Impacto de una debilidad de ciberseguridad en la arquitectura de un sistema electromédico

Diego Coulombie[1], Agustín Reyes[1], Alberto Miguens[1]

[1] Dto de Ingeniería e Investigaciones Tecnológicas, Universidad Nacional de La Matanza
San Justo, Buenos Aires, Argentina
{dcoulombie, aireyes, amiguens}@unlam.edu.ar

Resumen. El diseño de un equipamiento médico dedicado al monitoreo de profundidad de anestesia, que utiliza conectividad en su arquitectura con el fin de hacer el monitoreo de forma remota, se ve perjudicado cuando se enfrenta a las amenazas de ciberseguridad en la etapa de análisis de riesgos. La imposibilidad de validar de manera objetiva las medidas de control por parte de la organización que lo diseña, obligó a mitigar el elevado riesgo ante ciber-ataques con la drástica solución de hacer un cambio de arquitectura y de modelo de negocio abandonando la posibilidad de conectividad remota.

Palabras clave: Aplicaciones de uso médico, Internet de las Cosas, Telemedicina, Análisis de riesgo, Requisitos regulatorios de seguridad y protección.

1 Introducción

A veces las cosas se complican. Aquello que en un boceto parece una idea maravillosa y revolucionaria se desarma cuando se enfrenta con la realidad. Incluso cuando se tomaron precauciones previas puede ocurrir que algo inesperado, que no se imaginó al momento del diseño, se revele ante nosotros como un problema. La envergadura del problema puede tener gran importancia según el campo de aplicación de esa idea. En áreas que se saben sensibles, los contextos en los que se practican los diseños están ordenados por regulaciones y por autoridades de control que se encargan de verificar su cumplimiento.

En el área de la tecnología médica las regulaciones no solo plantean requisitos sobre el producto final, sino que también exigen, controlan y evalúan las estructuras y metodologías destinadas al diseño. La mejor forma de satisfacer esas regulaciones es logrando el cumplimiento de normas específicas, definidas por la industria y aceptadas por los organismos de control.

El conjunto de normas aplicables depende de las características del producto. En particular nos enfocamos en el marco regulatorio que cubre al producto electromédico para monitorizar la profundidad de anestesia. El desarrollo hecho en el ámbito de la universidad en los proyectos “PICTO 0087 Monitor de profundidad de anestesia” y “C2-ING-061 Comunicación inalámbrica de baja energía para aplicaciones electromédicas” consta de un sistema de adquisición de neuroseñales inalámbrico (Fig.1, Cabezal) con una pantalla de monitorización (Fig.1, Monitor) dentro del área

de uso y otra interfaz remota (Fig.1, Aplicación). Se trata de un dispositivo médico de aplicación en quirófano y terapia intensiva [1].

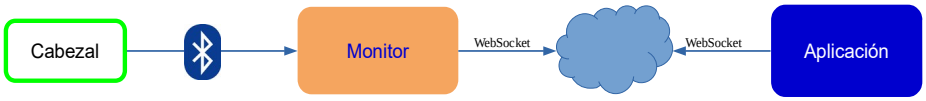

Fig. 1. Arquitectura del Monitor de profundidad de anestesia

El modelo de negocio al que responde esta arquitectura es el de telemedicina aplicada a un subsector de la salud en el que hay una dependencia absoluta del profesional de manera presencial. La anestesia en las intervenciones quirúrgicas y la sedación en terapia intensiva se hicieron durante muchas décadas mediante un profesional médico especializado en anestesiología. Este ajustaba la dosis para obtener el estado anestésico del paciente deseado, midiendo variables hemodinámicas como el ritmo cardíaco y la presión arterial; y parámetros clínicos como la sudoración, la piloerección, la dilatación de las pupilas, la sialorrea, y los movimientos espontáneos [2]. Hace unos cuantos años vienen usándose monitores de profundidad anestésica basados en parámetros objetivos que complementan la observación del profesional. Existen pocos fabricantes en el mundo. La mayoría usa señales electrofisiológicas que procesadas por un algoritmo propietario, dan un indicador dentro de una escala y registran los valores durante toda la maniobra anestésica con fines legales y de historia clínica [3].

La arquitectura propuesta con un “Cabezal” que registra y adecúa la señal junto a un “Monitor” con conectividad (que podría ser un Smartphone u otra plataforma con software embebido) permitirían sacar del área de quirófano al profesional de anestesia, para que actúe, verifique, avale, revise y registre de manera remota el efecto de la dosis suministrada al paciente. En un caso superador de telemedicina podría también ajustar la dosis de manera remota, si es que la mesa de anestesia lo permite

Considerando el producto electromédico descripto, el conjunto de normas aplicables para gestionar su seguridad y eficacia, abarca desde el sistema de gestión de calidad (ISO13485) [4], la gestión de riesgos (ISO 14971) [5], la de usabilidad (IEC 62366) [6], la del proceso del ciclo de vida del software (IEC 62304) [7], la de seguridad básica y funcionamiento esencial (IEC 60601-1, cuyo punto 14 se encarga del software del producto electro medico o PEMS) [8] y la de seguridad del software que puede funcionar autónomamente (IEC 82304-1) [9]. La relación entre estas normas y el producto se puede ver en la Fig. 2.

La gestión de riesgos es un estudio sistemático y predefinido hecho por el fabricante que busca conocer de antemano la mayor cantidad posible de los peligros que puedan afectar al usuario o paciente al entrar en contacto con el dispositivo médico. Atraviesa todo el ciclo de vida del producto, desde la concepción de la idea, las diferentes etapas del diseño, la producción, la posproducción, el uso, el mantenimiento y finaliza con la retirada del producto del mercado. Busca también que se valoren los peligros ponderándolos como riesgos para así poder justificar cual será la acción que se tomará con cada uno de ellos, con el fin de eliminarlos, mitigarlos o aceptarlos. La ISO 14971 brinda un marco de referencia y propone metodologías para abordar ese estudio sistemático para encontrar peligros, evaluar su gravedad y su probabilidad de ocurrencia, encontrando así riesgos. Requiere que el fabricante defina

criterios de aceptación o rechazo de esos riesgos, para definir cuales de ellos serán mitigados con soluciones técnicas que este proponga. La norma también establece requisitos de trazabilidad entre los peligros y entradas al diseño. La IEC 62304-1 establece el marco de responsabilidades, registro y verificación para cada una de las etapas del proceso del ciclo de vida del software, incluyendo obviamente las entradas de diseño que surgen de la gestión de riesgo y especialmente sobre como se trata la realimentación que brinda el proceso de resolución de problemas (bugs). Así como la norma de gestión de riesgos alimenta las entradas del proceso de diseño regido por la de ciclo de vida de software, la ISO 14971 se alimenta también de requisitos de seguridad y eficacia planteados por la IEC 60601-1 y la IEC 82604-1 que actúan como disparadores para el análisis de los riesgos. Estas normas son específicas de producto y proponen requisitos destinados a controlar peligros que están reconocidos por la industria.

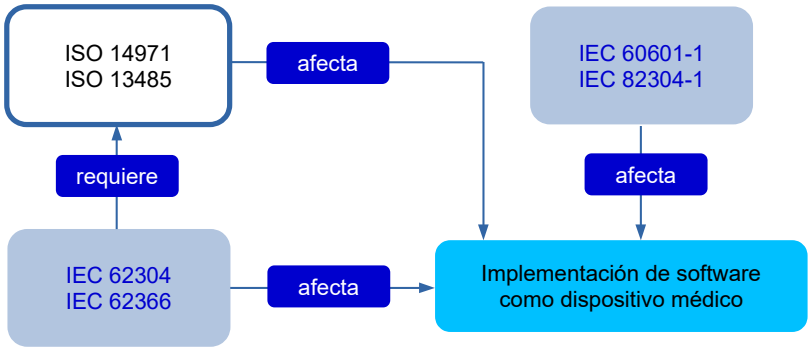

Fig. 2. Relaciones entre normas aplicables al producto, extraído y adaptado de IEC 62304-1 AMD:2015

Uno de esos peligros conocidos es la vulnerabilidad ante ataques a la ciberseguridad (Fig.3). Si bien es un elemento no definido en la norma de equipamiento médico [8] que se encarga estrictamente de los peligros relacionados con la seguridad (safety: prevención de accidentes sin intencionalidad), si se hace mención específica en la norma de software autónomo [9] considerando también como fuente de peligros a la amenaza proveniente de la falta de protección del dispositivo (security: prevención de actividades maliciosas intencionadas).

Fig. 3. Impacto de las medidas de protección en la seguridad, adaptado de TIR57 [10]

Esta diferencia que no era considerada hace unos años, hoy con el avance de la conectividad de los productos médicos hace que el problema de la ciberseguridad esté tomando cada vez mas relevancia [11]. Esto significa un cambio de paradigma en el enfoque de la gestión de riesgos, en donde transversalmente al diseño se debe considerar la protección del sistema como una entrada más al diseño.

El objetivo de este trabajo es mostrar cual fue el impacto que causó en la arquitectura de un sistema electromédico cuando en la gestión de riesgos se incorporaron herramientas de análisis de la ciberseguridad.

2 Métodos

Para hacer la gestión de riesgos de todo el producto médico se usó la herramienta Análisis Modal de Fallos y Efectos (AMFE) enunciándose aquí unicamente aquellos ítems relacionados con la ciberseguridad.

Las siguientes tablas establecen criterios para la aceptabilidad del riesgo. Las Tablas 1 y 2 dan una guía la valoración de la gravedad y la ocurrencia. La Tabla 3 establece los límites que definen cuando un riesgo es aceptable o cuando es inaceptable

Tabla 1. Guía para valoración de la Gravedad:

Gravedad	Consecuencias asociadas	Valor
Catastrófico	Origina la muerte del paciente	5
Crítico	Origina un deterioro permanente o una lesión que pone en peligro la vida	4
Serio	Origina una lesión o un deterioro que requiere intervención médica profesional	3
Pequeño	Origina una lesión temporal o un deterioro que no requiere intervención médica profesional	2
Insignificante	Inconveniente o molestia transitoria	1

Tabla 2. Guía para valoración de la Ocurrencia:

Probabilidad	Frecuencia del fallo	Valor
Frecuente	Fallo casi inevitable. Es seguro que el fallo se producirá frecuentemente.	5
Probable	El fallo se ha presentado con cierta frecuencia en el pasado en procesos similares o previos procesos que han fallado.	4
Ocasional	Defecto aparecido ocasionalmente en procesos similares o previos al actual. Probablemente aparecerá algunas veces en la vida del componente/sistema.	3
Remoto	Fallos aislados en procesos similares o casi idénticos. Es	2

	razonablemente esperable en la vida del sistema, aunque es poco probable que suceda.	
Improbable	Ningún fallo se asocia a procesos casi idénticos, ni se ha dado nunca en el pasado, pero es concebible.	1

Tabla 3. Guía para aceptar el Riesgo A = ADMISIBLE; I = INADMISIBLE:

Ocurrencia / Gravedad		Improbable 1	Remoto 2	Ocasional 3	Probable 4	Frecuente 5
Catastrófico	5	A	I	I	I	I
Crítico	4	A	A	I	I	I
Serio	3	A	A	I	I	I
Pequeño	2	A	A	A	I	I
Insignificante	1	A	A	A	A	I

Para la detección de los peligros se usó la técnica de análisis de situaciones relacionando los aspectos de uso de cada uno de los componentes del sistema y las amenazas de ciberseguridad a las que están expuestos. Estas amenazas pueden ser:

• Interrupción de la atención / servicio

• Engaño del personal con correo electrónico falso o sitios web falsos para obtener credenciales de inicio de sesión o instalar malware

• Amenaza interna, involuntaria o intencional, que puede representar una amenaza significativa debido a la posición de confianza dentro de la organización

• Pérdida de información del paciente

• Violación de datos, filtración de información y pérdida de privacidad

• Chantaje, extorsión y coacción a través de la explotación de datos filtrados.

El análisis permitió descubrir los peligros, y estos se registraron y sistematizaron como ítems en el AMFE de la sección resultados. De esta manera se identificó cual

es la secuencia de sucesos que desencadena una situación peligrosa causando un daño específico (columnas: Secuencia de sucesos, Situación peligrosa, Daño). También se ponderó el riesgo mediante las tablas 1, 2 y 3 antes mencionadas (columnas: O, G, R) y se propuso la medida de control que busca que el riesgo baje a niveles aceptables (columna: Mitigación). Como cada situación peligrosa debe ser trazable se la identificó alfa numericamente (columna: ID).

3 Resultados

Los resultados del análisis de riesgos y soluciones propuestas para mitigar los riesgos se enuncian en la Tabla 4 en el formato tradicional de un AMFE, aceptado por la industria y por los organismos regulatorios.

Se analizaron las secuencias de sucesos para ataques que logran modificar parámetros de funcionamiento, suplantan dispositivos y usuarios, detienen la acción del sistema, corrompen su funcionamiento y/o generan nuevas vulnerabilidades.

Los daños que responden a cada uno de los peligros detectados se circunscriben a la falta de monitorización tanto presencial como remota, a una posible dosificación incorrecta del agente anestésico y a la perdida de privacidad de los pacientes.

Se proponen las medidas de mitigación que buscan disminuir el riesgo mediante un blindaje del sistema minimizando las vías de conectividad lo que implica suprimir la aplicación remota. Las propuestas incluyen mejorar la protección de partes vitales del software impidiendo el acceso remoto, permitiendo solo el resguardo de datos de manera física y la ejecución de actualizaciones solo por personal autorizado. Las medidas de control también impactan en la selección del hardware donde ya no se permite la selección de una plataforma de uso general y se exige una plataforma de uso exclusivo para cumplir con la función de monitor.

Tabla 4. Extracto del AMFE con los ítems relacionados a la ciberseguridad con riesgo Inadmisible (I). MPA = Monitoreo de Profundidad Anestésica

ID	Secuencia de sucesos	Situación peligrosa	Daño	O	G	R	Mitigación
CS01	El monitor sufre un ataque que modifica parámetros de funcionamiento del cabezal	El cabezal interrumpe su transmisión	MPA no disponible	3	3	I	Desactivar conectividad monitor red externa. Protección contra escrituras y CRC de partes vitales. Resguardo de datos presencial (USB).Monitor en
CS02		El cabezal envía datos erróneos	Dosificación incorrecta de anestesia	2	5	I	

CS03	El monitor sufre un ataque que modifica sus propios parámetros de funcionamiento	El monitor genera e informa valores espurios al usuario local y/o al usurario remoto de la aplicación	Dosificación incorrecta de anestesia	2	5	I	plataforma exclusiva.
CS04	Suplantación de dispositivo cabezal por comunicación Bluetooth	El monitor recibe datos espurios interrumpiendo su funcionamiento	MPA no disponible	3	3	I	Identificación de cabezal encriptada periódica
CS05		El monitor recibe datos espurios y continúa funcionando	Dosificación incorrecta de anestesia	2	5	I	
CS06	Suplantación de dispositivo monitor	La aplicación recibe valores espurios	Dosificación incorrecta de anestesia	2	5	I	
CS07	Suplantación de usuario en aplicación remota	Un tercero toma control de la maniobra de dosificación	Dosificación incorrecta de anestesia	2	5	I	
CS08		Un tercero se apodera de la base de datos de pacientes.	Perdida de privacidad de pacientes	4	3	I	Suprimir la aplicación remota
CS09	La aplicación sufre un ataque	La aplicación no inicia, se desinstaló o muestra error.	MPA remoto disponible	4	3	I	
CS10		La aplicación muestra valores espurios	Dosificación incorrecta de anestesia	2	5	I	
CS11	Una actualización de alguna parte del sistema no controlada corrompe el funcionamiento o genera vulnerabilidades	El sistema queda fuera de funcionamiento	MPA no disponible	3	3	I	Permitir actualizaciones validadas del sistema solo de forma presencial en fábrica o por personal autorizado
CS12		El sistema queda vulnerable a ataques	MPA no disponible Dosificación incorrecta de anestesia	2	5	I	

4 Conclusiones

Las medidas para mitigar los peligros que surgen de los ciber-ataques, pueden parecer extremas a primera vista (Fig. 4). Todas las medidas de control no solo deben implementarse sino que también deben validarse. La validación de una solución muchas veces implica un esfuerzo mayor al de la implementación misma. Este motivo justifica lo radical de las soluciones planteadas que obligaron a abandonar el modelo de negocio de la telemedicina y blindaron al dispositivo de monitoreo de toda conexión externa.

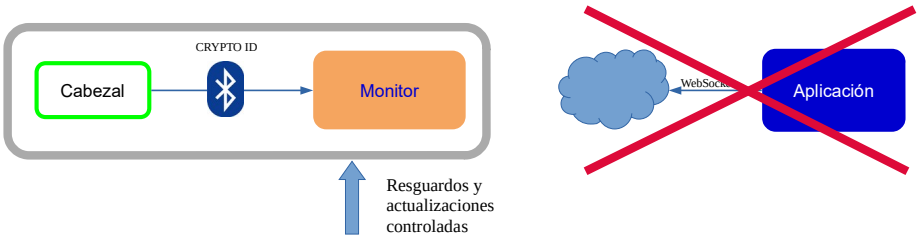

Fig. 4. Cambios en la Arquitectura del Monitor de profundidad de anestesia

Es importante destacar que no es imposible implementar y validar soluciones mejores. En este caso y en particular para la organización encargada de hacer el diseño, resultó estar muy por encima de sus posibilidades y recursos el hecho de proporcionar de manera objetiva evidencias que permitieran llevar adelante estrategias superadoras. Esta situación puede extenderse a muchos de los fabricantes de equipamiento médico tecnológico local que son PyMES [12]. Sus limitados recursos destinados al I+D+i están más inclinados a satisfacer los requisitos de funcionamiento y a mejorar las soluciones clínicas que a la protección de los sistemas. La incorporación de la ciberseguridad implica un cambio de paradigma donde más temprano que tarde los expertos en equipamiento médico deberán volverse también expertos en protección de sistemas médicos para hacer productos sostenibles en un mercado con cada vez más avidez de dispositivos conectados.

Referencias

1. D. Coulombie, F. Orthusteguy, A. Reyes, F. Ortalda. Monitor de Profundidad Anestésica , proyecto. Argentina. Buenos Aires. 2017. Libro. Artículo Breve. Workshop. WICC 2017 XIX Workshop de Investigadores en Ciencias de la Computación. Instituto Tecnológico de Buenos Aires.
2. Luis Miguel Torres Morera, “Tratado de anestesia y reanimación”, Madrid Arán cop. (2001)
3. J.Bruhn etal; “Depth of anaesthesia monitoring: what's available, what's validated and what's next?” British Journal of Anaesthesia,(2006), 97(1):85-94
4. ISO 13485:2016 Medical devices Quality management systems Requirements for regulatory purposes (2016)
5. ISO 14971:2019 Medical devices Application of risk management to medical devices

6. IEC 62366-1:2015 Medical devices Part 1: Application of usability engineering to medical devices.
7. IEC 62304:2006 Medical device software Software life cycle processes
8. IEC 60601-1:2005+AMD1:2012 CSV Consolidated version Medical electrical equipment Part 1: General requirements for basic safety and essential performance
9. IEC 82304-1:2016 Health software Part 1: General requirements for product safety
10. AAMI TIR57: 2016 Principles For Medical Device Security - Risk Management
11. Williams, Patricia & Woodward, Andrew. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical devices (Auckland, N.Z.). 8. 305-16. 10.2147/MDER.S50048.
12. F. Porta, G. Baruj, Nucleo Socio Productivo Estratégico Equipamiento Médico- Documento de Referencia, Argentina Innovadora 2020, 2012 Ministerio de Ciencia Tecnología e innovación productiva,