Los desafíos de la Ciberseguridad en la Tecnología Sanitaria

Introducción a la ciberseguridad en el entorno sanitario

La ciberseguridad es uno de los aspectos que más relevancia ha tenido en los últimos años en cuanto a la seguridad de los dispositivos y sistemas médicos, siendo un tema de vital importancia tanto para la seguridad del paciente y sus datos, como la continuidad de los servicios que los diferentes equipos y tecnologías sanitarias deben prestar. Se ha de considerar la implantación de buenas prácticas y un cambio de paradigma en las responsabilidades y relaciones de los diferentes actores implicados. La ciberseguridad hay que verla como un proceso con varias capas, y una forma de trabajar en sí misma, que involucra directamente a diferentes perfiles profesionales sanitarios. En estos nuevos planteamientos se requiere de una colaboración multidisciplinar, tanto de los centros sanitarios como de los fabricantes y proveedores de tecnología médica. Los diferentes servicios de Electromedicina e Ingeniería Clínica, los servicios TIC (Tecnologías de la Información y las Comunicaciones), los servicios técnicos de fabricantes y proveedores, y los profesionales sanitarios están implicados siendo corresponsables en cada ámbito de sus actuaciones.

En el entorno privado como el de la administración pública existen ya suficientes normativas legales que requieren se tome consciencia del alcance y la implantación de medidas en torno al problema de la ciberseguridad. Una síntesis y que nos guiarán a la hora de llevar a cabo los planes de seguridad y buenas prácticas, serían las siguientes:

- REGLAMENTO (UE) 2016/679 RGPD, Reglamento General de protección de Datos
- REGLAMENTO (UE) 2017/745 sobre los productos sanitarios
- ENS - Esquema Nacional de Seguridad normativa en el ámbito de la Administración Electrónica
- Norma UNE-EN 80001. Aplicación de la gestión del riesgo para las redes de tecnología de la información que incorporan dispositivos médicos.
- Normas UNE-ISO 27001 sobre Sistemas de Gestión de la Seguridad de la Información.

Básicamente todas estas normativas se basan en un concepto clave: la identificación del riego y su mitigación. Las normativas actualmente no nos van a indicar exactamente que de debemos hacer o qué medidas técnicas concretas aplicar. Nos orienta sobre qué debemos estudiar y cómo evaluar los riesgos, y en base a estos estudios implementar las medidas necesarias a cada uno de los riesgos identificados en base a su gravedad y probabilidad. Además, la normativa indica que la evaluación del riesgo ha de ser continua, durante toda la vida de uso del producto sanitario. Esto implica reevaluar periódicamente las condiciones técnicas y de uso del equipamiento, tanto por parte de los centros sanitarios como por los proveedores y fabricantes.

Las tendencias actuales son plantear medidas de seguridad aplicables para minimizar los riesgos, que conlleven pérdidas de información o fallos en la continuidad del servicio de los diferentes dispositivos y sistemas médicos, los cuales se encuentran interconectados entre sí mediante la red de comunicaciones, usando los mismos protocolos que se usan Internet y, por tanto, sometidos a los mismos problemas de ciberseguridad que aparecen allí. También es necesario cumplir los requerimientos legales en cuanto a la protección de la información de salud de los pacientes. Se plantea la necesidad de una seguridad integrada donde todos aquellos elementos de seguridad trabajen juntos, dotando a las redes de comunicación de la suficiente inteligencia para protegernos de las posibles amenazas de la seguridad. En el sector de la Electromedicina e Ingeniería Clínica tenemos que interiorizar y familiarizarnos con tecnologías para el cumplimiento de estándares de seguridad y cifrado, comunicaciones seguras, segmentación y perfiles de red, etc. Además de considerar retos potenciales como securizar sistemas y equipos más antiguos, o los más nuevos pero que aún no cuentan con las medidas de seguridad necesarias activas.

La problemática actual es que dentro de los centros hospitalarios existe una gran variedad de equipos y sistemas médicos conectados entre sí mediante una red de comunicaciones, más o menos segura, pero que requieren comunicarse con otros elementos internos o externos. Podemos decir que el protocolo de comunicación más utilizado es el TCP/IP, al igual que ocurre en Internet. Se habla del tándem Ethernet-TCP/IP como los protocolos universales para la interconexión de sistemas heterogéneos y de diferentes fabricantes. Por otro lado, cada vez más nos encontramos que los equipos médicos incorporan hardware y software comercial, junto a los elementos específicos de la tecnología médica.

Las dos tendencias indicadas han aportado beneficios en cuanto a la estandarización y reducción de costes dentro del ámbito de la globalización. Sin embargo, presentan unos riesgos añadidos debidos al uso de una tecnología común en el resto de los entornos tecnológicos. Tenemos que afrontar los problemas derivados de los protocolos en cuyo desarrollo inicial no fue la seguridad el objetivo prioritario. Los problemas que continuamente afectan a Internet pueden, en mayor o menor medida, repercutir en las redes internas de los Hospitales. En otro sentido, el uso de software comercial en los diferentes sistemas y equipos médicos presenta un riesgo por los posibles fallos de seguridad de este software comercial. Coinciden en la importancia de la ciberseguridad tanto la FDA como ECRI, que llevan los últimos años situándola a la cabeza de los riegos de seguridad. Básicamente nos encontramos con la proliferación de software no deseado malware (virus, gusanos, spyware, ramsonware, etc.) que puede ser propagado de forma no controlada en nuestras redes aprovechando las vulnerabilidades del software. Si a esto añadimos las dificultades que pueden surgir para mantener los equipos actualizados y con protección activa ante estas amenazas, debemos buscar soluciones que permitan proteger los equipos médicos sin perturbar su normal funcionamiento también para ataques intencionados.

Cambio del paradigma sobre los riesgos y la seguridad

En el concepto actual de seguridad se ha de plantear que es lo que queremos asegurar y de qué. Pensando en la seguridad como un concepto en el que interactúa la tecnología, con los procesos y procedimientos de trabajo, junto con el lado humano de toda actividad. De forma global la tecnología por sí sola no proporciona una seguridad total. Se habla en tecnología de la información que no existe ningún equipo o sistema totalmente seguro 100%, ya que siempre existirá un riesgo residual. De hecho, la definición de riesgo viene dado por las vulnerabilidades que presenten nuestros sistemas frente la amenaza que éstas puedan ser explotadas en la práctica. En esta época de pandemia debido al covid-19 un incidente de seguridad que produzca la indisponibilidad de los equipos, sistemas de diagnóstico, tratamiento o gestión clínica, es crítico. Debido a la covid-19 también se están implementando más equipos con acceso remoto para minimizar los riesgos de contacto y asistencia del paciente a pie de cama, introduciendo con ello nuevos elementos a controlar.

Cuando hablamos de equipos o sistemas médicos, la prioridad de la seguridad se ha de referir al paciente, tanto por la confidencialidad de sus datos como por el correcto funcionamiento de los equipos, y su repercusión sobre el paciente al que se le aplican. Si nos planteamos los perjuicios derivados de un fallo de seguridad causante de una avería de un equipo, hay que tener en cuenta distintos aspectos. En primer lugar, la integridad física del paciente debido al fallo, o la integridad y confidencialidad de los datos de este. En segundo lugar, las responsabilidades legales derivadas del incidente de seguridad en relación con lo anterior. Y, en tercer lugar, los costes planteados para solucionar la avería ocasionada, así como el tiempo de inactividad del equipo. Además de todo lo anterior, tampoco hay que olvidar la posibilidad de que el problema de seguridad se traslade al resto de equipos conectados a la red, aunque esta se suponga una red segura en sí misma.

Uno de los problemas de la seguridad en general es la falta de recursos o inversiones en medios para garantizarla. Sin duda, las inversiones en seguridad se ven como un gasto sin resultados aparentes en lugar de una inversión. Un gestor que analiza los costes espera obtener algún tipo de beneficio, no necesariamente económico, que sea visible. En seguridad se invierte en algo a priori intangible, y de lo que no se dispone de garantías 100% de ausencia de problemas. Actualmente la pregunta no es si vamos a sufrir un incidente de seguridad o no, sino en que momento lo sufriremos, y si en ese momento estaremos preparados para mitigarlo y reponernos al incidente. Aquí es cuando aparece el concepto de resiliencia que es lo que debemos buscar. Por todo esto, muchas veces la inversión en seguridad se ve como un gasto no prioritario ya que no se tienen en cuenta las repercusiones anteriormente comentadas.

Si el objetivo que se plantea es poder garantizar el correcto funcionamiento de los equipos y sistemas médicos de forma segura, se debe implementar una seguridad a distintos niveles, y de forma integrada. La integración se ha de llevar a cabo desde los elementos a nivel más bajo en los propios equipos médicos, tales como los antivirus o cortafuegos, hasta los sistemas de detección de intrusos y la inteligencia de la red de comunicaciones. Los desarrollos actuales nos llevan a confiar en la seguridad proactiva de las redes, mediante el uso de tecnología de redes inteligentes y seguras

El cumplimiento de las normativas legales vigentes nos obliga a extremar las medidas de seguridad, desde el simple control del acceso físico, hasta el almacenamiento y transmisión electrónica de los datos médicos. Como punto relevante tendríamos el tratamiento que se da los datos de salud cómo de "*máximo nivel de seguridad*". Esto implica que las medidas para garantizar la confidencialidad e integridad de los datos pasan por implementar métodos de control, registro, y cifrado de la transmisión y almacenamiento de la información, debiéndose realizar los análisis de riesgos y las medidas a aplicar que deben trasladarse a un "*Documento de seguridad*" donde queden reflejados los procedimientos y tecnologías utilizadas.

Si analizamos lo expuesto anteriormente entenderemos que el simple hecho de que un equipo médico esté conectado a una red supone ya un riesgo en cuanto a la seguridad. Esto es debido al hecho de que muchas veces los sistemas operativos y el software comercial instalado en los equipos pueden presentar vulnerabilidades, cuyas actualizaciones para corregirlos no han sido instaladas, o bien aún no existen. Las causas de que no estén instaladas las actualizaciones y correcciones pueden ser varias, desde que no estén validadas por el fabricante, que no sean compatibles con otro software, o incluso que se desconozca que son necesarias. Podemos incluir entre las vulnerabilidades posibles a determinados servicios del sistema operativo, como un servicio de correo electrónico o servicios Web, múltiples servicios software que no siendo necesarios para el funcionamiento del equipo se encuentren activados. Si además, por problemas de rendimiento o compatibilidad, no contamos con elementos de seguridad activa o pasiva en los propios equipos, como el antivirus o cortafuegos (firewall), la seguridad de los equipos y sistemas médicos puede quedar seriamente comprometida.

Adopción de medidas proactivas

Los centros sanitarios tienen que ser conscientes de los riesgos y fallos de seguridad de las redes y sistemas en funcionamiento, por lo que el realizar una auditoría de seguridad parece el primer paso razonable para detectar los principales puntos a proteger, basado como se ha expuesto en los análisis de riesgos que nos orientan en las diferentes normativas. Se ha de documentar la vulnerabilidad potencial de cada equipo y plantearnos la necesidad de un cambio de mentalidad respecto a la actualización continua del software de los sistemas médicos, considerando los problemas técnicos que esto conlleva. Siendo éste un punto importante todavía no asumido por muchos proveedores y fabricantes de tecnología médica.

Hay que destacar que la responsabilidad del correcto funcionamiento de los equipos y sistemas médicos durante su vida útil es compartida entre los fabricantes y el titular de la tecnología médica. Un problema adicional que se nos plantea es que la vida media del hardware y software comercial es menor a la vida de un equipo médico, por lo que el soporte y mantenimiento del fabricante original del

software puede dejar de estar disponible antes de tiempo. La aplicación de actualizaciones o instalaciones de software de seguridad debe ser aprobada por los fabricantes, que a su vez han utilizado hardware/software comercial de otro fabricante. Este proceso de aprobación es lo que conocemos como la validación, y que generalmente está llevando demasiado tiempo en relación al riesgo que se asume. La pregunta es, ¿en qué puntos podemos actuar para mantener seguros nuestros entornos externamente a los equipos y sistemas médicos?

Las redes tradicionales donde todos los equipos pueden realizar conexiones entre ellos, y donde la seguridad se controla solo en determinado punto como la conexión a Internet o hacia otra red, son ineficientes e inseguras. La denominada seguridad del perímetro ya no es válida y hay que ofrecer alternativas como la aplicación de tecnologías de redes seguras con la conjunción de diferentes elementos como VLAN (redes locales virtuales), cifrado con protocolos seguros como IPSec, o SSL, Infraestructuras de clave pública PKI mediante certificados digitales, protocolos de autentificación como 802.1x, electrónica de red con elementos activos de seguridad, etc. Pero todo esto nos lleva a lo que actualmente se conoce como la segmentación de la red y su uso basado en perfiles.

Es evidente que la proliferación de virus o software maliciosos en general denominado *malware* plantea riesgos importantes, sobre todo teniendo en cuenta que muchos de ellos aprovechan las vulnerabilidades de los servicios de red para infectar o atacar a los diferentes equipos y sistemas médicos como lo hacen con el resto de máquinas de la red, de forma automática y autónoma sin intervención de los usuarios. Con el tiempo estamos viendo el cambio de mentalidad sobre la importancia de mantener actualizado el software y de las posibilidades de ataques reales a los sistemas. Principalmente en el ámbito general los ramsonware han concienciado a mucha gente, y de igual aplicación al ámbito de la sanidad, donde a todos nos suena el impacto del *WannaCry*.

Hay que destacar que, aunque una gran parte del software malicioso afecta a sistemas Windows, no implica que otros sistemas como Linux o Mac sean más seguros. De hecho, se descubren fallos de seguridad tan graves como en Windows, pero con la ventaja de que las amenazas para estos sistemas suelen ser algo menores. Además de afectar a los Sistemas Operativos, los virus también aprovechan los fallos del software de aplicación como bases de datos, exploradores Web, aplicaciones de correo electrónico, etc. Se refleja por tanto la importancia de no activar servicios innecesarios que puedan suponer un agujero de seguridad en nuestros sistemas y equipos médicos. Ante todos estos problemas planteados la industria ha aumentado los esfuerzos en definir métodos y guías de trabajo para paliar los problemas evidenciados. Hace años que iniciaron la colaboración a nivel mundial, mediante grupos de trabajo de las asociaciones de fabricantes de sistemas médicos de Estados Unidos (NEMA), Europa (COCIR) y Japón (JIRA) en relación a los temas de ciberseguridad. Como representante de España en COCIR (European Coordination Committee of the Radiological and Electromedical Industry) contamos con FENIN (Federación Española de Empresas de Tecnología Sanitaria).

La seguridad de la conexión a la red interna, y con otras redes de la misma organización o externas (internet), como por ejemplo los propios proveedores con soporte remoto plantean riesgos y retos a resolver. La tendencia actual es aplicar una correcta gestión de la red local interna, intentando que todas las medidas de seguridad estén integradas trabajando en colaboración unas con otras. Se ha de buscar la integración sobre todo encaminada a la mayor efectividad posible y la gestión centralizada de todos los elementos de seguridad, desde las aplicaciones hasta la electrónica de red. Una gestión de red integrada pretende tener un control total desde el punto físico del cable de red, pasando por los puntos de acceso en la electrónica de red, hasta llegar a los niveles de aplicación de cada equipo y dispositivo médico.

Conclusiones sobre la ciberseguridad y el uso de redes inteligentes

La aplicación de las diferentes tecnologías, conjugadas con una correcta gestión de los procedimientos de trabajo y el control de accesos, nos va a permitir realizar redes con mayor seguridad. Por tanto, la redes inteligentes y seguras son el mejor medio de mitigar algunos de los problemas de ciberseguridad. Pero todo esto requiere una colaboración y esfuerzo conjunto de fabricantes, los profesionales de la Electromedicina e Ingeniería Clínica, el personal TIC y los profesionales sanitarios mediante equipos interdisciplinares.

La Inteligencia de las redes de comunicaciones seguras aprovecha todas las soluciones existentes de seguridad y las características intrínsecas de la electrónica de red para que ésta se convierta en el punto de integración de todas las tecnologías de seguridad. Utilizando la red como primer punto de aplicación de la seguridad podemos anticiparnos a las amenazas antes de se conviertan en un problema, eliminando riesgos innecesarios, y simplificando la gestión de la seguridad. Los principales fabricantes de equipos activos de red han apostado fuertemente por el desarrollo de tecnologías de seguridad proactivas en la red. En realidad, hoy no se comercializan equipos de red sino soluciones de red donde los componentes de seguridad son el elemento diferenciador.

Las redes inteligentes se adaptan de forma dinámica a los usuarios (equipos y sistemas) en función de la identidad y el contexto, y actúan respondiendo de forma automática y eficaz ante cualquier cambio del entorno. La seguridad se maneja de igual forma para los riesgos internos y externos protegiendo las comunicaciones extremo a extremo. En función de la combinación de los diferentes parámetros se pueden aplicar dinámicamente políticas muy granulares que permitan prevenir el problema antes de que ocurra, anticipándose a un incidente. Los usuarios solo acceden a los servicios y recursos que necesiten en cada momento en función de su necesidad. Por ejemplo, un CT que sólo precisa de la comunicación con el sistema PACS y estaciones de reconstrucción, podría limitarse en la red las comunicaciones exclusivamente a esos elementos impidiendo cualquier otra no contemplada. Para definir estas políticas se requiere que el fabricante defina los servicios necesarios y los detalles técnicos de cada dispositivo, los servicios de Electromedicina deben definir las funcionalidades y uso, acorde a las necesidades demandadas y en colaboración multidisciplinar, según cada organización sanitaria.

En el caso de un incidente, las soluciones de redes inteligentes (y seguras) son capaces de detectar de forma automática el problema concreto, el punto donde se origina el problema, el usuario que está originando el problema, de tal manera que se puede aislar al causante en el punto exacto donde se conecta a la red. De esta forma se puede reaccionar eficazmente y sin afectar a otros usuarios ni al funcionamiento de otros dispositivos médicos en la red. Son soluciones de redes que previenen los problemas, y se adaptan reaccionando eficazmente y de manera automática ante las condiciones cambiantes del entorno. Cada día los riesgos relativos a la seguridad de los equipos y sistemas médicos aumentan debido a los problemas derivados de las redes de datos a los que se conectan. Asimismo, las diferentes normativas legales obligan a cumplir unos requerimientos de seguridad que en el caso de los equipos médicos es del nivel más alto. Los fabricantes han de dedicar esfuerzos a implementar y desarrollar mecanismos de seguridad compatibles, que permitan operar de manera confiable y segura durante toda la vida del producto.

Adicionalmente podemos buscar soluciones externas a los sistemas y equipos médicos que proporcionen la seguridad deseada sin perturbar el correcto funcionamiento de los mismos, y que garanticen la seguridad de los pacientes en todos los aspectos. Para esto tenemos que hacer uso de las últimas tecnologías disponibles en seguridad, sin olvidar los otros factores implicados no dependientes de una u otra tecnología. Hay fabricantes que cuentan con productos para securizar un dispositivo o sistema médico permitiendo únicamente la comunicación segura con los otros elementos predefinidos. La incorporación de inteligencia a las redes, el control de las comunicaciones y la monitorización del tráfico de datos entre los diferentes componentes de la red de una forma granular nos va a permitir proteger los equipos y sistemas médicos de una forma más eficaz y segura. De hecho, un elemento que aparece cada vez más en las contrataciones, requerido en los pliegos técnicos, son elementos referentes a seguridad, donde se solicita al proveedor proporcione determinados elementos de seguridad. Bien internamente en el propio equipo o con productos externos.

Finalmente indicar que hay que tener presente el factor humano en el contexto de la seguridad, así como el cambio de mentalidad en la necesidad de invertir en sistemas de seguridad y gestión de redes. La seguridad debe ser conocida y para su evaluación se requiere hacer un estudio de riesgos y medidas a aplicar, algo que es responsabilidad de todos los actores que intervienen en un dispositivo o sistema médico: desde su fabricación hasta su retirada al fin de su vida útil. Aspectos que ya en 2021 serán obligatorios por las diferentes normativas en vigor.

Referencias

[1] RGPD (Reglamento general de protección de datos) - REGLAMENTO (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos www.boe.es/doue/2016/119/L00001-00088.pdf

[2] REGLAMENTO (UE) 2017/745 sobre los productos sanitarios. www.boe.es/doue/2017/117/L00001-00175.pdf

[3] ENS - Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010 que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/eli/es/rd/2015/10/23/951

[4] ENS - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/eli/es/rd/2010/01/08/3

[5] CN-CERT Centro Criptológico Nacional. Guías sobre el Esquema Nacional de Seguridad. www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

[6] UNE-EN 80001-1:2012. Aplicación de la gestión del riesgo para las redes de tecnología de la información que incorporan dispositivos médicos. Parte 1: Funciones, responsabilidades y actividades. www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0050043

[7] Normas UNE relacionadas con aplicaciones de las tecnologías de la información en la sanidad. www.une.org/encuentra-tu-norma/busca-tu-norma/?k=(i:3524080)

[8] Ciberseguridad con ISO 27001. www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058428

[9] IEEE 1073 Point of Care Medical Device Communication Standards, www.ieee.org

[10] HealthCare IT News, www.healthcareitnews.com

[11] Agencia Española de Protección de Datos, www.agpd.es

[12] COCIR (European Coordination Committee of the Radiological and Electromedical Industry) www.cocir.org

[13] ECRI Institute, www.ecri.org

[14] FDA (Food and Drug Administration), www.fda.gov

[15] JIRA (Japan Industries Association of Radiological Systems), www.medis.or.jp

[16] NEMA Association of Electrical Equipment and Medical Imaging Manufacturers, www.nema.org

[17] FENIN (Federación Española de Empresas de Tecnología Sanitaria), www.fenin.es

[18] SEEIC (Sociedad Española de Electromedicina e Ingeniería Clínica), ww.seeic.org

José Ángel Hernández Armas
Tesorero de la SEEIC - Sociedad Española de Electromedicina e Ingeniería Clínica
Vocal del COITTCAN y vicepresidente de ACITICS
Jefe de Ingeniería de Telecomunicaciones y Telemática del Hospital Universitario de Canarias
jherarmy@gobiernodecanarias.org

SEEIC, julio de 2020.