Controles y auditoría en los dispositivos médicos

Como expliqué en el post anterior, existen múltiples formas de atacar o de poner en riesgo los dispositivos médicos que utilizamos día a día y cada vez con más vulnerables, desde ataques a través de software mal configurado, hasta la obtención de datos erróneos del paciente. Esto último podría ser fatal ya que pondría en peligro directamente al paciente. ¿Qué pasaría si "por un error informático", le suministramos una dosis errónea de un medicamento a un paciente? El resultado podría ser fatal. Y eso no ocurre solo a los ordenadores como tal, también dispositivos que tienen los pacientes como los marcapasos o wearable que recogen datos que podrían usarse en caso de emergencia. Por lo que no podemos arriesgarnos en la salud de las personas, hay que controlar los posibles riesgos.

En el post anterior también me adelanté explicando la ISO 14971, que permite evaluar y controlar los riesgos. Este, define unos pasos a seguir. [1]

1. Crear un plan de gestión de riesgos para el dispositivo
    - Define los pasos detallados de un dispositivo en concreto, incluyendo el análisis del riesgo, en control del riesgo, la revisión y el reporte.
2. Ejecutar actividades de riesgo
    - Utilizar herramientas de análisis de riesgo, para

reducirlos al mínimo. También es conveniente hacer un balance riesgos-beneficios.

3. Revisar los resultados obtenidos y realizar un reporte
    - Documentar el trabajo realizado y comentar los resultados

Un concepto interesante que se puede usar para medir la probabilidad de que ocurra un riesgo y su posible resultado sería la utilización de una matriz de aceptación de riesgos, que mide con 3 colores el nivel de riesgo. [2]

PROBABILITY OF OCCURENCE	SEVERITY OF HARM				
	Negligible Minor injury or property damage	**Minor** Limited injury or property damage	**Serious** Medically reversible injury or significant property damage	**Critical** Permanent injury or serious property damage	**Catastrophic** Life-threatening injury or catastrophic property damage
Frequent Happens with almost every use of the device	CAPA	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE
Probable Occurs the majority of times but not with every use	CAPA	CAPA	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE
Occasional Occurs with increased frequency	ACCEPTABLE	CAPA	CAPA	UNACCEPTABLE	UNACCEPTABLE
Remote More than one occurrence per year but still unlikely	ACCEPTABLE	ACCEPTABLE	CAPA	UNACCEPTABLE	UNACCEPTABLE
Improbable Less than one occurrence per year; isolated events	ACCEPTABLE	ACCEPTABLE	ACCEPTABLE	CAPA	CAPA

Ahora que ya hemos identificado los riesgos, los hemos analizado por niveles, podemos controlarlos. La ISO 14971 sigue ayudándonos
haciéndonos las siguientes preguntas.

- ¿Podemos reducir el riesgo?
- ¿Cuál es la mejor manera de hacerlo?
- ¿Ha funcionado el control del riesgo?
- ¿Es aceptable el nivel de riesgo que tenemos

ahora?

HERRAMIENTAS

Si no contamos con experiencia anterior en control de riesgos, puede ser complicado evaluar cuál es la más indicada para tu problema. ¿Tiempo? Finito. ¿Herrramientas? Infinitas (más o menos). Se pueden separar básicamente en 3 tipos: Botton-up, top-down y el resto. La siguiente imagen muestra varias de las más comunes. [3]

BOTTOM-UP TOOLS	HOW IT IS USED
Preliminary Hazard Analysis (PHA)	"What if" analysis that takes a *hazard* and traces it to harm. Useful early in the risk management process.
Failure Mode and Effects Analysis (FMEA)	"What if" analysis that takes a *failure* and traces it to an injury or hazard. Often used in design and process phases. Focuses on one piece of the puzzle, but don't rely on it alone for your risk management process. Best for manufacturing and use instructions.
Failure Mode, Effects, and Criticality Analysis (FMECA)	Builds on the FMEA model but adds risk evaluation, including severities and probabilities.

TOP-DOWN TOOLS	HOW IT IS USED
Ishikawa or Fishbone (Cause-and-Effect) Diagram	Imagine this as a diagram resembling an artery with veins that branch off from it. It starts with six primary possible causes (veins) and then branches off further to show more specific causes related to that primary potential cause.
Fault Tree Analysis (FTA)	Starts with failure and works back to the component. Focuses on the big picture, unlike FMEA. Good choice for design activities. Use with FMEA for new design technology unless failure modes are unknown.

MORE TOOLS	HOW IT IS USED
Brainstorming	Generates a wide variety of ideas. It's important to crystalize the true objective so time is not wasted. Clusters can be then grouped to form an Ishikawa diagram.
Turtle Method	Starts with a process and examines factors that influence the process such as training, equipment, procedures, installation, etc.
Hazard Analysis and Critical Control Points (HAACP)	Identifies various errors and hazards in production processes that can cause finished products to be unsafe. Designs measurements to reduce risks to a safe level.
Hazard and Operability Analysis (HAZOP)	Assumes accidents are caused by deviations from design or operating intentions. Uses keywords to focus attention on specific aspects of design intent or associated process condition.

También me parece importante destacar que solo se pueden prever los riesgos que están bajo tu control. Por ejemplo, no debemos obsesionarnos con los riesgos que acarrea una pandemia

mundial, ya que no está bajo nuestro control y además es nuevo para todos.

Para terminar, también es importante evaluar los beneficios. El tipo, la magnitud o la probabilidad pueden ser unos indicadores positivos

Como ejemplo, voy a intentar establecer los posibles controles para los riesgos identificados en el anterior post: [4]

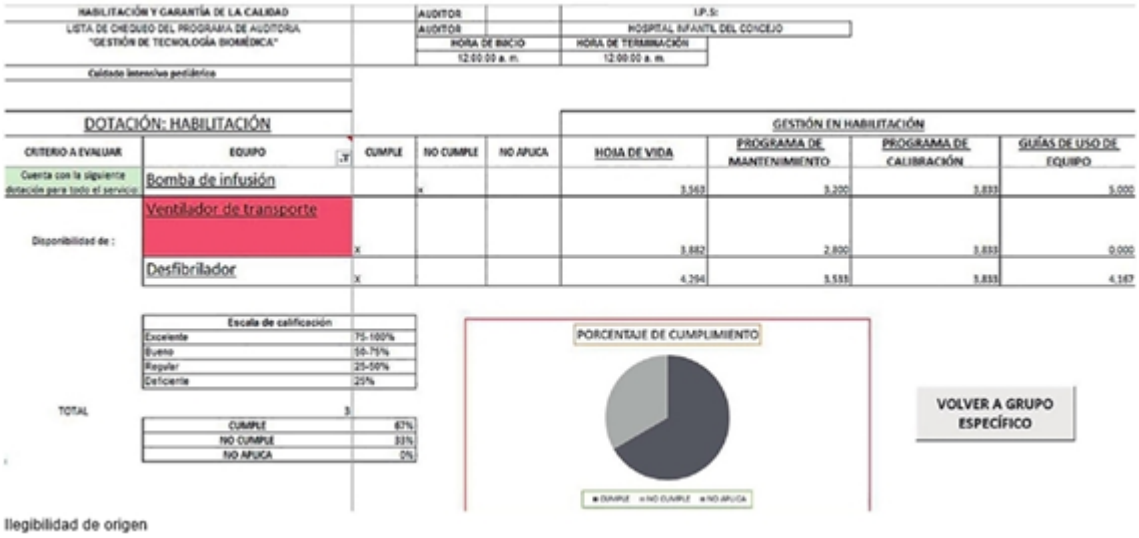
- Limitar los controles de acceso –> Solamente al dispositivo que está conectado y establecer la autenticación en 2 pasos.
- Actualizaciones periódicas –> Aplicar parches de seguridad es la mejor práctica.
- Aplicar estándares en el código –> Testearlo rigurosamente antes de desplegarlo y establecer unas características para desarrollarlo de la mejor manera posible.
- Seguridad por diseño –> Asegurar el inventario de las terceras partes en cuanto a software y hardware. También podría ser importante en el uso de canales encriptados para comunicarse con el resto del mundo.

No se puede hablar sobre los controles sin hablar de los auditores, que tienen una labor esencial en lo que llevamos hablando en este post y en muchas otras acciones. Son los responsables en cumplimentar las regulaciones y procedimientos que se utilizan.

Por ejemplo, el MDSAP (Programa de Auditoría Única de Dispositivos Médicos) es una iniciativa internacional que permite realizar una única auditoría del sistema de gestión de calidad de los fabricantes de dispositivos médicos satisfaciendo todas las regulaciones en múltiples países. De esta manera se logra centralizar un poco la forma de auditar

entre los distintos países. [5]

Un ejemplo sobre ello es un artículo que he visto sobre la "gestión de equipos médicos: implementación y validación de una herramienta de auditoría", en el que explican los detalles, pasos, etapas y la importancia de esta actividad. Es un poco extenso, pero dejo este par de imágenes de resumen. [6]



HABILITACIÓN Y GARANTÍA DE LA CALIDAD
LISTA DE CHEQUEO DEL PROGRAMA DE AUDITORIA "GESTIÓN DE TECNOLOGÍA BIOMÉDICA"
Cuidado Intensivo pediátrico
AUDITOR
AUDITOR
HORA DE INICIO 12:00:00 a. m.
I.P.S: HOSPITAL INFANTIL DEL CONCEJO
HORA DE TERMINACIÓN 12:00:00 a. m.

DOTACIÓN: HABILITACIÓN

CRITERIO A EVALUAR	EQUIPO	CUMPLE	NO CUMPLE	NO APLICA	GESTIÓN EN HABILITACIÓN: HOJA DE VIDA	PROGRAMA DE MANTENIMIENTO	PROGRAMA DE CALIBRACIÓN	GUÍAS DE USO DE EQUIPO
Cuenta con la siguiente dotación para todo el servicio	Bomba de infusión		x		3.563	3.200	3.833	5.000
Disponibilidad de :	Ventilador de transporte	x			3.882	2.800	3.833	0.000
	Desfibrilador	x			4.294	5.555	3.833	4.167

Escala de calificación	
Excelente	75-100%
Bueno	50-75%
Regular	25-50%
Deficiente	25%

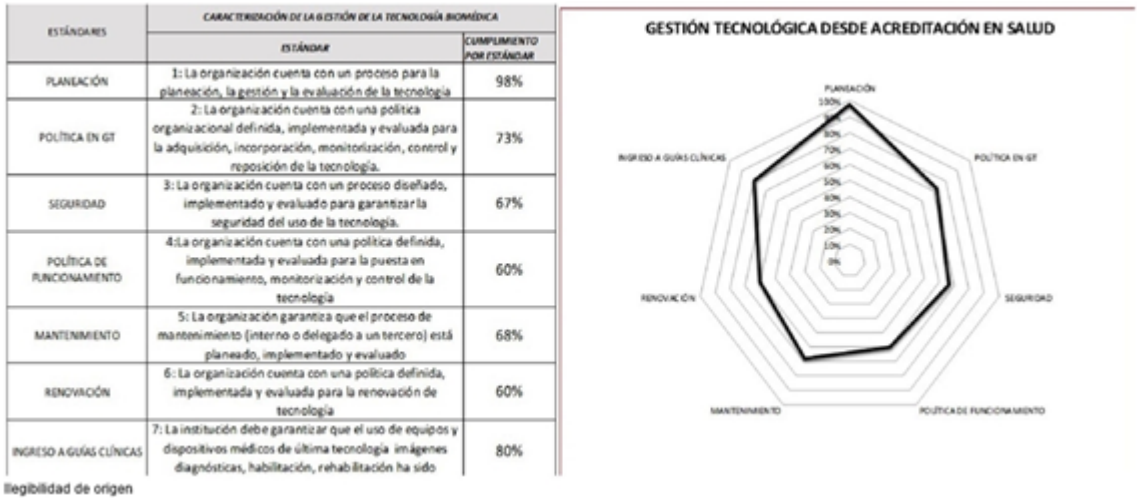
TOTAL 3

CUMPLE	67%
NO CUMPLE	33%
NO APLICA	0%

VOLVER A GRUPO ESPECÍFICO

Ilegibilidad de origen

Evaluación de gestión de equipos médicos en el marco de la resolución 2003 de 2014



ESTÁNDARES	CARACTERIZACIÓN DE LA GESTIÓN DE LA TECNOLOGÍA BIOMÉDICA: ESTÁNDAR	CUMPLIMIENTO POR ESTÁNDAR
PLANEACIÓN	1: La organización cuenta con un proceso para la planeación, la gestión y la evaluación de la tecnología	98%
POLÍTICA EN GT	2: La organización cuenta con una política organizacional definida, implementada y evaluada para la adquisición, incorporación, monitorización, control y reposición de la tecnología.	73%
SEGURIDAD	3: La organización cuenta con un proceso diseñado, implementado y evaluado para garantizar la seguridad del uso de la tecnología.	67%
POLÍTICA DE FUNCIONAMIENTO	4:La organización cuenta con una política definida, implementada y evaluada para la puesta en funcionamiento, monitorización y control de la tecnología	60%
MANTENIMIENTO	5: La organización garantiza que el proceso de mantenimiento (interno o delegado a un tercero) está planeado, implementado y evaluado	68%
RENOVACIÓN	6: La organización cuenta con una política definida, implementada y evaluada para la renovación de tecnología	60%
INGRESO A GUÍAS CLÍNICAS	7: La institución debe garantizar que el uso de equipos y dispositivos médicos de última tecnología imágenes diagnósticas, habilitación, rehabilitación ha sido	80%

Ilegibilidad de origen

Resultados dinámicos de la evaluación de estándares de gestión de la tecnología en el marco de acreditación en salud

Como se puede ver en la imagen superior, el resultado es muy similar a las actividades que realizamos en clase así que es fácilmente

entendible y muy visual.

Al final del artículo, vuelven a recalcar los beneficios cuando se ha aplicado la auditoría en este ámbito y la importancia de desplegarla en los mayores entornos posibles.

Para terminar, en el próximo post, el último, trataré algunos temas que se me han quedado en el tintero para finalizar con este contenido.

Referencias

[1] <<ISO 14971 and Medical Device Risk Management 101>>, Oriel Stat a Matrix, consultado el 5/11/2020, https://www.orielstat.com/blog/iso-14971-risk-management-basics/

[2] <<Creating a Medical Device Risk Management Plan and Conducting a Risk Analysis>>, Oriel Stat a Matrix, consultado el 5/11/2020, https://www.orielstat.com/blog/medical-device-risk-management-planning-analysis/

[3] <<Medical Device Risk Control and Risk Management Tools>> , Oriel Stat a Matrix, consultado el 5/11/2020, https://www.orielstat.com/blog/risk-controls-risk-management-tools/

[4] <<Device manufacturers – A Snapshot of Guidance>>, ISACA, vol 4 (2019): 30-31

[5] <<Medical Device ISO 13485:2003 Voluntary Audit Report Pilot Program; Termination of Pilot Program; Announcement of the Medical Device Single Audit Program Operational Phase>>, Océano, consultado el 5/11/2020, https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_cdi_proquest_reports_1749683809&context=PC&vid=deusto&lang=es_ES&search_scope=default_scope&adaptor=primo_central_m

ultiple_fe&tab=default_tab&query=any,contains,medical%20devices%20audit

[6] <<Gestión de equipos médicos: implementación y validación de una herramienta de auditoría>>, SciELO, consultado el 5/11/2020, http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-95322017000100076