Shitsuke s.r.l.

Como siempre... Innovando y creando valor para Usted, y por Usted

Cuadernos de Orientación al Cliente

Nivel Básico

EAM 3

Recomendaciones básicas sobre el Análisis del Software en Equipos Médicos

Resumen: *Este trabajo tiene por objetivo orientar a los fabricantes de equipos electromédicos en cómo generar la información básica necesaria para cumplimentar las exigencias de las normativas vigentes en relación al software. Debido al estado actual del arte se implementara la norma IEC 60601-1:2005 en lo referido a su Capitulo 14*

Palabras claves: *Análisis de riesgo, software de grado medico, seguridad y eficacia*

Autor: *Ing Gustavo Javier Wain | Electrotecnología en área médica | gwain@shitsukesrl.com.ar*

La Norma Internacional **IEC 60601-1:2005** en su **Capitulo 14**, especifica los requerimientos a cumplimentar por parte del fabricante, en relación a la seguridad inherente que debe tener un equipo electromédico para considerarse seguro.

¿Cuándo se debe aplicar el Capitulo 14 de la Norma?

Dado el estado actual del arte en lo que se refiere al diseño electrónico, es muy común hoy encontrar en la mayoría de los equipos electromédicos algún microprocesador, un microcontrolador, o cualquier otro tipo de sistema embebido programable, ya sea de muy bajo nivel como de alto nivel.

Estos sistemas pueden controlar desde un teclado, una pantalla, o ser la interface de otros sistemas, a funciones muy especificas de medición o control de parámetros fisiológicos del paciente.

La gestión de riesgos del software debe ser implementada y verificada, si se demuestra que el aparato o sistema electromédico efectivamente puede ser riesgoso a causa de cualquier inconveniente suscitado por el mal funcionamiento del software.

En el caso que a través de un análisis de riesgo según la **Norma ISO 14971**, se determine de manera fehaciente que el software (su falla, deterioro o degradación) no puede producir un efecto adverso sobre el paciente, el usuario o el medio ambiente y las prestaciones del equipo son acordes a su funcionamiento esencial, **en ese caso, no se requiere el análisis exigido en este capitulo de la norma.**

Nivel de conformidad del Capitulo 14

A diferencia de otros puntos de la norma **IEC 60601-1:2005** en los cuales se debe realizar un ensayo determinado para corroborar el cumplimiento o verificación del punto, lo exigido en este caso por la norma para dar conformidad en el cumplimiento es la de realizar una inspección al **ARCHIVO DE GESTION DE RIESGOS**, y la evaluación de todos los procesos que se van desglosando en este capitulo en particular.

El fabricante deberá demostrar ante el laboratorio el cumplimiento de las exigencias de este capitulo mediante la presentación de toda la información que haya generado a este respecto, justificando los riesgos residuales obtenidos y dando prueba evidente y comprobable de la seguridad y eficacia implementada a nivel del software.

La información debe ser generada conforme a las exigencias de la **Norma ISO 14971** y el formato de la documentación deberá ser acorde en la Republica Argentina a las exigencias de las **Buenas Prácticas de Fabricación** según la **Disposición 191/99** en su **Parte D**. Para otros países fuera del Mercosur, se deberá implementar según los requerimientos de la Norma **ISO 13485** en su **Punto 4**, o según sus normativas vigentes propias.

Documentación a generar

La mínima documentación a generar por parte del fabricante y la cual es parte del **Archivo de Gestión de Riesgos** y requerida para el cumplimiento del Capitulo 14 es la mostrada en las siguientes Tablas:

ARCHIVO DE GESTION DE RIESGOS	ISO 14971
Proceso de gestión de riesgos	3.2
Resultados concretos del análisis del riego	4.1
Resultados de la evaluación de riesgos	5
Uso previsto / Mal uso razonablemente	4.2
Política de calidad y aceptación del riesgo	3.3
Características relativas a la seguridad	4.2
Revisión de la gestión de riesgos	3.3
Evaluación global del riesgo residual	7
Riesgo estimado del peligro	4.4
Clasificación de los riesgos	4.4
Informe de gestión de riesgos	8
Registros de verificaciones	6.3
Retroalimentación post producción	9
Evaluación del riesgo residual	6.4
Análisis de riesgo/beneficio	6.5
Control del riesgo	6.6
Criterios de valoración	6.7
Medidas para el control del riesgo	6.2; 6.3
Riesgo residual	6.4; 6.5

Tabla 1

En este caso, la información de cómo generar estos documentos debe ser la especificada en la Norma ISO 14971 y redactada conforme a las **Buenas Practicas de Fabricación**.

ARCHIVO DE GESTION DE RIESGO	IEC 60601	ISO 14971
Plan de gestión de riesgos	14.3	3.5
Ciclo de vida del desarrollo	14.4	
Proceso de resolución de problemas	14.5	
Especificación de requisitos	14.7	
Especificaciones de subsistemas	14.7	
Listado de los peligros	14.6	4.3
Especificaciones de la arquitectura	14.8	
Entorno de diseño	14.9	
Plan de verificación	14.10	
Registros de validación	14.11	
Plan de validación del sistema programable	14.11	
Informacion de acoplamiento, red de datos	14.13	

Tabla 2

Para esta Tabla se deberá tener en consideración específicamente lo declamado en la **IEC 60601-1:2005**, siendo que algunos puntos además deberán conformarse según la norma **ISO 14971** simultáneamente.

Para cada peligro encontrado en el Análisis de Riesgo se debe generar documentación específica según consta en la siguiente Tabla:

PELIGRO n		
		ISO 14971
Análisis del riesgo		4
Riesgo		
	Evaluación del riesgo	5
Control del riesgo		6.2; 6.3
	Registros del control	
Verificación		
	Registros de verificación	6.3
Riesgo residual		
	Evaluación	6.4

Tabla 3

Ciclo de vida del desarrollo del software

Es fundamental a la hora del análisis de la información, contar de manera precisa y clara con un esquema que determine el ciclo de vida del desarrollo. Para cumplimentar las exigencias normativas, se deben definir hitos, los cuales deben estar claramente identificados durante todo el proceso.

Para cada hito fijado en el ciclo de vida del desarrollo se deberán describir las actividades, métodos y procesos que le son inherentes. Es fundamental a la hora de la evaluación, que cada hito tenga claramente especificado como se lo verifica y que existan métodos documentados relativos a este control.

Cada hito es definido por cierta información que ingresa y que egresa del mismo. Debe estar claramente detallado cada uno de estos parámetros para considerarse como valido este ítem.

A manera de ejemplo y de dar evidencia de cumplimiento es una buena practica que en cada hito se declaren los documentos y registros que ingresan y egresan, justificando la manera en la cuales se verifica y/o valida.

Proceso de gestión de riesgos

El proceso de gestión de riesgos se cumplimenta cuando el fabricante realiza un listado exhaustivo de todos aquellos riesgos razonables y previsibles, relacionados específicamente con aquellos donde el software tenga algún tipo de injerencia o sea de manera directa o indirecta responsable de algún tipo de daño. También durante esta gestión, se debe tener en cuenta aquellos peligros relacionados con la transmisión o recepción de información digital como ser un acoplamiento con otros sistemas ya sean médicos o no o redes de datos.

A manera de ejemplo algunas posibles causas podrían ser:

1. Fallo del acoplamiento/red de datos
2. Retorno indeseado [físico y datos] (posibilidades de incluir: entrada no solicitada, entrada fuera de rango o inconsistente, y entrada originada por interferencia electromagnética)
3. Datos no disponibles
4. Falta de integridad de datos
5. Datos incorrectos
6. Sincronización incorrecta de datos
7. Interacciones imprevistas
8. Aspectos o calidad desconocida del software de una tercera parte
9. Carencia de seguridad de los datos, particularmente la vulnerabilidad para la manipulación, interacción imprevista con otros programas y virus.

Se deberán elegir y documentar las herramientas necesarias para toda la gestión de riesgo.

Estas herramientas pueden ser obtenidas tanto de los Anexos de la **Norma ISO 14971** como también de la **Norma ISO 31010**.

Es importante en este punto dejar evidencias de las herramientas utilizadas. En el caso que el fabricante haya optado por una **Tormenta de Ideas**, para establecer los riesgos de determinada etapa, esta debe estar debidamente documentada según como se especifique en el sistema.

Las herramientas mas ampliamente difundidas (a manera de ejemplo) son:

- Tormenta de Ideas
- Análisis Modal de Fallas y Efectos (AMFE)
- Árbol de fallas
- Diagramas de Ishikawa

Plan de verificación

Cada hito planteado en el ciclo de vida del desarrollo debe ser verificado. Es por ello que la norma exige un plan de verificación en aquellos hitos en los cuales exista un verdadero riesgo que vulnere el funcionamiento esencial o la seguridad básica del equipo medico.

Este plan de verificación consta básicamente de los siguientes puntos:

- En qué hito se realiza la verificación
- Selección y documentación de las estrategias, actividades y técnicas a desarrollar
- Organigrama fijando responsabilidades de los auditores e independencia de áreas auditadas

- Selección y utilización de las herramientas mas idóneas según el desarrollo
- Criterios de cobertura

Algunas de las técnicas sugeridas por la norma son las siguientes:

- Lecturas cruzadas
- Inspecciones
- Análisis estático
- Análisis dinámico
- Ensayos de caja blanca
- Ensayos de caja negra
- Ensayos estadísticos

Plan de validación

El plan de validación es **FUNDAMETAL**, a la hora que el fabricante demuestre que su producto cumple con los requisitos de seguridad básica y de funcionamiento esencial.

Se deben proporcionar evidencias contundentes que se efectuó una validación, ya sea de cada hito que corresponda y del sistema general. Esta validación deberá ser coherente con las condiciones impuestas al sistema de gestión de la calidad.

La validación deberá ser realizada por personal idóneo con independencia del ítem auditado.

En el **Archivo de Gestión de Riesgos** debe estar documentado y rubricado por el responsable los resultados completos de las validaciones efectuadas.

Especificación de requisitos

Es fundamental que el fabricante determine completamente y de manera tajante las especificaciones tanto del aparato electromédico como de aquellos bloques con riesgo debido al software o a la arquitectura hardware.

Debe estar documentado las especificaciones y corroborarse que durante la entrada y salida de información de cada bloque se mantengan estas características.

La documentación mínima a presentar por el fabricante debe ser la siguiente:

- Requisitos de funcionalidad, incluyendo las características del funcionamiento esencial; características físicas, y condiciones ambientales bajo las cuales el software funcionará
- Interfaz externas del software
- Requisitos de seguridad incluyendo las medidas de control de riesgos para los fallos del hardware y defectos potenciales del software y especificaciones relativas a los métodos de funcionamiento y mantenimiento, influencias ambientales, y control de riesgos
- Señales de alarma, advertencias y mensajes para el usuario controlados por software
- Requisitos de seguridad, cuando la pérdida de seguridad pudiera comprometer la seguridad
- Requisitos de ingeniería de la usabilidad relacionados al uso del equipo o sistema electromédico, incluyendo aquellos relativos para soportar operaciones manuales, interacciones hombre-equipo, limitaciones sobre el personal, y áreas que necesitan concentrar la atención humana que son sensibles a los errores y formación humanos
- Definición de datos y requisitos de la base de datos
- Requisitos de instalación y aceptación para el software
- Documentación a desarrollar
- Requisitos de funcionamiento y ejecución
- Requisitos de mantenimiento.
- La gestión de riesgos debería ser usada para determinar hasta qué punto el diseño de la arquitectura se puede usar

Auditoria interna final

Es recomendable que antes que el equipo sea evaluado en el laboratorio y se realice la auditoria sobre el **Archivo de Gestión de Riesgos de Software**, el fabricante realice una auditoria interna, a fin de encontrar sus propios deslices y tener una idea cabal de que haya cumplimentado todos los puntos de la norma.

La auditoria de **Archivo de Gestión de Riesgos del Software** se realiza analizando cada punto del Capitulo 14. Existe un TRF de la IEC indicando la manera de cómo realizar las preguntas y los puntos donde se realiza hincapié en la información solicitada.

Bibliografía utilizada

- Norma IEC 60601-1:2005
- Norma ISO 14971
- Norma ISO 31000
- Norma ISO 31010

Shitsuke S.R.L. (CBTL de IECEE)
Av. Carlos Pellegrini (Ex-R7) Nº 460.
Luján, B.A., B6702LVJ, Argentina
(02323)435565/432668/429701
www.shitsukesrl.com.ar