Dispositivos medicos: una mirada atrás

A lo largo de estas entradas hemos podido ver diferentes temas de interés relacionados con los dispositivos médicos, las redes a las que están conectados, su regulación en diferentes países y sobre todo, los riesgos que tenerlos supone.

No querría acabar esta serie de entradas sin hacer un pequeño inciso y mostraros en forma de timeline un par consecuencias asociadas a la mala gestión de este tipo de dispositivos. Así que antes de nada os dejo una pequeña 'evolución' de lo que han supuesto los dispositivos médicos.

Timeline

- **2008**

  Hack de un marca-pasos – Kevin Fu, UMass Amherst

- **2011**

  Hack de una bomba de insulina – Jerome Radcliffe, Black Hat Conference

- **2013**

  Descubrimiento de una serie de riesgos en multitud de dispositivos médicos como equipamiento de operaciones, dispositivos de anestesia, ventiladores, bombas de insulina, desfibriladores, monitores de constantes, equipamiento de laboratorio, etc. – Billy Rios, Security Researcher.

- **2014**

  Múltiples alertas de seguridad publicadas por el ICS-

CERT (U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team), el FBI, y la FDA (US Food and Drug Administration)

- **2015**

  TrapX y Protiviti publican una investigación demostrando que los dispositivos médicos son realmente explotados por cibercriminales como punto de entrada para acceder a la red del hospital y obtener información sensible de los pacientes.

- **2014 & 2016**

  Se publica la guía de seguridad de la FDA para la Presentación de Premercados y la Administración de Posventa

Viendo que esta clase de eventos son realmente posibles y pueden llegar a tener un gran impacto en la vida humana, y teniendo en cuenta el panorama actual, muchas empresas y compañías están empezando a adoptar nuevos paradigmas de gestión y control. Algunos de esos paradigmas son:

- **Normativas de tratamiento de datos seguros:**

  La creciente integración en la red de dispositivos médicos está conduciendo a nuevos riesgos para la seguridad de los pacientes. En octubre de 2014, la FDA publicó su famosa guía sobre: *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, seguido en enero de 2016 por *Postmarket Management of Cybersecurity in Medical Devices*. Estos documentos ayudan a identificar las cuestiones relacionadas con la ciberseguridad que los fabricantes deben tener en cuenta en el diseño y el desarrollo (premercado) de los dispositivos, así como la necesidad

de compartir y gestionar las vulnerabilidades de los dispositivos que circulan en el mercado.

- **Gestión del riesgo:**

  Reconociendo los riesgos de seguridad introducidos a través de vulnerabilidades de dispositivos médicos y para cumplir con las regulaciones regionales (por ejemplo, HIPAA para los EE.UU.), los proveedores de atención médica incluyen dispositivos médicos en sus análisis de riesgos de seguridad. La serie de normas ISO / IEC 80001 proporciona un marco específico para el ecosistema de dispositivos médicos mediante la definición de roles y responsabilidades como si de una matriz RACI se tratara.

- **Gestión del ciclo de vida:**

  Cada vez más, las organizaciones sanitarias están tomando medidas activas para proteger sus ecosistemas de dispositivos médicos contra las amenazas cibernéticas y los riesgos, tanto internos como externos. Como parte de sus procesos de evaluación de activos y riesgos, ahora segregan las redes de dispositivos médicos y supervisan los eventos de seguridad a nivel de red para tener un mayor control, minimizar la superficie de exposición y minimizar los riesgos en la medida de lo posible.

Por eso, con la influencia de todos estos nuevos paradigmas, el dispositivo medico cambia, evoluciona y pasa a ser algo mucho mas complejo, del que se necesita mayor supervisión, control y gestión. Como consecuencia todas las partes involucradas en el proceso de creación pasan a formar parte de un mismo todo, en el que cada una tiene un roll diferente, tal y como se puede apreciar, a continuación, en la imagen.

Minimizando los riesgos

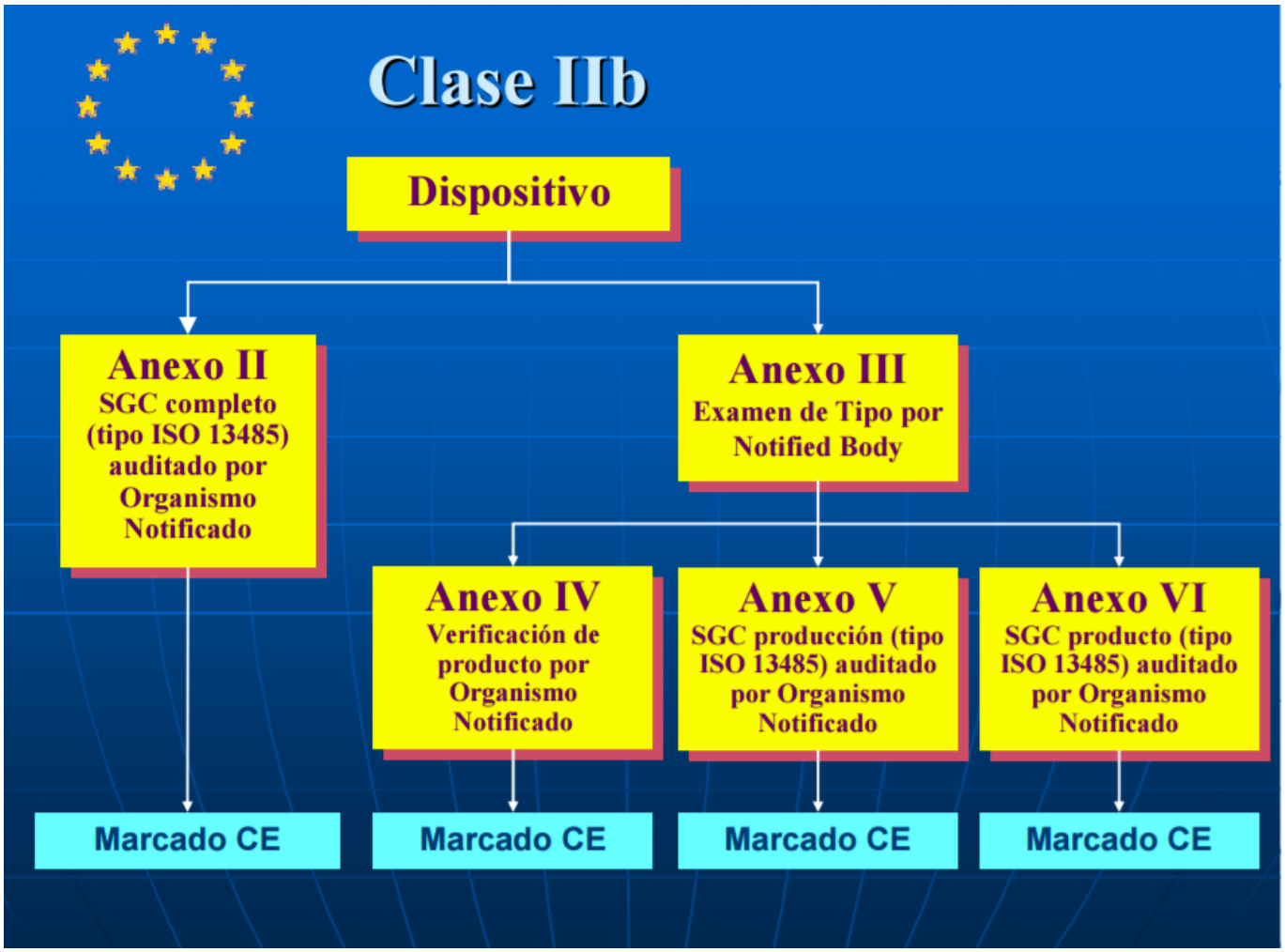
Una manera efectiva de minimizar los riesgos de un producto medico es a través de las normativas territoriales. En caso de cumplirlas, el producto tendrá menos riesgos que en caso de no cumplirlas. En el caso de la UE, un producto medico cumple con las normativas vigentes cuando tiene el documento de conformidad.

La declaración de conformidad CE es un documento que valida que un dispositivo medico:

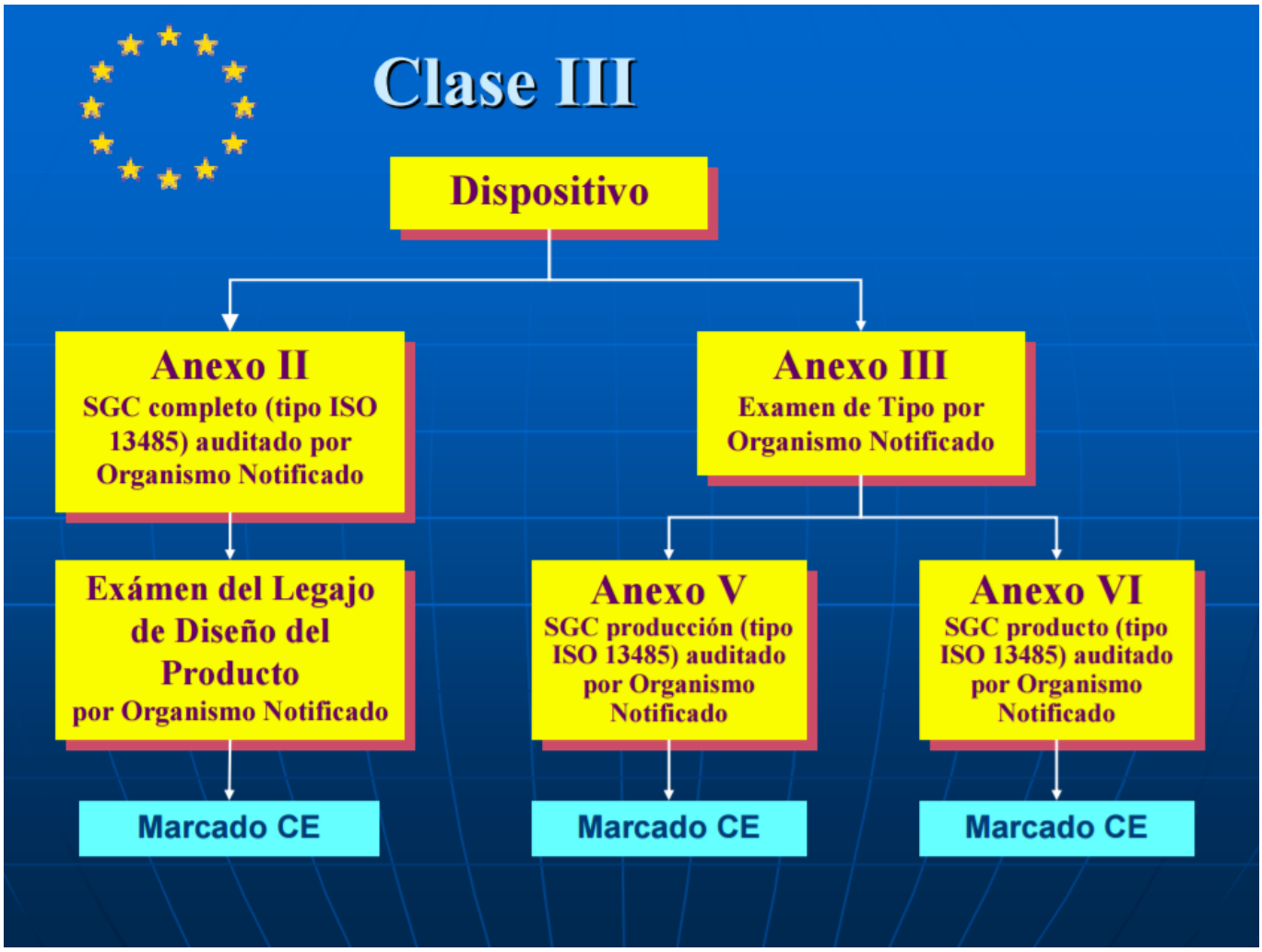
- Satisface las provisiones de la directiva.
- Existe un representante autorizado
- Existe un organismo notificado
- Se han aplicado los procedimientos de conformidad adecuados
- Se ha marcado el producto con la etiqueta ‘CE’

Existen diferentes procesos a llevar a cabo dependiendo del tipo de dispositivo medico sea, por lo que para no alargar la entrada, me centraré en los de clase dos y clase tres especialmente. Estas clases tienen un proceso de ‘*certificación CE*‘ similar que se puede ver, en las dos imágenes siguiente:

Proceso de certificación de un dispositivo de clase II



Proceso de certificación de un dispositivo de clase III



Con toda esta información podemos llevar a la conclusión que, el evitar los riesgos es una responsabilidad compartida. No solo se tiene que involucrar los fabricantes sino que ademas, las empresas que suministran los componentes, los centros que usan dichos dispositivos, los pacientes, los gobiernos, e incluso la sociedad.

Porque si algo falla, es un problema que nos afecta a todos.

Medical devices security risks

Referencias:

[1] **Security Challenges for Medical Devices**

http://cacm.acm.org/magazines/2015/4/184691-security-challenges-for-medical-devices/fulltext

[2] **Understanding ISO 14971 Medical Device Risk Management**

http://blog.greenlight.guru/iso-14971-medical-device-risk-management

[3] Symantec™ Industry Focus: Medical Device Security, https://www.symantec.com/content/dam/symantec/docs/data-sheets/symc-med-device-security-en.pdf