



SW DE DISPOSITIVOS MÉDICOS / PRODUCTO SANITARIO: CICLO DE VIDA Y VALIDACIÓN. PARTE 2.

Tal y como vimos en la parte 1 del artículo, el software de un dispositivo médico / producto sanitario debe ser implementado de una forma segura y efectiva para asegurar el uso y seguridad del producto final. Tras analizar en dicha parte el estándar IEC 62304, a continuación, echaremos un vistazo a las actividades de Verificación y Validación (V&V) dentro del proceso de desarrollo del software, así como revisaremos, la interrelación de los estándares IEC 62304 e IEC 82304-1, así como otros conceptos derivados de los nuevos retos tecnológicos a tener en consideración.



MAR DIAZ,
Responsable Técnica Validaciones Trescal Life Sciences.

Verificación y Validación

Las actividades de Verificación y Validación (V&V) son partes fundamentales del proceso de desarrollo del software para garantizar el uso y seguridad del dispositivo médico.

Mientras, la verificación se refiere a la comprobación del producto desarrollado conforme a sus requisitos especificados, la validación comprueba si se cumple su uso previsto en arreglo a las necesidades del usuario. De forma general, los términos de verificación y validación responden cada uno, a las siguientes preguntas:

- **Verificación:** ¿El diseño del dispositivo cumple los requisitos definidos?
- **Validación:** ¿Se cumplen los requisitos para el uso previsto del dispositivo? ¿Se ha diseñado el dispositivo adecuado?

A su vez, las actividades de verificación y validación en el proceso de diseño de dispositivos médicos deben estar respaldadas por un sólido plan de gestión de riesgos, en



línea con las normas ISO 14971, y cumplir con los procedimientos del sistema de gestión de calidad correspondiente (alineado con ISO 13485).

Es importante tener en consideración que dentro del ejercicio de gestión de riesgos se haya identificado el diseño más crítico o el peor caso, considerando los riesgos identificados y los resultados. Puede ser necesario

evaluar varios diseños críticos para demostrar un control efectivo de los riesgos asociados.

El nivel de formalidad de las pruebas será determinado a su vez bajo un ejercicio de gestión de riesgos.

A continuación, se muestra el diagrama en cascada de los controles de diseño de la FDA.

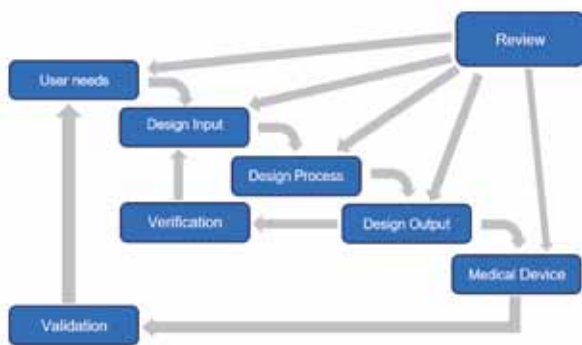


Figura 1: Aplicación de controles de diseño al proceso de diseño en cascada (fuente Guidance for Industry FDA - Design Control Guidance For Medical Device Manufacturers).

En resumen, el propósito principal de las actividades de verificación y validación de diseño es garantizar que el dispositivo se encuentra dentro de los límites del diseño especificado, y se cumplen las necesidades del usuario y de su uso previsto, dentro de un proceso controlado y trazable.

Actividades de Verificación

Las actividades de verificación se llevan a cabo en todas las etapas y niveles del diseño del dispositivo. Cualquier enfoque que establezca la conformidad con un requisito de entrada del diseño es un medio aceptable para verificar el diseño con respecto a ese requisito, en muchos casos, son posibles una variedad de enfoques. En línea con la IEC 62304, podemos distinguir diferentes niveles de verificación:

- **Ensayos de la unidad del software.** Ensayos dirigidos a verificar la implementación del diseño para cada elemento de software.
- **Ensayos de integración del software.** Ensayos que verifican la completa integración del elemento de software en el sistema software. Se trata de un proceso progresivo hasta la completa integración del sistema software. Incluye los ensayos de regresión que comprueban las capas adicionales de software conforme no introducen errores en el software previamente integrado.
- **Ensayos del sistema software.** Ensayos dirigidos a verificar el sistema de software de forma completa.

Actividades de Validación

Las actividades de validación del diseño prosiguen a las de verificación, una vez éstas han concluido de forma exitosa y ya se dispone del dispositivo acabado o equivalente. Esta actividad puede incluir unidades de producción inicial, lotes o sus equivalentes con la justificación de la elección del producto, y su evaluación clínica.

Los pasos a seguir en el proceso de validación del diseño son los siguientes:

- **Desarrollo del Plan de validación.** Se trata de un documento de sistemática, definición de alcances y estrategia. Este documento debe incluir la identificación del alcance de las actividades de validación, así como su enfoque de especificación/ensayo, restricciones posibles, criterios de aceptación, entornos de trabajo, recursos, cronología, y metodologías a aplicar. Es importante revisar la incorporación al plan del cumplimiento de los requisitos reguladores, así como hacer referencia a otro tipo de actividades relacionadas, como por ejemplo, las de especificación/verificación, o de evaluación clínica.
- **Desarrollo de un ejercicio de evaluación de riesgos** integrado y completo teniendo en cuenta el uso previsto, y los factores de influencia secundarios, como componentes de interfaz del sistema/producto final o el modo de montaje.
- **Redacción del Plan de pruebas** que incluya los criterios de aceptación y los resultados. Deben incluirse los casos de test con los escenarios comunes que demuestren que el software cumple con su uso previsto. Están diseñados para descubrir errores potenciales y demostrar si las funciones clave funcionan correctamente.
- **Ejecución del Plan de pruebas** en arreglo a los procedimientos de prueba, los requisitos reglamentarios, y



Figura 2: Ciclo de vida del software.

Dispositivos médicos

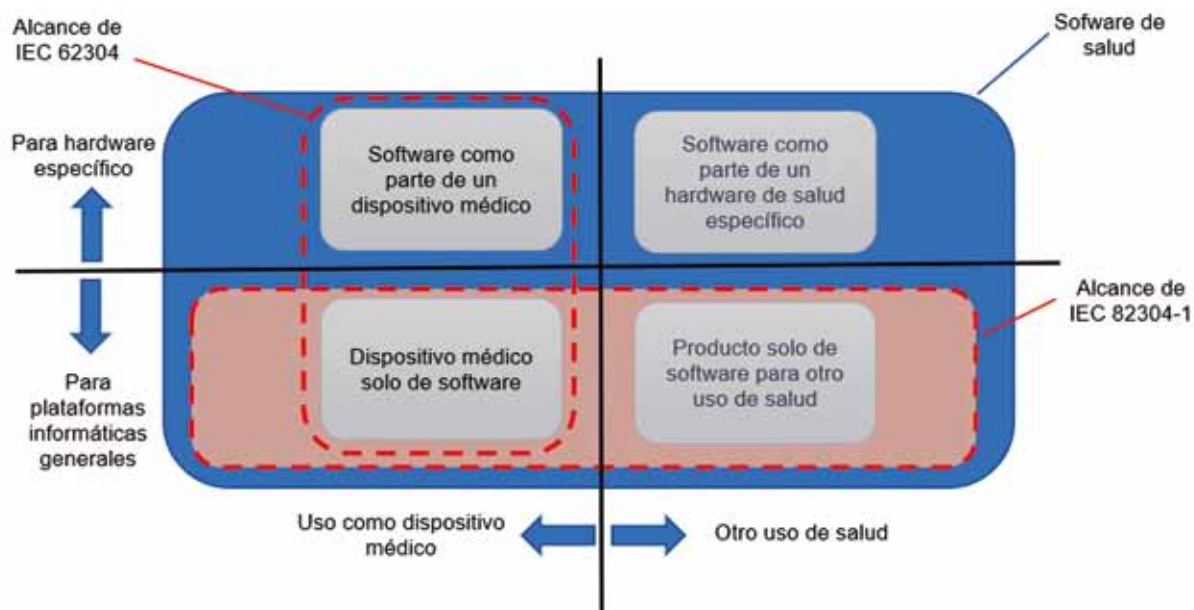


Figura 3: Dominios de aplicaciones de software de salud y alcance de los estándares relacionados (fuente figura A.1 IEC 82304-1).

buenas prácticas documentales.

• **Informe final de validación** con el resumen de resultados e información de soporte para la adecuada liberación del software. Es la respuesta al Plan de Validación. En esta etapa, se aprovecha a su vez para la revisión de los procedimientos de uso / instrucciones, así como el riesgo residual final.

Remarcar que las actividades de verificación y validación no se limitan a una actividad única, ya que debe asegurarse que el sistema software es conforme tras los cambios de configuración o mejoras que puedan llegar a producirse a lo largo de su ciclo de vida.

Estándar IEC 82304-1 y su interrelación con IEC 62304

La norma IEC 82304-1 (Software sanitario. Parte 1: Requisitos generales para la seguridad de los productos) aborda la seguridad de los productos de software de salud concebidos para funcionar en plataformas informáticas convencionales, destinados a ser comercializados sin hardware específico (software autónomo). Su enfoque principal radica en los requisitos para los fabricantes y abarca todas las fases del ciclo de vida, que incluyen diseño, desarrollo, validación, instalación, mantenimiento y desinstalación de los productos de software de salud.

La norma define el software de salud como "software destinado a ser utilizado específicamente para mantener o mejorar la salud de personas individuales o la prestación de atención médica", por lo que puede incluir software

no clasificado como dispositivo médico. A su vez, es un estándar orientado a producto, lo que significa que proporciona orientación sobre cómo diseñar un producto, desde el establecimiento de sus requerimientos, validación, identificación y documentos acompañantes, y actividades de poscomercialización.

Ejemplos de aplicaciones de software de salud a los que le aplicaría este estándar son:

- Aplicaciones móviles
- Aplicaciones estándar para PC
- Aplicaciones servidor
- Sistemas de gestión de información de salud hospitalarios
- Aplicaciones basadas en soluciones SaaS (software as a service)

La Figura 3 muestra los dominios de aplicación para el software de salud y su cobertura por los estándares IEC 62304 e IEC 82304-1.

La fase entre la definición de los requisitos del sistema y la validación del producto final es el proceso de desarrollo del producto. Este proceso de desarrollo se presenta esquemáticamente en la Figura 4, en donde se recogen las actividades adicionales que se añaden a la normativa IEC 62304 vista en la parte 1 del artículo anterior. El proceso real puede seguir varios enfoques, como el enfoque lineal (en cascada) o enfoques iterativos o incrementales.

Dado que la IEC 62304 se centra especialmente en elementos de software integrados en dispositivos médicos, se formulan requisitos para la verificación de software, pero no para la validación. Por lo tanto, los fabricantes de dispositivos



Figura 4: Procesos de productos de software de salud basado en IEC 82304-1).

médicos pueden confiar para ello en la norma IEC 82304 aplicable al software independiente.

Trazabilidad y automatización

Tanto para las actividades de Verificación, así como de Validación, es muy importante contar con una Matriz de Trazabilidad de Requisitos (RTM) que asegure la correcta trazabilidad entre requisitos y ensayos de forma sencilla y eficaz.

A su vez, las nuevas herramientas existentes en el mercado para la automatización de las actividades a lo largo del desarrollo de software, así como de validación digital, hacen posible una mejor gestión de las actividades, permitiendo la trazabilidad de cada requisito, con su especificación, análisis, y ensayo/test de verificación y validación, incluyendo las evidencias, así como una reducción de los errores humanos.

Este enfoque para la mejora de la trazabilidad es especialmente útil para detectar suposiciones o premisas ocultas. Las suposiciones ocultas son peligrosas porque a menudo conducen a un diseño excesivo, lo que añade costes y complejidad innecesarios al diseño. En otros casos, resultan en un diseño no documentado.

Ciberseguridad

Las actuales regulaciones sobre dispositivos médicos están evolucionando para garantizar que los dispositivos comercializados sean aptos para los nuevos desafíos tecnológicos relacionados con los riesgos en materia de ciberseguridad.

En la actualidad, existen numerosos documentos guía publicados por los diferentes organismos reguladores que debemos tener en cuenta a la hora de implementar las medidas de ciberseguridad más adecuadas en nuestros dispositivos.

En especial debemos prestar atención a los requisitos esenciales de seguridad para todos los dispositivos médicos que incorporen sistemas electrónicos programables

(PEMS, por sus siglas en inglés) y software que sean en sí mismos dispositivos médicos. Debemos aplicar en este campo principios de gestión de riesgos, incluida la seguridad de la información, así como establecer requisitos mínimos de seguridad informática, incluida la protección contra el acceso no autorizado.

Por otro lado, existen muchos dispositivos que no fueron diseñados con estas mismas consideraciones y exigencias, por lo que pueden presentar riesgos para los pacientes. Por ello, debemos abordar sus amenazas de ciberseguridad, tal y como recomiendan las regulaciones y buenas prácticas actuales.

Pensamiento crítico y enfoque CSA

El enfoque CSA de la CDRH (FDA) intenta clarificar la interpretación de los requisitos regulatorios con el entorno tecnológico actual, para cambiar el foco de la documentación al pensamiento crítico durante todo el ciclo de vida del software de un dispositivo médico.

La “garantía de la calidad del software” se debe centrar en prevenir la introducción de defectos en el proceso de desarrollo de software y fomenta el uso de un enfoque basado en el riesgo para establecer la confianza conforme el software es adecuado para su uso previsto.

Este nuevo enfoque promueve por lo tanto buenas prácticas de calidad orientadas en los siguientes conceptos:

- Aprovechar la experiencia de los expertos en la materia (SME) aplicando el pensamiento crítico para determinar la metodología y tecnología de verificación más apropiada basada en el riesgo.
- Generación de evidencias documentales de soporte siempre y cuando aporten un valor añadido a la calidad de las pruebas.
- Mayor dedicación a la verificación activa para la búsqueda de defectos y menor dedicación a la generación de especificaciones por adelantado.
- Cambio de foco desde la documentación al pensamiento crítico y a la verificación.



Figura 5: Enfoque CSA y pensamiento crítico.

Machine Learning y Artificial Intelligence

En la actualidad se ha acelerado la adopción y el uso de tecnología AI/ML en dispositivos médicos. Este tipo de dispositivos tienen el potencial de transformar la atención médica al obtener conocimientos nuevos y relevantes en consecuencia de la gran cantidad de datos generados durante todas las fases del proceso de atención médica.

Uno de los mayores beneficios de este tipo de dispositivos reside en la oportunidad de seguir aprendiendo e iterando a medida que hay datos adicionales disponibles, incluso del uso y la experiencia en el mundo real, para mejorar su rendimiento.

Al ser aún una tecnología con una introducción aún incipiente, las entidades reguladoras están publicando documentos de reflexión y concepto sobre la materia para alertar a la industria sobre sus riesgos, para la no introducción de sesgos, clarificación de responsabilidades, mantenimiento de la privacidad, seguridad y confidencialidad de los datos, así como de no introducción de errores por una no adecuada fiabilidad y precisión de los resultados.

Guía GAMP® 5 Second Edition

Las guías GAMP pretenden ofrecer un marco de referencia en buenas prácticas dentro del sector Life Science para garantizar que los sistemas informáticos sean efectivos, confiables y de alta calidad, de forma que sean adecuados para su uso previsto y cumplan con las regulaciones aplicables.

La nueva guía GAMP® 5 Segunda Edición ha revisado prácticas, desarrollos tecnológicos (ej.: AI/ML, proveedores de servicios en la nube), enfoques en evolución del desarrollo de software (Agile), así como el uso ampliado de herramientas de software automatizadas. Destaca el

uso del pensamiento crítico de los expertos en la materia (SME), así como el aprovechamiento de las actividades del proveedor, para poder definir los enfoques más apropiados de especificación y verificación en las circunstancias específicas en base a su conocimiento y experiencia. Por todo ello, se trata de una guía de referencia que puede integrarse plenamente con las exigencias de los dispositivos médicos y brindar soporte en aspectos como la arquitectura de software y segregación, así como la gestión de riesgos de diseño y el desarrollo de software.

Conclusiones

El software ha adquirido una relevancia significativa en el ámbito de los dispositivos médicos. Es esencial desarrollarlo de manera segura y eficiente para garantizar el uso y la seguridad óptimos del dispositivo médico correspondiente. Las nuevas tecnologías, nos ofrecen nuevas oportunidades, pero a su vez, nuevos desafíos que debemos abordar en base al conocimiento científico, la experiencia, y en donde la aplicación de los correctos estándares a lo largo de los procesos de desarrollo de software y validación, son clave para asegurar la conformidad regulatoria.

Acrónimos

- AI: Artificial Intelligence
- CDRH: Center for Devices and Radiological Health
- CSA: Computer Software Assurance
- FDA: Food and Drug Administration
- IEC: International Electrotechnical Commission
- ISO: International Organization for Standardization
- ML: Machine Learning
- PC: Personal Computer
- PEMS: Programmable Electrical Medical Systems
- RTM: Requirements Traceability Matrix
- SME: Subject-Matter Expert
- SW: Software