Con la salud no se juega

¿Con ganas de seguir profundizando en el ámbito de los dispositivos médicos? Ojalá que así sea.

Antes de empezar me gustaría recapitular un poco. En el primer post pudimos obtener una visión general sobre el amplio mundo del IoMT, mientras que en el segundo post profundizamos en mayor medida en la relevancia de la cual disponen este tipo de dispositivos en la industria. En este post, sin embargo, nos vamos a centrar más en sus riesgos.

¿Os lo podrías imaginar no? A pesar de disponer de múltiples beneficios, los riesgos son una cuestión importante a tener en cuenta.

Algunos de los principales riesgos asociados a los dispositivos médicos son los **riesgos cibernéticos**. El ataque WannaCry, por ejemplo, muestra cómo la interconexión de los sistemas de salud y las **débiles prácticas de seguridad** pueden poner en riesgo tanto a las organizaciones como a los pacientes. Este malware afectó a dos hospitales de EE. UU, en los cuales los atacantes aprovecharon las vulnerabilidades conocidas en el software de los dispositivos para atacar. Muchos dispositivos en todo el sistema sanitario utilizan software antiguo que es difícil de actualizar, lo que significa que están indefensos a que actores maliciosos los exploten. [1]

En junio de este mismo año, por ejemplo, la empresa Medtronic tuvo que retirar del mercado algunas bombas de insulina ya que resultaban vulnerables a ataques, siendo imposible su enmienda a través de una actualización. Este tipo de dispositivos estaban siendo utilizados por alrededor de 4000 pacientes, pudiendo cualquier persona que no fuese cuidador o proveedor de atención médica conectarse de forma inalámbrica y cambiar la configuración de la bomba. Esto podría permitir a cualquier persona administrar insulina en exceso a un paciente (lo que llevaría a un nivel bajo de azúcar en sangre) o a detener la administración de insulina (lo que podría conllevar a una cetoacidosis diabética). [2]

En octubre, hace escasamente un mes, la Administración de Drogas y Alimentos (FDA) emitió una advertencia a los consumidores sobre posibles fallos de ciberseguridad en algunos dispositivos médicos. Los investigadores identificaron 11 vulnerabilidades que permitían que cualquier persona tomara el control de los dispositivos médicos a distancia y cambiara su función, causara fugas de información o incluso causara un ataque de denegación de

servicio inhabilitando el dispositivo. [3]

Además, las compañías de dispositivos médicos poseen datos sensibles y de alto valor que los ciberdelincuentes o los hacktivistas pueden intentar robar. **La información de identificación personal** (IIP) como los **datos clínicos** de los pacientes son un objetivo primordial a proteger. Estos datos no solo deben ser protegidos antes atacantes externos, sino que también se deben controlar los accesos internos realizados por empleados a los datos sensibles y restringir aquellos accesos no autorizados.

Según un estudio realizado en 2016 por el Ponemon Institute, que incluyó a empresas de dispositivos médicos, el 90 por ciento de las organizaciones de salud habrían sufrido una violación de datos en los dos años previos a la realización del estudio. Ponemon estima que estos incidentes le costaron a la industria de la salud 6.200 millones de dólares. [1]

¿Y cuales son los mayores riesgos que presentan actualmente los dispositivos médicos?

De acuerdo al informe realizado por el instituto ECRI con vistas al año 2020 acerca de los peligros tecnológicos más candentes en cuanto a dispositivos médicos se refiere, [4] se pueden resaltar los siguientes:

- **Procedimientos quirúrgicos robóticos no probados:** Los centros de salud necesitan procesos robustos para aprobar la aplicación de robots quirúrgicos en nuevos procedimientos, así como programas integrales de capacitación y acreditación para cirujanos y personal de quirófano.
- **Sobrecarga de alarmas, alertas y notificaciones:** Se necesita un enfoque global que tenga en cuenta todas las fuentes de datos a fin de evitar la sobrecarga cognitiva que puede distraer o desensibilizar a los médicos. Esto puede hacer que profesionales sanitarios ignoren notificaciones relevantes.
- **Riesgos de la ciberseguridad en el entorno de atención sanitaria a domicilio:** Al igual que con cualquier dispositivo médico en la red, los dispositivos médicos utilizados en el hogar deben estar protegidos contra amenazas que puedan interrumpir el flujo de datos, alterar o degradar el rendimiento del dispositivo o exponer información médica protegida.
- **Las tuercas y tornillos sueltos:** Las tuercas y tornillos que sujetan los componentes de los dispositivos médicos pueden aflojarse con el tiempo. Si no se reparan o reemplazan estos mecánicos, se pueden producir consecuencias graves. Los dispositivos pueden volcarse, caerse o colapsar durante su uso, lo cual puede provocar lesiones o incluso la

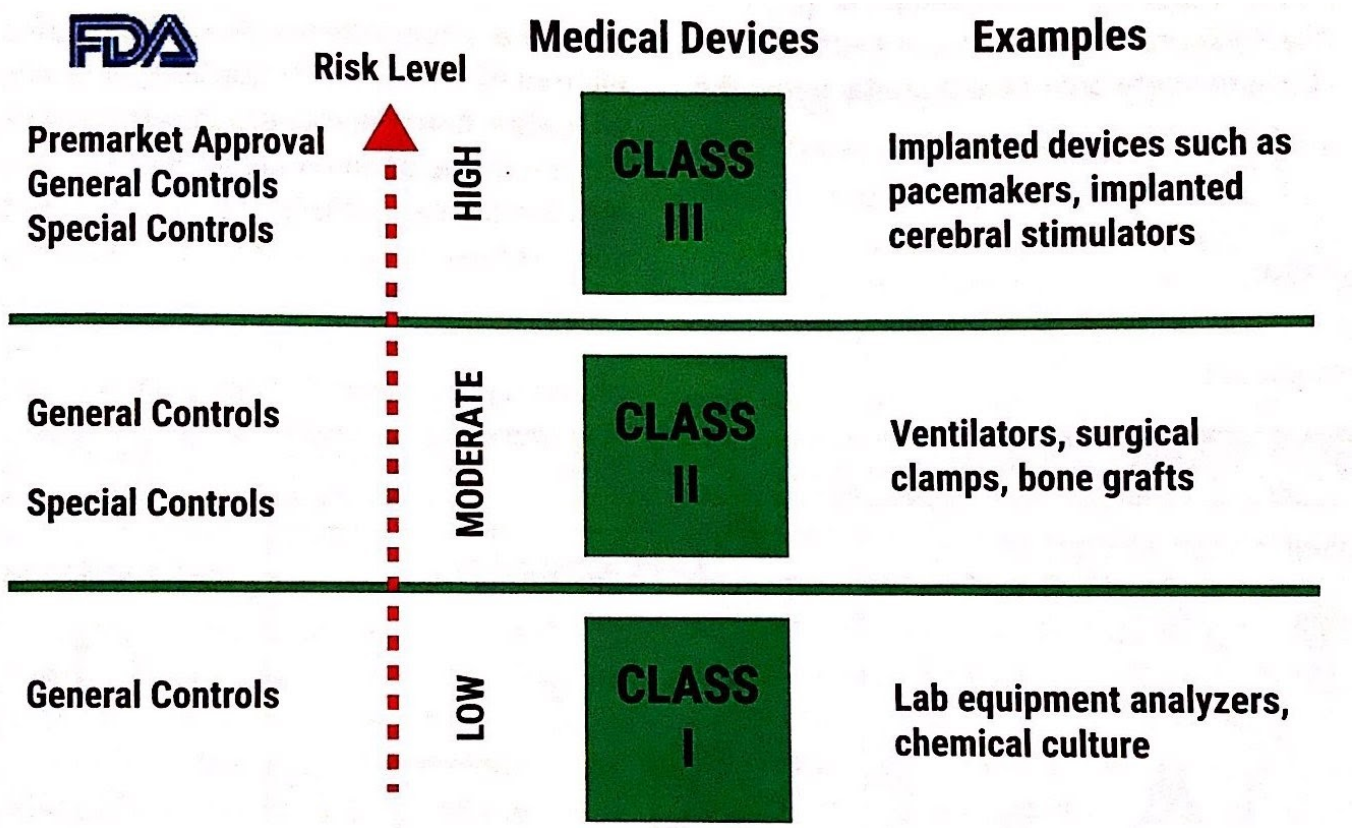
muerte de pacientes.

En este estudio también se contemplan otro tipo de peligros que no corresponden explícitamente al ámbito tecnológico, por lo que no los he tenido en cuenta en este artículo.

Ante este contexto, en 2014 la FDA (Food and Drug Administration) por primera vez en su historia y como el primer organismo regulador del mundo, identificó y abordó el riesgo de la ciberseguridad asociada a los dispositivos médicos. Esta fue la primera mejora para proteger a los pacientes desde la perspectiva de la ciberseguridad de los dispositivos médicos. [5]

Vale, bien… ¿Y cómo podemos clasificar los dispositivos médicos?

De acuerdo a la FDA, los dispositivos médicos pueden ser clasificados de acuerdo a su riesgo de la siguiente forma: [6]



Clasificación de dispositivos médicos en base a riesgos (ISACA)

- **Dispositivos clase I:** Estos dispositivos presentan un **potencial mínimo**

de daño al usuario y a menudo tienen un diseño más simple que los dispositivos de Clase II o Clase III. Por ejemplo, se pueden incluir dentro de esta clasificación dispositivos como los estetoscopios.
- **Dispositivos clase II:** La mayoría de los dispositivos médicos se consideran dispositivos de Clase II. Estos dispositivos disponen de un **riesgo moderado** y dentro de esta clase se pueden incluir dispositivos como las sillas de ruedas eléctricas o dispositivos de rayos X.
- **Dispositivos clase III:** Estos tipos de dispositivos normalmente son responsables de mantener con vida al paciente, son implantados o presentan **un riesgo potencial** de enfermedad o lesión. Ejemplos de dispositivos de Clase III pueden ser los marcapasos implantados.

Dado que la clasificación de los dispositivos médicos se basa en el riesgo, es importante entender el nivel de riesgo y, lo que es más importante, para qué se va a utilizar el dispositivo desde el punto de vista médico y su alcance.

Espero que con este artículo os haya quedado más claro la ingente cantidad de riesgos a los cuales están expuestos los dispositivos médicos (control remoto no autorizado, robado de información personal, ataques a la disponibilidad,…) y cómo podemos clasificarlos de acuerdo a su riesgo para luego poder establecer **controles**.

Pero de esto hablaremos en mayor profundidad en el siguiente post, espero que os haya gustado.

Referencias

[1] <<Life Sciences, Pharmaceutical and Medical Device Companies Need to Trust Less and Question More to Keep High-Value Data Safe>>, Knowledge Leader, acceso el día 15 de noviembre del 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/hotissuekeephighvaluedatasafe

[2] <<Medtronic recalls some insulin pumps as FDA warns they can be hacked>>, CNBC, acceso el día 15 de noviembre del 2019, https://www.cnbc.com/2019/06/27/medtronic-recalls-some-insulin-pumps-as-fda-warns-they-can-be-hacked.html

[3] <<FDA issues warning on medical devices that are vulnerable to takeover

from hackers>>, CNBC, acceso el día 16 de noviembre del 2019, https://www.cnbc.com/2019/10/01/fda-issues-warning-on-medical-devices-that-are-vulnerable-to-cyberattacks.html

[4] <<Top 10 Health Technology Hazards for 2020>>, ECRI Institute, acceso el día 16 de noviembre del 2019, https://assets.ecri.org/PDF/White-Papers-and-Reports/ECRI-Top-10-Technology-Hazards-2020.pdf

[5] <<The Internet of Medical Things – Anticipating the Risk>>, ISACA, vol 4 (2019): 27-32

[6] <<Classify Your Medical Device>>, FDA, acceso el día 17 de noviembre del 2019, https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device