el rango de uno a cinco. Siendo uno el menor riesgo y cinco el máximo.

Severidad (S)

Valor	Descripción
1	Sin impacto en las BPx
2	Impacto menor en calidad, integridad o confiabilidad o BPx
3	Impacto moderado en calidad, integridad o confiabilidad o BPx
4	Impacto significativo en calidad, integridad o confiabilidad o BPx
5	Impacto crítico en calidad, integridad, confiabilidad, seguridad del paciente o BPx

Ocurrencia (O)

Valor	**Descripción**
1	Muy improbable casi inexistente
2	Probabilidad baja
3	Probabilidad moderada
4	Probabilidad alta
5	Probabilidad muy alta

Detectabilidad (D)

Valor	**Descripción**
1	Fácilmente detectable
2	Detectable mediante controles rutinarios
3	Detectabilidad moderada con uso de controles avanzados de detección (herramientas de seguridad mejorada (ES))
4	Detectabilidad difícil incluso con controles avanzados
5	Detectabilidad muy difícil o imposible de detectar antes del impacto

Ahora que se tiene el valor numérico de cada factor se puede clasificar el riesgo de forma numérica con el Número de Prioridad de Riesgo (NPR). Este NPR se obtiene multiplicando los tres factores. Entonces NPR = S x O x D

Como referencia se usa la siguiente tabla para calcular el NPR y por ende la criticidad/importancia del riesgo que supone. La clasificación suele ponerse tanto de forma textual como en color. El verde significando un riesgo bajo, el amarillo un riesgo medio, el naranja un riesgo alto y el rojo un riesgo muy alto y por ende crítico.

NPR	Clasificación	Prioridad
1-20	Bajo	Baja
21-50	Medio	Moderada, Mediana
51-80	Alto	Alta
81-125	Muy alto, crítico	Muy Alta

Ahora teniendo los equipos analíticos y sus softwares respectivos podemos catalogarlos con el NPR y clasificarlos según prioridad de validación.

Equipo y Modelo	Software	S	O	D	NPR	Riesgo	Prioridad de Validación
Titulador Karl Fischer 899 Coulemeter	Tiamo™ 3.0	4	3	3	36	Medio	Mediana
Estufa al Vacío Memmert	AtmoCONTROL FDA Edition 3.7	3	3	3	27	Medio	Mediana
Polarímetro MCP 150	AP Connect 2.5	4	3	3	36	Medio	Mediana
Espectrofotómetro IR Spectrum Two FT-IR	Spectrum ES IR 10.7	4	3	3	36	Medio	Mediana

Microbalanza XPR2U	LabX Balance 2022.1	2	2	2	8	Bajo	Baja
Balanza XPR205DR	LabX Balance 2022.1	2	2	2	8	Bajo	Baja
Balanza XPR205DR	LabX Balance 2022.1	2	2	2	8	Bajo	Baja
Balanza XPR205DR	LabX Balance 2022.1	2	2	2	8	Bajo	Baja
Balanza XPR205DR	LabX Balance 2022.1	2	2	2	8	Bajo	Baja
Balanza XPR205DR	LabX Balance 2022.1	2	2	2	8	Bajo	Baja
HPLC Alliance e2695	Empower 3 FR5 2022	5	3	4	60	Alto	Alta
HPLC Arc HPLC	Empower 3 FR5 2022	5	3	4	60	Alto	Alta
HPLC 1260 Infinity II	Empower 3 FR5 2022	5	3	4	60	Alto	Alta
HPLC Nexera X2	Empower 3 FR5 2022	5	3	4	60	Alto	Alta
GC 8890 GC	OpenLab CDS 2.7	5	3	4	60	Alto	Alta
Titulador Automático 905 Titrando	Tiamo™ 3.0	4	3	3	36	Medio	Mediana
Potenciómetro SevenExcellence S500	LabX pH	3	2	3	18	Bajo	Baja
Potenciómetro SevenExcellence S500	LabX pH	3	2	3	18	Bajo	Baja
Espectrofotómetro UV/VIS Cary 3500	Cary UV Workstation 2.1	4	3	3	36	Medio	Mediana

La cantidad de riesgo que conlleva usar cada equipo está ligado principalmente al nivel de complejidad de los softwares que están ligados a cada equipo. Esta clasificación de complejidad está en base a guías de clasificación por parte de GAMP5 y de USP <1058>.

Una vez identificado cada factor de riesgo se debe evaluar y proponer medidas para reducir y/o mitigar el riesgo y disminuir el NPR si es que este sobrepasa 20 (máximo para nivel considerado bajo).

Anexo 8: Ciclo de Vida de Sistemas Computarizados

El ciclo de vida muestra de una forma generalizada cada etapa por la cual pasa un sistema. Desde la concepción de requerirlo en la empresa hasta el retiro del mismo al quedar obsoleto debido a cambios en los requerimientos tanto regulatorios como ligados a integridad de datos y BPx.

Fase 1: Planificación y Evaluación Inicial

- Se define el alcance y el uso previsto del sistema.
- Identificar los requisitos regulatorios que aplican.
- Determinar el impacto que tiene en las BPx.
- Determinar el impacto que tiene en la integridad, calidad y confiabilidad de los productos.

Fase 2: Especificación de Requerimientos

- Elaboración, revisión y aprobación de URS.
- Identificar las funciones críticas del sistema que tienen impacto sobre todo en la seguridad e integridad de datos ligado a CFR 21 Parte 11.

Fase 3: Clasificación de Software Análisis de Riesgos

- Clasificar a los equipos según tipo de Software en base a GAMP 5 y USP <1058>.
- Calcular el NPR de cada software ligado a los equipos y clasificar por prioridad de validación.

Fase 4: Configuración e Implementación

- Compra del sistema.
- Instalación del sistema.
- Ajustes de parámetros del sistema según URS.

Fase 5: Validación

- Redacción, revisión y aprobación de protocolos de IQ, OQ y PQ.
- Ejecución de IQ, OQ y PQ.
- Redacción, revisión y aprobación de reportes de IQ, OQ y PQ.

Fase 6: Uso, Mantenimiento y Revisión Periódica

- Gestión de usuarios y accesos.
- Revisión periódica de Audit Trail.
- Gestión de Back up y recuperación de data.
- Capacitación de usuarios.
- Gestión de desviaciones e incidentes.
- Evaluación constante del desempeño, seguridad, cumplimiento regulatorio y mantenimiento del estado validado.

Fase 7: Control de Cambios

- Establecer un procedimiento formal (POE de Control de Cambios) para proceder de forma adecuada frente a modificaciones que afecten el estado validado del sistema.
- Evaluar el impacto que tienen las modificaciones y cambios sobre la integridad de datos, la seguridad del paciente, la calidad, la integridad de los productos y sobretodo el cumplimiento de CFR 21 Parte 11.
- Clasificar el cambio según criticidad y utilizando el cálculo de riesgo con el NPR.
- En base al NPR proponer las nuevas medidas que se necesitan para estar dentro de todos los parámetros aceptables.
- Enviar el control de cambios para que sea revisado y aprobado.
- Ejecución de pruebas de verificación o revalidación en base a las nuevas medidas estipuladas en el control de cambio.
- Redacción, revisión y aprobación de las implementaciones.
- Documentación de las implementaciones y cierre de control de cambio.

Fase 8: Retiro del Sistema

- Gestión de la descontinuación del sistema en base a evidencia que pruebe que el sistema actual ya no cumple con los requisitos estipulados por CFR 21 Parte 11 como requisitos regulatorios.
- Redacción, revisión y aprobación de documento que exige retiro del sistema.
- Conservación, migración y recuperación de los registros electrónicos y data del sistema a dar de baja.
- Retiro del sistema.
- Archivar en documentación el proceso de baja del sistema.

Anexo 9: Criterios de Aceptación para URS, Análisis de Riesgo, IQ, OQ y PQ

1. URS (Especificación de Requisitos de Usuario)

N°	Criterio de aceptación	Ítem	Sí	No	N/A
1	La URS identifica claramente el propósito y alcance del sistema.	Alcance definido			
2	Todos los requisitos funcionales se encuentran documentados.	Requisitos funcionales documentados			
3	Los requisitos regulatorios aplicables han sido incluidos.	Requisitos regulatorios incluidos			
4	Los requisitos de integridad de datos están definidos.	Integridad de datos considerada			
5	Los requisitos de seguridad y acceso están documentados.	Requisitos de seguridad definidos			
6	Los requisitos de audit trail están definidos.	Audit Trail considerado			
7	Los requisitos de firma electrónica están definidos cuando aplique.	Firma electrónica considerada			
8	Los requisitos son claros, verificables y medibles.	Requisitos verificables			
9	Existe trazabilidad entre requisitos y pruebas de validación.	Trazabilidad establecida			
10	La URS ha sido revisada y aprobada por las áreas responsables.	Documento aprobado			

2. Análisis de Riesgos

N°	Criterio de aceptación	Ítem	Sí	No	N/A
1	Se identificaron las funciones BPx críticas.	Funciones BPx identificadas			
2	Se identificaron riesgos de integridad de datos.	Riesgos identificados			
3	Se evaluó severidad de cada riesgo.	Severidad evaluada			
4	Se evaluó ocurrencia de cada riesgo.	Ocurrencia evaluada			
5	Se evaluó detectabilidad de cada riesgo.	Detectabilidad evaluada			

6	Se calculó la criticidad o NPR	NPR calculado			
7	Se definieron medidas de mitigación.	Mitigaciones definidas			
8	Los riesgos residuales fueron evaluados.	Riesgo residual evaluado			
9	No existen riesgos críticos sin mitigación.	Riesgos críticos cerrados			
10	El análisis fue revisado y aprobado.	Documento aprobado			

3. IQ (Calificación de Instalación)

N°	Criterio de aceptación	Ítem	Sí	No	N/A
1	El equipo/software corresponde al aprobado.	Modelo correcto instalado			
2	La versión instalada coincide con la especificada.	Versión correcta instalada			
3	La infraestructura cumple con requisitos técnicos.	Infraestructura verificada			
4	Los componentes fueron instalados correctamente.	Componentes instalados			
5	Las licencias son válidas.	Licencias validadas verificadas			
6	La configuración inicial fue documentada.	Configuración documentada			

7	Los usuarios administrativos fueron configurados.	Usuarios creados			
8	Los respaldos iniciales fueron configurados.	Backup configurado			
9	No existen desviaciones críticas abiertas.	Sin desviaciones críticas			
10	Toda la evidencia fue documentada.	Evidencia completa			

4. OQ (Calificación Operacional)

N°	Criterio de aceptación	Ítem	Sí	No	N/A
1	El sistema permite autenticación de usuarios.	Login validado			
2	Los permisos funcionan según los roles definidos.	Roles verificados			
3	El audit trail registra eventos correctamente.	Audit Trail validado			
4	La fecha y hora son registradas correctamente.	Fecha y hora verificadas			
5	Las firmas electrónicas funcionan correctamente.	Firma electrónica validada			

6	Los registros electrónicos son almacenados adecuadamente.	Almacenamiento validado			
7	Los datos pueden recuperarse correctamente.	Recuperación validada			
8	Las funciones críticas operan según la URS.	Funciones críticas probadas			
9	No existen desviaciones críticas abiertas.	Sin desviaciones críticas			
10	Todos los casos de prueba cumplen los criterios establecidos.	Casos de prueba aprobados			

5. PQ (Calificación de Desempeño)

N°	Criterio de aceptación	Ítem	Sí	No	N/A
1	El sistema funciona en condiciones rutinarias de uso.	Uso rutinario validado			
2	Los usuarios pueden ejecutar procesos reales.	Procesos reales ejecutados			
3	Los datos generados son completos y consistentes.	Datos consistentes			
4	Los resultados cumplen las especificaciones establecidas.	Resultados correctos			
5	Los flujos de aprobación funcionan correctamente.	Flujo de aprobación correcto			

6	Las firmas electrónicas son aplicables en operaciones reales.	Firma electrónica operativa			
7	Los reportes se generan correctamente.	Reportes generados			
8	La trazabilidad de los registros se mantiene.	Trazabilidad verificada			
9	No existen desviaciones críticas abiertas.	Sin desviaciones críticas			
10	Los usuarios aprueban el desempeño del sistema.	Aprobación de usuarios			

GLOSARIO DE TÉRMINOS

Plan Maestro de Validaciones: Es la estrategia a nivel de sitio, independiente del producto, que explica cómo su organización validará procesos, sistemas informáticos, equipos, instalaciones, servicios públicos, métodos y limpieza de forma controlada, basada en riesgos y auditable. (15)

Integridad de Datos: Se refiere a que la información se recopila, almacena y utiliza de manera segura y controlada, de manera que respalde resultados confiables y permita una toma de decisiones adecuada a lo largo de su ciclo de vida. (16)

CFR 21 Parte 11: La parte 11 del título 21 del Código de Regulaciones Federales (CFR) es regulado por la Administración de Alimentos y Medicamentos de los Estados Unidos (FDA) y establece criterios bajo los cuales registros electrónicos y firmas electrónicas son considerados confiables.(2)

GAMP 5: Las Buenas Prácticas de Manufactura Automatizada (GAMP) es una guía publicada por la Sociedad Internacional de Ingeniería Farmacéutica (ISPE) que proporciona orientación en la aplicación de los principios de gestión de riesgos al desarrollo de sistemas informáticos en industrias reguladas como la farmacéutica. (5)

POE (Procedimiento de Operativo Estándar): Según el Manual de Buenas Prácticas de Manufactura de DIGEMID, un Procedimiento Operativo Estándar (POE) es un procedimiento escrito autorizado que establece instrucciones para realizar operaciones específicas de manera uniforme y consistente.

BPx (Buenas Prácticas): Según el Manual de Buenas Prácticas de Manufactura de DIGEMID, las buenas prácticas son un término genérico para los estándares de calidad en lo que compete a la industria farmacéutica.