ANEXO VI PPT

SERVICIO DE CIBERSEGURIDAD

13.1. INTRODUCCIÓN

Se entiende por Servicio de Ciberseguridad los elementos y normas que permiten la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, que garantizan la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos proporcionados por los sistemas de tecnologías de información o de operación según su ámbito de aplicación.

Todos los trabajos a realizar en esta materia se deben aprobar por Organismos y Servicios responsables de la ciberseguridad en el ámbito de la Junta de Andalucía y la Unidad, Sección o Servicio de Electromedicina de cada Centro Directivo. No se podrá realizar ninguna acción si no están aprobados por ambos estamentos.

Dentro del entorno hospitalario en lo referente a los servicios que usan comunicaciones a través de redes IP, entendemos que se encuentran los siguientes:

- Red de equipos electromédicos: esta red involucra a los equipos de máquinas diagnósticas, monitorización de pacientes y máquinas médicas tales como respiradores, bombas de medicamentos, etc.
- Red de equipos IT: esta red involucra los ordenadores, tablets, servidores, impresoras etc necesarios para la gestión de la información dentro del centro.
- Red de confort: esta red involucra equipos tales como televisiones que usen IPTV, tabletas, terminales de cama, telefonía, interfonía y WiFi de cortesía.
- Red de gobierno del edificio: esta red involucra los equipos que controlan ascensores, luminarias, alarmas, puertas, bombas de agua, sistemas de calefacción y aire acondicionado, etc. Esto es todos los mecanismos de gobierno del edificio.

Es una práctica recomendable de seguridad dado que estas redes tienen requisitos distintos de calidad de servicio, equipos conectados, protocolos utilizados, criticidad del servicio, etc. que estas redes estén separadas físicamente o en su defecto estén separadas lógicamente.

En el presente documento se va a tratar la manera de aportar ciberseguridad a la red de equipos electromédicos. Es decir, seguridad dentro de la red de comunicaciones. Queda fuera del alcance de este documento prácticas relacionadas con la seguridad física de los activos. Esto es, prácticas como evitar que personas ajenas puedan acceder físicamente a los activos o electrónica de red, puedan acceder a la alimentación de los equipos o la electrónica de red o al acondicionamiento (sistemas de HVAC) de los mismos.

13.2. SEGURIDAD DE LOS EQUIPOS ELECTROMÉDICOS

La red de equipos electromédicos se considera una red crítica por los siguientes motivos:

- La información de las máquinas diagnósticas es información confidencial protegidas por la normativa sobre protección de datos personales.
- Los equipos electromédicos dada su naturaleza y función pueden ser soporte vital para los pacientes que hacen uso de las mismas por lo que la alteración de su funcionamiento o de los datos de las pruebas puede tener consecuencias catastróficas.

Para poder aportar seguridad a la red de equipos electromédicos es necesario el implantar una política de seguridad que busque cubrir las necesidades de identificar, proteger, detectar, responder y recuperar incluyendo trabajos de instalación y mantenimiento de las medidas necesarias para ello.

Estos principios deberán seguir los criterios de minimizar la superficie de exposición, el bastionado y minimización de privilegios.

Por último, dada la criticidad de la red, las soluciones aportadas no deben afectar bajo ningún concepto al desempeño de la red. Esto es, han de ser pasivas y por tanto no pueden inyectar tráfico a la red de equipos electromédicos.

13.3. CARACTERÍSTICAS DE LA SOLUCIÓN

Dadas las necesidades del presente proyecto y en relación a las políticas de seguridad anteriormente definidas, a continuación se detallarán en cada punto los requisitos mínimos que debe cumplir la solución:

Identificar

La solución debe ser capaz de identificar tanto los dispositivos dentro de la red de equipos electromédicos como los protocolos que se utilicen y las vulnerabilidades que éstos puedan tener. Asimismo la solución debe ser capaz de dibujar un mapa de red mostrando qué dispositivos se comunican unos con otros, con qué uso de ancho de banda y usando qué protocolo.

Proteger

Dada la imposibilidad de poder instalar soluciones típicas de seguridad tales como antivirus o EDR en los equipos electromédicos, la seguridad a estos equipos debe darse desde la red.

Para ello se seguirán políticas de minimización la superficie de exposición permitiendo que únicamente los equipos electromédicos se comuniquen con los equipos mínimos indispensables, políticas de bastionado en donde los equipos médico tendrán habilitados los protocolos y aplicaciones mínimos e indispensables para su funcionamiento y para la protección se deberán aplicar soluciones de tipo "parcheado virtual" utilizando equipos tales como un cortafuegos (NGFW) o un sistema de prevención de intrusos (IPS).

Detectar

La solución propuesta deberá ser capaz de detectar amenazas o ataques que se estén produciendo dentro de la red de equipos electromédicos así como conexiones nuevas a la red, no inventariadas o autorizadas.

Responder

Una vez se ha detectado un ataque, una amenaza o una conexión no autorizada, la solución propuesta debe ser capaz de actuar sobre las mismas ya sea aislando la amenaza o conexión, cortando la comunicación o deshabilitando la misma.

Recuperar

La solución propuesta debe poder facilitar actividades de recuperación una vez un ataque o una amenaza haya podido tener éxito. Por tanto, la solución debe poder facilitar información del estado de la red y los equipos para una futura recuperación restaurando los equipos de una solución de backup.

13.4. ARQUITECTURA DE LA SOLUCIÓN

Para poder dar servicio y cumpliendo los requisitos anteriormente indicados la arquitectura de la solución deberá cumplir los siguientes puntos:

- La solución propuesta no deberá interferir en el tráfico de producción de la red de equipos electromédicos. Por consiguiente, no se contemplan soluciones que inyecten tráfico en la red como puedan ser consultas a los equipos tipo ICMP, nmap, ssh, wmi o similares.
- Para la captura de información de la red de equipos electromédicos se podrán utilizar prácticas como la inclusión en la red de equipos TAP o el uso de puertos de SPAN o espejo. Esta captura de información deberá ser gestionada "fuera de banda" esto es, deberá crearse una infraestructura paralela para la gestión de esta información.
- La solución debe ser capaz de identificar y reconocer los activos dentro de la red de equipos electromédicos además de poder detectar comportamientos anómalos.

- Asimismo, la solución planteada deberá permitir conexiones remotas para la gestión y mantenimiento de la misma.

13.5. TRABAJOS DE MANTENIMIENTO Y ALCANCE

Los trabajos de mantenimiento de los dispositivos electromédicos deberán incluir capacidades de implementación de políticas de ciberseguridad, enfocadas a la reducción del riesgo de incidentes de seguridad por acceso no autorizado a información sensible o disrupción de la actividad asistencial de la infraestructura, permitiendo maximizar la disponibilidad del servicio.

Esto se concreta en la definición, mantenimiento y evolución de una política de ciberseguridad que ha de trabajar principalmente en la obtención de una segmentación de red adecuada a la actividad clínica, que permita una distribución eficiente de los dispositivos de electromedicina y su consiguiente mantenimiento y gestión. Para ello, se deberá trabajar en 4 líneas principales:

1. Inventario de activos:
    - ¿Qué hay conectado a la red?
    - ¿Qué tipos/familias de dispositivos?
    - ¿Qué versiones de OS o firmware?
    - ¿Qué tipo de aplicaciones?
    - ¿Qué capacidades de conexión se están utilizando?
    - ¿Qué hace cada dispositivo (función de negocio)?
    - ¿Cuál debe ser la ubicación de cada dispositivo?
2. Contexto clínico del tráfico entre activos:
    - ¿Cuáles son los flujos de interacción entre dispositivos?
    - ¿Qué protocolos de comunicación se están utilizando? ¿Son necesarios?
    - ¿Qué función clínica tiene cada flujo de interacción entre dispositivos?
    - ¿Cuál es la definición teórica de la función de cada dispositivo identificado?
3. Generación de una política de seguridad:

- Generación de una política de segmentación desde el punto de vista de la seguridad *"clinically driven"*, que esté alineada con la definida a nivel global en el entorno hospitalario correspondiente.
- Análisis en tiempo real de la evolución de la implementación de la segmentación y del estado de la red actual.

4. Definición de modelos de integración posible con sistemas SIEM, NAC y FW específicos del entorno IoMT/IoT así como sistemas de gestión de equipos médicos para inventariado, en línea con los requisitos de segmentación antes identificados.

En consecuencia, para asegurar una adecuada implementación de una política de ciberseguridad, se deberá gestionar un modelo de gestión de dispositivos electromédicos ("*asset management*"), que incluya políticas para:

1. Adquisición y registro.
2. Despliegue y uso.
3. Mantenimiento.
4. Retirada y gestión de la obsolescencia.

Estas políticas deberán dar respuesta, al menos, a cuestiones como:

1. ¿Qué sistemas de gestión GMAO o CMMS (*Computerized Maintenance Management System*) se usarán para seguimiento de dispositivos y mantenimiento preventivo?
2. ¿Cómo implementará esta CMMS o GMAO una política de actualización de dispositivos de direccionamiento dinámico?
3. ¿Cómo se gestionarán los registros médicos generados por los dispositivos?
4. ¿Cómo se coordinará el esfuerzo operativo de gestión de la CMSS y GMAO corporativo?
5. ¿Cuál será la política de evolución de la planta de dispositivos?
6. Identificación y notificación de vulnerabilidades en la infraestructura de dispositivos electromédicos.
7. Procesos y protocolos de remediación de vulnerabilidades y parcheo (real o virtual), tanto iniciales como posteriormente identificadas.
8. Definición de política de gestión del riesgo.

El contratista deberá prever estos trabajos y contar con personal formado y disponible para realizar trabajos de intervención en las actuaciones relacionadas con este servicio, a la vez que capacidad de realizar trabajos de ingeniería en vías de realizar la consultoría y

auditoria previa y posterior (trabajos preventivos y reactivos) en las materias de ciberseguridad que sean necesarias.

13.6. DESARROLLO DE LA SOLUCIÓN

Desde la Unidad, Sección o Servicio de Electromedicina se seguirán todas las recomendaciones y actuaciones dictadas desde los Organismos y Servicios responsables de la ciberseguridad en el ámbito de la Junta de Andalucía y particularmente en el SAS, en el que como referencia podemos nombrar:

- Andalucía CERT.
- Unidad de Seguridad TIC del SAS.

Los principios básicos, los requisitos mínimos y las medidas de seguridad a implantar en los sistemas de información de las Administraciones públicas se recogen en el Esquema Nacional de Seguridad (ENS), principal referente desde 2010 de la ciberseguridad en el ámbito público. La Junta de Andalucía alinea sus actuaciones con lo dictado por el ENS y las particulariza en la Política de Seguridad TIC, publicada en 2011 y actualizada en 2017, y en sus órdenes y resoluciones de desarrollo. La normativa reguladora en el ámbito de las tecnologías de la información se encuentra ya regulada en el ANEXO DE CONDICIONES TIC de este pliego, las cuales armonizan todos los requisitos normativos a cumplir. Igualmente estas normativas pueden ser ampliadas o sustituidas por normativas de ámbito superior y de aplicación a los Organismos de la Junta de Andalucía y en particular al SAS, siendo de aplicación a este contrato.

Estas actuaciones comprenderán tanto acciones correctivas como preventivas, entre las que podemos enumerar:

Acciones Correctivas:

- Incidentes de seguridad tecnológica relacionados con código dañino, fraude e intrusiones.
- Avisos y alertas de seguridad.

Acciones Preventivas:

- Análisis de vulnerabilidades
- Implantación de recomendaciones sobre políticas de seguridad TIC y análisis de riesgos en equipos o sistemas electromédicos.

Estos requisitos exigirán una mayor dedicación de recursos y de medidas organizativas adecuadas que den soporte a este escenario tecnológico por parte de la empresa contratista, la cual tendrá que ser dimensionada y valorada en la oferta adecuadamente.

Para calcular el impacto en el proyecto, podemos indicar a modo de referencia lo tipos de equipos electromédicos susceptibles de conexión a algún sistema de información o de generación de información digital que pueda ser tratada en una estación de trabajo.

A título indicativo del listado de tipos de equipos que se podrían mantener:

Electrocardiógrafo, Ecográfo, Radiología computerizada, Tomografía computerizada, Torax Digital, Radiografia digital, senógrafo, Resonancia magnética, Gammacamara, PET, Telemando, Dicomizador, Angiógrafo, polígrafo, Holter, oxímetro, coagulómetro, pulsioxímetro, monitor multiparamétrico, dermatoscopio, torre de endoscopia, videoendoscopio, videocolonoscopio, videogastroscopio, mediastinoscopio, videomediastinoscopio, fibroscopio, videolaparoscopio, torre de laparoscopia, videoprocesador, torre de videoendoscopia, Polo Anterior (Lámpara de Hendidura), Retinógrafo, Microscopios, Frontocómetro, Refractoqueratómetro, fibronasolaringoscopio, otoscopio, estroboscopio (fuente de luz fría), audimetría, impedanciometría, pruebas vesticulares, pruebas calóricas, potenciales evocados, colposcopio, equipo de videoendoscopia urológica, equipo de laparoscopia, video grabador, nefroscopio hopkins, uretero-renoscopio, visualizador 3d, videoprocesador, citoscopio, equipo de videoendoscopia urológica, ureteroscopio flexible

El número mínimo de equipos a mantener bajo ciberseguridad será de 500 equipos,