Ciberseguridad en Infraestructuras y Dispositivos Sanitarios

Trabajo de Fin de Máster

Autor: Rayco Manuel Monzón Castillo – raycomc@uoc.edu

Concepto: TFM del Máster de Ciberseguridad y Privacidad

Tutor: Jorge Chinea López

Profesor: Victor Garcia Font

Fecha: 29/12/2022

A todos mis maestros y profesores, por su provechosa labor social, desinteresada implicación y virtuosa vocación. En especial, a mi tutor, Jorge Chinea, por su exquisito trato, apoyo constante y dadivosa motivación.

A mis familiares y amigos, por su generoso afecto, valiosa compañía e inestimable sustento humano.

A mis colegas del sector de la salud, sea cual sea su profesión, por su exquisita profesionalidad, desprendida entrega y formidable aportación a la mejora de la calidad de vida de los pacientes.

Esta obra está sujeta a una licencia de Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

FICHA DEL TRABAJO FINAL

Título del trabajo:	Ciberseguridad en Infraestructuras y Dispositivos Sanitarios
Nombre del autor:	Rayco Manuel Monzón Castillo
Nombre del consultor/a:	Jorge Chinea López
Nombre del PRA:	Victor Garcia Font
Fecha de entrega:	29/12/2022
Titulación o programa:	Máster de Ciberseguridad y Privacidad
Área del Trabajo Final:	Seguridad Empresarial
Idioma del trabajo:	Castellano
Palabras clave	Sanidad, Sanitario, Salud

Resumen del Trabajo

La cada vez más creciente tecnologización del sector sanitario hace de la seguridad de las tecnologías de la información y de las comunicaciones (TIC) un elemento clave dentro de este. Algunos de los motivos son:

- La digitalización de los datos sensibles, tanto de salud como personales.
- La conexión a la red de los dispositivos electromédicos.
- La compartición de la información clínica y personal de los pacientes entre diferentes organizaciones sanitarias a nivel internacional.
- La cada vez más creciente utilización de nuevas disciplinas tecnológicas tales como el Internet of Medical Things (IoMT), machine learning, big data, cloud, etc.

Para contextualizar cómo el uso de la tecnología ha transformado y evolucionado a la medicina históricamente, el proyecto analizará cronológicamente varios hitos desde el antiguo Egipto, hace unos 3.000 años, hasta hoy día, en lo que se considera la aparición y evolución de la ingeniería biomédica.

De la misma forma, se ahondará en el marco legal que normaliza y legisla la ciberseguridad en el sector de la sanidad en España.

Los ciberdelincuentes son conscientes de que la multimillonaria infraestructura sanitaria todavía es muy vulnerable pese a su criticidad y el valor de los datos que posee. El sector está envuelto en un apresurado proceso de evolución tecnológica que en ocasiones no va acompañado de las medidas de seguridad que lo protegen de forma adecuada. Además, utiliza una gran cantidad de sistemas antiguos que no siempre renuevan, actualizan o parchean; en muchas ocasiones, por motivos económicos o políticos; y en otras, para no afectar al rendimiento o la continuidad del servicio que estos ofrecen.

Por ello, someten a la industria a grandes robos de datos sensibles de pacientes y la extorsionan económicamente de forma incesante.

Pero la extorsión y el acceso indebido a datos clínicos y personales de pacientes no son las únicas

amenazas que acechan al sector. Los novedosos dispositivos médicos portan frecuentemente vulnerabilidades. Estas han sido descritas en las fronteras de autenticación y cifrado de información de dispositivos implantados en personas y podrían permitir que un atacante los alterara conectándose de forma inalámbrica y pudiendo atentar contra la vida de los pacientes.

La mayor parte del trabajo se centrará en tres ciberamenazas relacionadas con los riesgos anteriormente expuestos. De ellas, se analizarán sus ciberincidentes en el sector de la salud, sus mecanismos de acción e infección, y sus medidas de prevención, contención y contramedidas. Se aprovechará el detalle de estas dos últimas para guiar al lector en el desarrollo óptimo de un completo plan de gestión de incidentes en todas sus fases.

Los sistemas comunes y los procedimientos universales permiten que las vulnerabilidades se propaguen por las infraestructuras sanitarias de todo el mundo. Es por ello por lo que se describirán las vulnerabilidades y posibles ciberataques que amenazan a los propios estándares sanitarios utilizados a nivel internacional en la interoperabilidad de los sistemas médicos.

Si bien no se puede predecir con exactitud cuál será el futuro de la tecnología sanitaria a largo plazo, sí se conocen las incorporaciones de varias disciplinas tecnológicas con un gran potencial en el avance del sector y que marcarán la tendencia de su progreso de forma inminente: la telemedicina, el IoMT, el big data, la IA, la realidad virtual, los chips implantables, la robótica y la nube. En su correspondiente apartado se analizará su utilidad en la medicina del futuro inminente y los riesgos asociados que su uso conlleva.

Finalmente, la conclusión del proyecto hará un repaso en la motivación de este y profundizará en los aspectos y las medidas que la composición de este trabajo ha determinado que ayudarán a minimizar o incluso evadir varios de los riesgos en materia de seguridad tecnológica sanitaria.

Abstract

The increasing technologization of the health sector makes ICT (information and communication technology) security an essential element within it. There are several events in which ICT security should be considered:

- The digitalization of sensitive data (both medical and personal).
- The connection of electromedical devices to the network.
- Sharing patients' clinical history and personal information with other international healthcare organizations.
- Using new technological disciplines such as the Internet of Medical Things (IoMT), machine learning, big data, the cloud, etc.

In order to contextualize how the use of technology has historically transformed and aided in advancing medicine, this project will chronologically analyse various technological milestones dating from ancient Egypt (about 3,000 years ago) to the present day, in what is considered the evolution of biomedical engineering.

Parallelly, the accompanying legal framework that normalizes and legislates the Spanish healthcare's cybersecurity will be examined in depth.

Cybercriminals are aware that the multimillionaire healthcare infrastructure is still highly vulnerable despite the great value of the data it holds. The sector is involved in a hurried process of technological evolution that is not always accompanied by the security measures that adequately protect it. Moreover, a lot of old systems are used that are not always renewed, updated or patched (due to economic or political reasons, or to avoid discontinuance of service provided).

Consequently, the healthcare industry suffers frequent massive sensitive data breaches and extortion.

However, extortion and improper access to clinical and personal data of patients are not the only threats to the sector. Novel medical devices frequently carry vulnerabilities. These have been described by other researchers in the processes of authentication and encryption of information from devices implanted in people and could allow a cybercriminal to alter them by connecting wirelessly, potentially endangering the lives of patients.

Most of this Master thesis will focus on three cyberthreats related to the aforementioned risks and will perform an analysis of their incidence in the healthcare sector, and will discuss their mechanisms of action and infection, their prevention, containment and their countermeasures. The specifics of these last two mechanisms will be used to guide the reader in the optimal development of a complete incident management plan in all its phases.

Common systems and universal procedures enable vulnerabilities to spread throughout healthcare infrastructures around the world. It is for this reason that vulnerabilities and possible cyber-attacks that threaten the very healthcare standards used worldwide in medical systems' interoperability will be described.

Although the long-term future of healthcare technology cannot be accurately predicted, the results of incorporating pioneering technological disciplines (telemedicine, IoMT, big data, artificial intelligence, virtual reality, implantable microchips, robotics and the cloud) to advance the sector are known and will set the trend for imminent progress in the field. In its corresponding section, their usefulness in the medicine of the near future and the associated risks that their use entails will be analysed.

This project will conclude by emphasizing the motivation that started it and will delve into the aspects and measures that the researching of this Master thesis has determined will help to minimize or even avoid several of the risks related to healthcare cybersecurity.

Índice

1. Introducción

El motivo principal que suscita la realización de este Trabajo de Fin de Máster (TFM) es responder a la cuestión de si la tecnologización del sector sanitario se está realizando de una manera garante. Es decir, yendo de la mano de las medidas de seguridad técnicas adecuadas que protegen cada avance.

Para ello, se detallará un plan de trabajo que definirá el contexto, los objetivos y la metodología que se seguirá en el proyecto del TFM. A su vez, se dividirán las tareas en forma de entregas que se planificarán mediante un diagrama de Gantt. A continuación, se revisará el estado del arte de la materia en estudio. Posteriormente, se indicará el impacto que tendrá a nivel de sostenibilidad, ético-social y de diversidad. Por último, se analizarán la viabilidad y los riesgos que conllevan la realización del proyecto.

Para ahondar en el contexto y proceso de tecnologización del área médica y en cómo los avances de la tecnología han influido de manera directa en el progreso de la medicina, se expondrá un apartado dedicado, a modo esquemático, a la historia de la ingeniería biomédica.

Debido a que la seguridad no puede ser entendida sin el tejido de normas que la promueve y regula, se detallará el marco legal que influye directa o indirectamente en la ciberseguridad del entorno sanitario en España.

Casi todo el proyecto se centrará en tres de las principales o más inherentes amenazas del sector de la sanidad a escala mundial. De ellas, se profundizará en cómo actúan, cómo prevenirlas y qué medidas de contención y contramedidas se deben poner en marcha cuando las de prevención no han sido suficientes.

De forma más resumida, se analizarán vulnerabilidades que propician ciberataques en casi cualquier instalación sanitaria del planeta, sin importar el modelo o la versión de los sistemas que utilicen. Y es que los estándares de interoperabilidad sanitaria que establecen la normalización de las comunicaciones entre sistemas médicos no están precisamente exentos de vulnerabilidades.

Se culminará la investigación con la exposición de las disciplinas tecnológicas que hoy sabemos que estarán presentes en muchas de las soluciones médicas del futuro próximo. De cada una de ellas se examinará qué consecuencias podría tener no implementar las convenientes medidas técnicas de seguridad.

Finalmente, se redactará la conclusión del proyecto repasando tanto la motivación inicial como el desenlace de este y profundizando en las medidas que se proponen como fruto de la investigación para evadir las amenazas de ciberseguridad que acechan al sector.

2. Plan de trabajo

El presente apartado define el plan de trabajo que se seguirá para la elaboración del proyecto TFM sobre el análisis de la ciberseguridad en el mundo de la salud. Dicha definición describirá el tema principal en el que se basará el estudio, así como los objetivos a alcanzar y la metodología a utilizar. También detallará las tareas a realizar, su planificación, viabilidad, riesgos y dependencias; el estado del arte y el impacto en sostenibilidad, ético-social y de diversidad.

2.1 Contexto y justificación

Sin duda, el aspecto más relevante y diferenciador entre la medicina tradicional y la contemporánea son los avances tecnológicos que se han llevado a cabo en el sector sanitario.

Estos avances han centrado durante siglos la atención y el júbilo en los progresos médicos conseguidos, descuidando otros aspectos. Y es que todo cambio debe de ser meticulosamente analizado desde el punto de vista de la seguridad. Especialmente con la entrada en la era de la digitalización, que propicia la vulneración de diversas brechas de seguridad desde diferentes tipos de vectores de ataque debido a su extensa conectividad y almacenamiento de valiosos datos.

El campo profesional dedicado a la conjunción entre la ingeniería y la medicina es la ingeniería biomédica. Actúa en diferentes áreas de la tecnología sanitaria: bioinformática, biomecánica, biomaterial, óptica biomédica, ingeniería de tejidos, instrumentación, robótica, etc.

Este campo ha dado lugar a la implementación de diferentes dispositivos trascendentales en la era moderna tales como el desfibrilador, el marcapasos, el electrocardiograma, el ecógrafo, entre otros; con enormes beneficios para el diagnóstico, el tratamiento y el bienestar del paciente.

El interés del ser humano en mejorar la calidad de vida mediante artificios clínicos se remonta más allá de hace 3.000 años, según el descubrimiento de una prótesis de madera del dedo gordo del pie descubierta en una tumba egipcia [1]. Hoy día, en la era de la información, la tecnología sanitaria se centra principalmente en la digitalización plena de los datos y la interconexión de dispositivos electromédicos como los anteriormente comentados. Hace uso, por lo tanto, de redes de cualquier ámbito, dimensión y tecnología; el uso del IoMT (Internet of Medical Things), la nube, el análisis de datos o la inteligencia artificial, entre otras disciplinas.

Sin embargo, todo avance conlleva riesgos. La conexión a la red de los dispositivos sanitarios que velan por la salud o gestionan las historias clínicas de los pacientes aumenta la posibilidad de que puedan ser interceptados por un atacante o infectados por un software malicioso. Esta exposición no solo afecta a la privacidad del paciente, sino a su propia vida.

Cabe destacar que en el RGPD y la LOPDGDD los datos personales relativos a la salud están considerados como una categoría especial y, por tanto, se encuentran especialmente protegidos. En 2021 se registraron 680 reclamaciones relacionadas con sanidad ante la Agencia Española de Protección de Datos, incrementándose un 75% respecto a 2020 [2].

Dentro del marco legal que afecta a la ciberseguridad del ámbito sanitario en España existen otras regulaciones, además del RGPD y la LOPDGDD. Entre ellas, destaca el Esquema Nacional de Seguridad. Su objetivo es, básicamente, garantizar la seguridad electrónica de las actividades en régimen de derecho público de las administraciones y los ciudadanos. Si bien, principalmente afecta a las administraciones públicas que sostienen casi toda la infraestructura sanitaria en España, su certificación está siendo codiciada por otras entidades del sector tales como clínicas y hospitales privados.

Apenas existen fuentes oficiales que apunten a datos estadísticos específicos en España, e incluso Europa; lo cual refuerza la motivación concienciadora de este proyecto. Por ello se deberá apoyar también en datos de empresas privadas expertas en ciberseguridad y medios de comunicación para su investigación.

Según Check Point, el sector sanitario español es el tercero más atacado del mundo en los últimos años detrás de los de Canadá y Alemania [3]. Solo un par de años antes alertaba de que este sector estaba a nivel general y mundial entre los más desprotegidos contra los ciberataques avanzados [4].

Fundamentalmente, los motivos por los que este sector es uno de los principales objetivos de los ciberatacantes son dos:

1. Ofrece menor resistencia y complejidad ante ciertos ataques debido a su **vulnerabilidad**. Razones:

    - Está abocado a utilizar software y hardware antiguo por problemas de compatibilidad, falta de contratación de mantenimiento o el gran coste que supone la adquisición de nuevas licencias y equipos médicos.
    - Sufre un cambio constante de proveedores tecnológicos y una fuerte externalización que van contra la estabilidad y la especialización del personal de los sistemas a mantener.
    - Hay poca o nula unión y comunicación entre los departamentos de informática de las diversas entidades que componen el sector tanto público como privado.
    - No existe un órgano centralizado especializado en el sector de la salud encargado de unificar y gestionar la ciberseguridad a nivel estatal y de la Unión Europea.
    - El sector tiene mayor vocación clínica que tecnológica. Se concibe a la informática simplemente como a un servicio auxiliar.
    - Se opta por minimizar o incluso evitar la actualización y parcheado de los sistemas sanitarios para no interrumpir la continuidad de su servicio y/o ralentizar su rendimiento.
    - Soporta un apresurado proceso de digitalización que no permite segurizar de forma paralela cada avance.
    - Prima más la inversión en los avances médicos que en los informáticos, más específicamente en los de la ciberseguridad.
    - Contratan a poco o nulo personal especializado en seguridad TIC.
    - Mantiene el foco en la seguridad clínica del paciente y no en la seguridad IT.

2. Es más propenso a ceder ante extorsiones económicas debido a su **criticidad**. Razones:

    - Alberga información muy sensible: datos personales de pacientes, historias clínicas, etc.
    - Lo componen infraestructuras críticas y servicios esenciales para la nación.
    - El corte de su servicio supone grandes pérdidas económicas e incluso vidas humanas.
    - La sanidad de un país está sometida a una fuerte presión social y política.
    - Atraviesa crisis sanitarias como la de la pandemia del COVID-19 que aumenta su presión y saturación.

Precisamente por su facilidad ante el chantaje, la extorsión y la coacción; la ciberamenaza más utilizada es el ransonware. El WannaCry llegó a tumbar gran parte del Sistema Nacional de Salud del Reino Unido en mayo del 2017 tal y como demuestra una investigación de la National Audit Office sobre los efectos del Wannacry en el National Health Service de Inglaterra [5].

Estos ciberataques no solo se traducen en el secuestro de una gran cantidad de información sensible de pacientes y el consecuente pago de su rescate. También en la inutilización de los sistemas clínicos y farmacéuticos, produciendo un grave bloqueo en la continuidad del servicio sanitario nacional por un tiempo indefinido. Las consecuencias son la anulación de todas las pruebas médicas, citas y operaciones; la paralización de la dispensación de medicamentos y la imposibilidad del correcto ejercicio de los profesionales de la salud. Estos profesionales carecen de acceso a las historias clínicas de los pacientes ingresados para poder comprobar sus patologías, resultados de analíticas, alergias, medicación, etc., poniendo en grave peligro sus vidas.

El portal británico de divulgación en materia de ciberseguridad, Comparitech, ha publicado en octubre de este año que, en 2021, 108 ataques individuales de ransomware afectaron a 2.302 organizaciones médicas en EE. UU., lo que potencialmente afectó a 19,76 millones de registros de pacientes. Se estima que estos ataques cuestan a las entidades médicas casi 7.800 millones de dólares solo en tiempo de inactividad [6].

Por otro lado, otro vector de amenaza en crecimiento en este sector es el de las vulnerabilidades de los dispositivos médicos. Un análisis de la compañía Cynerio realizado en 2022 sobre 10 millones de dispositivos IoT e IoMT en más de 300 centros sanitarios de EE. UU. ha detectado que el 53% de ellos contienen vulnerabilidades críticas a pesar del aumento de las inversiones en seguridad. Las bombas intravenosas serían el dispositivo IoMT más común y con mayor riesgo. De ellas, el 73% contaría con una vulnerabilidad que podría poner en peligro la seguridad del paciente, la confidencialidad de los datos y la disponibilidad del servicio [7].

Esta compañía también ha valorado en sus investigaciones que el 24% de los hospitales habían aumentado las tasas de mortalidad después de un ciberataque [8].

La FDA (Food and Drugs Administration), máxima institución que regula la legalidad de ciertos alimentos y medicamentos en EE. UU., ha advertido e incluso cesado cautelarmente el uso de algunos dispositivos médicos electrónicos por sus vulnerabilidades a ataques informáticos. Entre ellos, la bomba de insulina Medtronic MiniMed 600 Series con conexión inalámbrica, de la que alertaron que era factible su acceso no autorizado [9]. Este ataque podría manipular la administración de insulina provocando la sobredosis y consecuente muerte a pacientes diabéticos.

Otros de los dispositivos médicos más temibles que han presentado vulnerabilidades son los implantes desfibriladores y los marcapasos. La manipulación remota de estos dispositivos podría dar lugar a impulsos eléctricos malintencionados sobre el corazón del paciente, lo que podría desencadenar en una parada cardíaca.

2.2 Enumeración de los objetivos

Se priorizarán como objetivos principales del proyecto los inherentes a un TFM, así como los solicitados en el propio área y especialización de este: "*Principales ciberdelitos/ciberincidentes. ¿Cómo comprometen a las organizaciones y usuarios?"* Siendo los demás objetivos de grado adicional, sujetos a la disponibilidad en tiempo y a la viabilidad de estos en el desarrollo del proyecto, la cual solo puede ser evaluable durante su transcurso.

Objetivos principales inherentes al TFM:

- Demostrar comprensión detallada en un ámbito especializado dentro de la seguridad de la información.
- Saber analizar diferentes alternativas y elegir la más adecuada, justificando su elección.
- Saber evaluar y discutir decisiones tomadas, ya sea por uno mismo o por otros.
- Elaborar y defender un documento que sintetice un trabajo original en el ámbito de la seguridad de la información.
- Saber transmitir de forma eficiente y eficaz las partes más importantes de un contenido voluminoso a diferentes audiencias.
- Consolidar las competencias básicas, generales, transversales y específicas del TFM.

Objetivos principales inherentes al área y especialización del TFM:

- Investigar y analizar los principales ciberincidentes en infraestructuras y dispositivos sanitarios.
- Investigar y analizar los mecanismos de acción e infección de los principales ciberincidentes en infraestructuras y dispositivos sanitarios.
- Investigar, analizar y proponer las medidas de contención y contramedidas de los principales ciberincidentes en infraestructuras y dispositivos sanitarios.
- Investigar, analizar y proponer las medidas de prevención de los principales ciberincidentes

en infraestructuras y dispositivos sanitarios.

Objetivos adicionales:

- Investigar y exponer un resumen sobre la historia de la ingeniería biomédica.
- Investigar y referenciar el marco legal español de la ciberseguridad en el entorno sanitario.
- Relatar de forma teórico-práctica vulnerabilidades y ciberataques propios de la tecnología sanitaria.
- Investigar y redactar los riesgos y amenazas del futuro cercano de la tecnología sanitaria.

2.3 Descripción de la metodología

El proyecto seguirá una metodología cualitativa basada en la respuesta ante cuestionamientos e incidentes (empirismo), así como percepciones y opiniones tanto a nivel de usuarios como de profesionales del sector de la sanidad y de la ciberseguridad. Por lo tanto, contará con una gran aportación de análisis cualitativo de datos.

Por otro lado, se apoyará en una metodología cuantitativa basada en el análisis de los datos obtenidos, especialmente de tipo estadístico. También, dado el carácter científico y experimental de las ramas que participan en el estudio (ingeniería y medicina), se consolidará con la recopilación de información medible, práctica y comparativa.

Por lo tanto, implementará una metodología de investigación mixta.

El modelo a seguir será implementado por los siguientes procedimientos y a su vez etapas de manera iterativa hasta la conclusión final del trabajo:

1. Búsqueda de información.
2. Recogida de información.
3. Análisis de contexto.
4. Interpretación de datos.
5. Redacción del informe de investigación.

Finalmente, el tipo de diseño de investigación mixta será el diseño exploratorio secuencial, en el que se recopilarán y analizarán los datos procedentes de la investigación cualitativa y, paralelamente, pero en grado ulterior, los de la investigación cuantitativa. Se dará prioridad al aspecto cualitativo a causa de la fuerte naturaleza social del estudio. Las conclusiones de ambos resultados se integrarán durante la fase de interpretación y conclusión del mismo.

2.4 Listado de las tareas

1. Plan de trabajo: PEC 1.
    a. Contexto y justificación.
    b. Enumeración de los objetivos.
    c. Descripción de la metodología.
    d. Listado de las tareas.
    e. Planificación de tareas.
    f. Revisión del estado del arte.
    g. Impacto ético, social y ambiental.
    h. Análisis de viabilidad y riesgos.

2. Entrega de seguimiento 1: PEC 2.

    a. Ciberincidentes en infraestructuras y dispositivos sanitarios.
    b. Mecanismos de acción e infección.
    c. Historia de la ingeniería biomédica.

3. Entrega de seguimiento 2: PEC 3.

    a. Medidas de contención y contramedidas.
    b. Medidas de prevención.
    c. Marco legal español de la ciberseguridad en el entorno sanitario.

4. Memoria final: PEC 4.

    a. Ciberataques propios de la tecnología sanitaria.
    b. Futuro de la tecnología sanitaria: riesgos y amenazas.
    c. Maquetación.
    d. Recopilación de toda la información.
    e. Estructuración.
    f. Conclusión.

5. Presentación en vídeo.

    a. Elección de contenido de relevancia.
    b. Guion.
    c. Grabación.

6. Defensa del TFM.

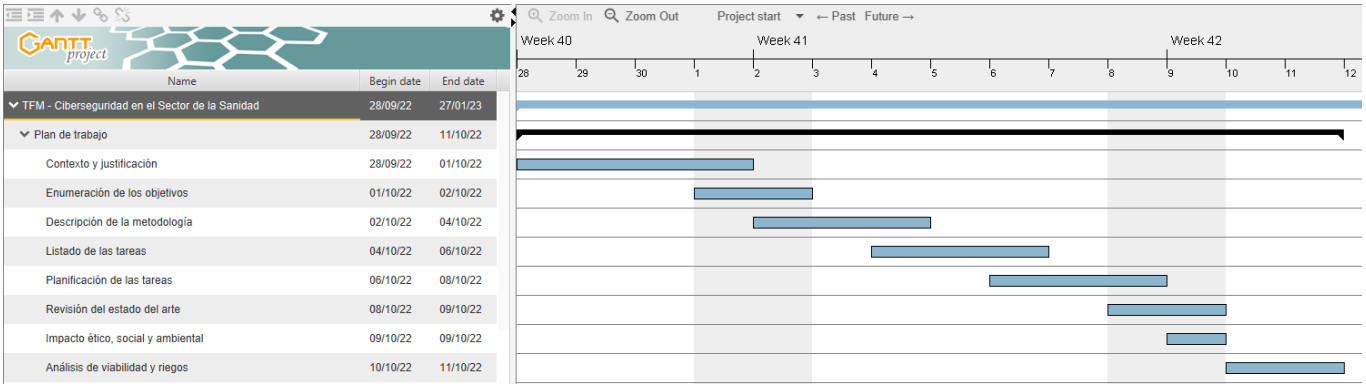
    Defensa del proyecto ante el tribunal evaluador.

2.5 Planificación de las tareas

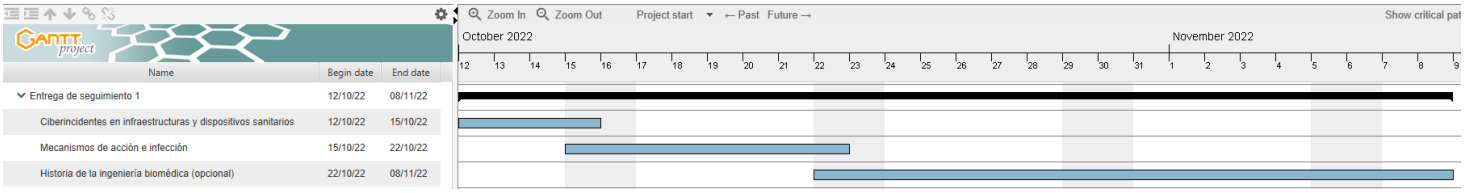
A continuación, se muestra la planificación de tareas del proyecto mediante un diagrama de Gantt.

Los hitos parten del proyecto principal, TFM, del 28/09/2022 al 27/01/2023.

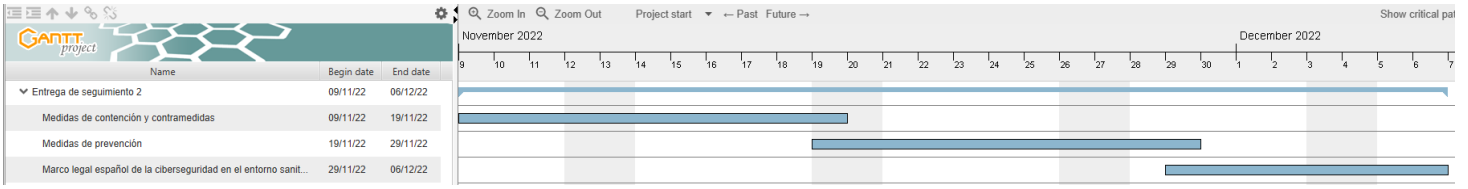
El primer hito es el plan de trabajo, que se corresponde con la PEC 1 del 28/09/2022 al 11/10/2022.



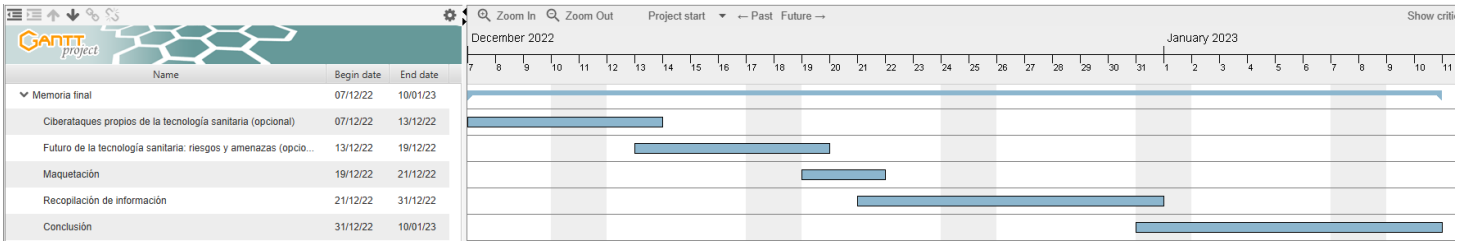
El segundo hito es la entrega de seguimiento 1, que se corresponde con la PEC 2, del 12/10/2022 al 08/11/2022.



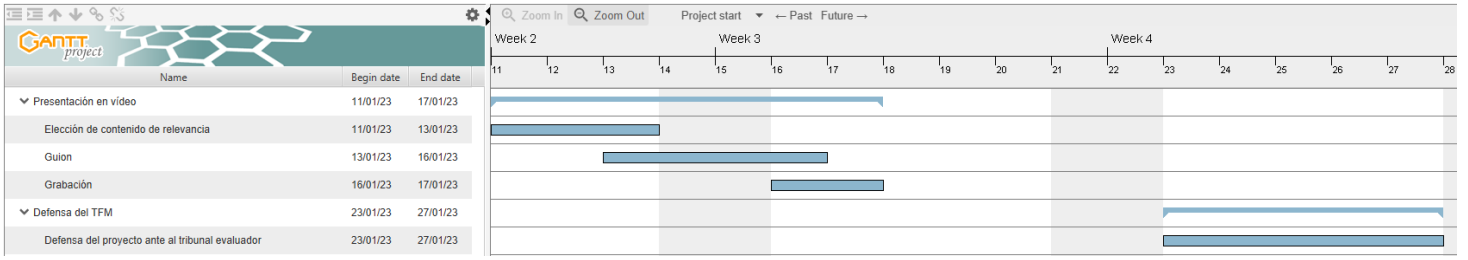
El tercer hito es la entrega de seguimiento 2, que se corresponde con la PEC 3, del 09/11/2022 al 06/12/2022.



El cuarto hito es la Memoria Final, que se corresponde con la PEC 4 y última, del 07/12/2022 al 10/01/2023.



Los quinto y sexto hitos son, respectivamente, la presentación en vídeo, del 11/01/2023 al 17/01/2023 y la defensa del TFM, del 23/01/2023 al 27/01/2023.



2.6 Revisión del estado del arte

La declaración de infraestructura crítica corresponde al Ministerio del Interior de España mediante el Catálogo Nacional de Infraestructuras Estratégicas, el cual no es público. Se estima que no fue hasta la declaración de la pandemia del 2020 del COVID-19 bajo el virus SARS-CoV-2 que se tomó la decisión de incluir, por fin, al menos a los más relevantes centros sanitarios del país. Un requerimiento coherente pero tardío, según varios expertos y organismos sanitarios, especialmente tomando en consideración las siguientes normas y medidas relacionadas con los servicios esenciales y las infraestructuras críticas que no fueron aplicables a tiempo.

Tal y como menciona la Ley 8/2011, de 28 de abril, por la que se establecen las medidas para la protección de las infraestructuras críticas [10], un servicio esencial es aquel servicio necesario para

el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

El Real Decreto-ley que delimita el ámbito funcional de actuación de los CSIRT de referencia en España es el 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los digitales, y establecer un sistema de notificación de incidentes [11].

Este mismo decreto, desarrollado por el Real Decreto 43/2021, de 26 de enero [12]; establece como autoridad competente en materia de seguridad de las redes y sistemas de información para los operadores de servicios esenciales que no sean operadores críticos en materia de la salud al Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales.

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [13] define dos documentos de especial afectación a los operadores críticos:

- Los Planes de Protección Específicos son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.
- Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.

La ciberseguridad en el sector de la salud es una de las asignaturas pendientes no solo en España, sino en casi todo el marco europeo. Según datos del ENISA Report de finales del año pasado, no existe un CSIRT del sector de la sanidad a nivel nacional en toda la Unión Europea salvo en 3 países: Francia (CERT Santé), Luxemburgo (HealthNet-CSIRT41) y Países Bajos (Z-CERT43) [14].

En España, al igual que en el resto de los 24 países de la Unión Europea, no existe una entidad dedicada al sector de la salud en materia de ciberseguridad. Depende, por lo tanto, del INCIBE-CERT51 que es el centro de respuesta a incidentes de seguridad de referencia para ciudadanos y entidades de derecho privado en España, operado por el Instituto Nacional de Ciberseguridad de España (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

En cuanto al sector público, que lidera casi la totalidad de la infraestructura sanitaria del país, el Centro Criptológico Nacional Computer Emergency Response Team, también conocido por sus siglas CCN-CERT, es el servicio estatal encargado de su ciberseguridad. El CCN-CERT depende directamente del Centro Criptológico Nacional, que es un organismo del Estado español adscrito a su vez al Centro Nacional de Inteligencia.

El CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las administraciones públicas, así como de empresas y organizaciones de interés estratégico para el país.

El hecho de que en España no exista aún una entidad dedicada al sector de la salud en materia de ciberseguridad conlleva una serie de desventajas en cuanto a la resiliencia de la seguridad tecnológica del sistema sanitario de salud. No hay un organismo estatal especializado en el área sanitario que gestione y coordine la ciberseguridad a nivel centralizado de todos los servicios de la

salud de cada comunidad autónoma y los centros privados sanitarios que operan en el país.

A su vez, aunque cada servicio de la salud de cada región sí suela tener su propio CSIRT, de él subyacen varias gerencias tanto hospitalarias como de atención primaria que gestionan su propia infraestructura de sistemas (redes, software, electromedicina, etc.) y seguridad con independencia y autonomía. Esto dificulta en gran medida la actuación conjunta ante amenazas e incidentes que podrían incluso escalar a las diferentes infraestructuras del gobierno de la comunidad autónoma, ya que generalmente es él quien provee la red a la que se interconectan las redes internas de cada una de estas gerencias.

Por supuesto, los servicios de salud mantienen una constante integración con el Sistema Nacional de Salud, y este con los diferentes sistemas de salud de los diversos países de la UE debido a los proyectos cada vez más crecientes de compartición de información clínica entre los países miembros, como son el HCDSNS (Historia Clínica Digital del Sistema Nacional de Salud).

En conclusión, existen diversos ciberincidentes que podrían generarse en un centro de salud local y tener trascendencia a nivel europeo y, por lo tanto, es hoy día tan importante garantizar la seguridad del sistema sanitario de la UE, como la del más pequeño consultorio de salud de barrio.

En materia de ciberseguridad, en el sector de la salud existe poca documentación rigurosa y de fuentes neutrales u oficiales, señal de la poca especialización y concienciación a la que se ve sometida pese a su crecimiento digital exponencial. Esta digitalización está dando lugar desde a sistemas de información que comparten historiales clínicos de pacientes a nivel internacional, como al almacenamiento de datos sanitarios en la nube, o el uso de dispositivos médicos implantados en pacientes. En su mayoría, estos dispositivos poseen conectividad inalámbrica y por lo tanto son accesibles remotamente. Proteger de forma adecuada este acceso es vital, pues cuentan con la responsabilidad de suministrarle insulina o efectuarle impulsos eléctricos en el corazón al paciente, lo cual podría ser manipulable malintencionadamente.

Algunos de los aspectos relevantes en la necesidad de concienciación de la importancia de mantener una ciberseguridad depurada en el entorno sanitario podemos encontrarlos en el Check Point Software's 2022 Security Report [15]:

- El sector de la salud genera alrededor de un 30% de los datos mundiales, incluso por encima del sector financiero.
- Se enfrenta a diversos ataques de cada vez mayor complejidad: ransomware, botnets, ejecución remota de código, DDoS, etc.
- Sufrió un promedio de 830 ciberataques cada semana en 2021 (un 71% más que en 2020).
- Sufre crisis sanitarias, como la del COVID-19, que aumentan el azote de los ciberataques por la facilidad de extorsión para conseguir rescates debido a la crítica necesidad de mantener los datos y sistemas a salvo, así como la saturación del personal. La pandemia multiplicó por diez la efectividad de extorsión, y algunos ransomware, como el Ryuk, cambió su enfoque para infectar específicamente a hospitales.
- La creciente informatización de los dispositivos médicos genera cada vez más puntos de entrada a diversas ciberamenazas en el sector.

2.7 Impacto en sostenibilidad, ético-social y de diversidad

Este proyecto, en relación institucional a la Universitat Oberta Catalunya, se implicará en cumplir la competencia de compromiso ético y global (CCEG) definida a nivel de máster como la actuación de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional, y diseñar soluciones para mejorar estas prácticas.

Dimensión en la sostenibilidad medioambiental y/o huella ecológica:

El sector de la sanidad ha sido uno de los máximos actores en gran cantidad de ensayos en animales y plantas, así como en la producción industrial y química a lo largo de la historia, especialmente en las eras industriales.

Con el cambio a la era de la digitalización, los sistemas de cómputo han permitido el hallazgo de nuevos descubrimientos clínicos que han permitido prescindir del ensayo sobre diversos seres vivos, preservando así la biodiversidad y favoreciendo la protección de especies. A su vez, el uso de la biotecnología y de los dispositivos médicos han rebajado la utilización de fármacos derivados de animales y plantas. Este último punto ha contribuido a reducir la producción de gases y materiales que contaminan e intoxican el medioambiente, a disminuir el calentamiento global y a mejorar la gestión de residuos.

El presente trabajo pretende contribuir a la digitalización de la sanidad junto con todos sus beneficios mediante la concienciación y la divulgación de la relevancia de las medidas que garantizarán su exitoso cambio desde el punto de vista de la seguridad digital.

Dimensión en el comportamiento ético y de responsabilidad social:

El desamparo de los aspectos relativos a la confidencialidad, integridad y disponibilidad de los datos clínicos, así como de la seguridad de los dispositivos médicos, generan un caldo de cultivo ideal para los cibercriminales. Además, tratándose del ámbito sanitario, los incidentes tienen un gran impacto social y económico.

Este proyecto realiza un trabajo de investigación y análisis con el fin de concienciar acerca del mal estado de la ciberseguridad en el sector de la salud y sus consecuencias sociales, minimizando así los delitos a los que se ve sometido y contribuyendo a la mejora del comportamiento ético y de la responsabilidad social en la materia.

A su vez, expone los beneficios de la contratación, bienestar, formación, estabilidad y demás mejoras laborales, ambientales y psicosociales del equipo humano que compone las entidades sanitarias: técnicos, clínicos, vigilantes, etc.

Finalmente, realza el valor de la profesión informática dentro de las organizaciones, la cual ha sufrido desde su nacimiento una infravaloración notable en España, donde incluso carece de un convenio colectivo propio. Cada vez más, esta profesión se está convirtiendo en una parte esencial y de gran valor para el eficiente funcionamiento de cualquier empresa y la protección de sus activos tanto digitales como físicos.

Dimensión en diversidad, género y derechos humanos:

La confidencialidad de los datos sensibles y la seguridad de la salud de las personas son los dos aspectos clave a salvaguardar mediante la ciberseguridad del sector de la sanidad.

Los datos clínicos de las personas son categorizados como de carácter especial dada la vulnerabilidad de las personas ante su exposición. Por otro lado, el uso de dispositivos médicos inseguros pone en grave peligro la vida de las personas más frágiles.

El objetivo de este trabajo es contribuir a la revisión del estado de la ciberseguridad en el ámbito sanitario. Se recalcará la relevancia no solo de avanzar tecnológicamente en el área médica, sino de hacerlo de forma segura, garantizando el derecho a la privacidad y la calidad de vida de las personas.

2.8 Análisis de viabilidad y riesgos

A continuación, se enumeran una serie de riesgos a mitigar para posibilitar la viabilidad de este proyecto:

1) Pocas fuentes de información oficiales y rigurosas.

   Medidas de mitigación:

   - Utilización de la experiencia propia profesional en el sector sanitario tanto a nivel técnico, funcional, como de gestión.
   - Recabado de información a partir de entidades y personal experto en el sector.
   - Uso de fuentes de impacto.
   - Contrastación con fuentes de segundo nivel.
   - Contrastación con fuentes oficiales de otros sectores o del mismo sector y diferentes países.
   - Elección de fuentes de información secundarias pero utilizadas a su vez por fuentes oficiales y/o rigurosas.

2) Pocos precedentes de investigación en la materia.

   Medidas de mitigación:

   - Recopilación de datos de interés.
   - Organización y análisis de la información.
   - Aprovechamiento de las investigaciones colaterales de otro sector o país.
   - Iniciación de una nueva investigación.
   - Explotación de análisis y noticias del sector.

3) Imposibilidad de realizar un desarrollo práctico por la inexistencia de un laboratorio debido a que:

   a. Son sistemas demasiado caros.
   b. Ni siquiera las clínicas suelen tener entornos de pruebas.
   c. Es un sector fuertemente auditado.
   d. Son sistemas críticos y con datos protegidos.

   Medidas de mitigación:

   - Empirismo profesional propio.
   - Realización de desarrollo teórico-práctico frente a desarrollo práctico.
   - Laboratorio doméstico de software frente a laboratorio de equipos y dispositivos.
   - Análisis de vulnerabilidades ya conocidas.
   - Análisis de documentación de fabricantes.

4) En ocasiones, la información es de parte y con fines comerciales ya que es un sector que mueve demasiado dinero.

   Medidas de mitigación:

   - Priorización de fuentes de información no comerciales.
   - Evitación de fuentes de información con fuerte prevalencia comercial o sensacionalista.
   - Preferencia de fuentes de análisis, neutrales, académicas u oficiales.
   - Contrastación, investigación y análisis de la información.

5) Es un entorno muy opaco e inaccesible a investigaciones externas.

Medidas de mitigación:

- Recabado de información basado en la experiencia propia y de compañeros del sector.
- Hallazgo de información en congresos y conferencias celebradas y documentadas o grabadas.
- Utilización de licitaciones como método de prospección de los sistemas de salud, especialmente públicos.
- Exploración de bases de datos de amenazas y vulnerabilidades.
- Análisis de la información de compañías auditoras del sector.

6) Cada país e incluso región tiene un marco legal y orgánico en materia de salud muy particular.

Medidas de mitigación:

- Concentración en el marco legal y orgánico español.
- Escalamiento al ámbito europeo solo para afectaciones de la Unión Europea.
- Escalamiento al ámbito internacional solo para contextualizar en caso de no hallar información suficiente a nivel nacional.

3. Historia de la ingeniería biomédica

La adaptación y uso de artefactos que mejoren la salud y la calidad de vida del ser humano ha existido desde siempre. Por ejemplo, el uso de bastones de madera ha ido de la mano de la evolución bípeda de los homos y ha determinado en una herramienta ortopédica que, a día de hoy, sigue siendo fundamental para personas de movilidad reducida.

1000 A.C.
- De más avanzado diseño fue la prótesis de madera del dedo gordo del pie descubierta en una tumba egipcia del 1000 A.C. por un equipo de egiptólogos de la Universidad de Basilea y que se cree, fue hecha para la hija de un sacerdote egipcio.

460 A.C.
- Sobre el 460 A.C., Hipócrates sentó los principios científicos al campo de la medicina. A él se deben las referencias más antiguas de técnicas como la endoscopia.

1485
- Sin embargo, para muchos, el nacimiento de la ingeniería en el campo de la medicina parte de las aportaciones de Leonardo Da Vinci a la anatomía y la mecánica del cuerpo humano aproximadamente en 1485. Logró diseñar la simulación mecánica de un cuerpo hecho de madera.

S. XVI
- En el siglo XVI, el médico y físico italiano Luigi Galvani fundó la ingeniería electroquímica y la biofísica con descubrimientos tales como el impulso nervioso. Otro de los físicos de gran aportación a la conducción eléctrica en los seres vivos fue William Thomson (Lord Kelvin) un siglo más tarde.

1816
- En 1816, el médico e inventor francés René Laënnec creó el primer estetoscopio debido al pudor que este sentía al acercar su oído al pecho de los pacientes, así como a la dificultad para percibir los ruidos en pacientes con sobrepeso.

1880-1940
- Entre 1880 y 1940 se produjo el mayor desarrollo de la instrumentación eléctrica y electrónica, demostrando así los grandes beneficios que estas dos áreas podrían aportar a la medicina.

1887
- Se crea el registro de señales electrofisiológicas en corazones humanos, por A. D. Waller en 1887.

1924
- Se crea el registro de señales electroencefalográficas en humanos por parte de Hans Berger en 1924.

1895
- Surge el desarrollo en el campo de la imagenología con el descubrimiento de los rayos-X por Wilhelm Conrad Röntgen, en 1895. Solo un año más tarde, Siemens y General Electric ya vendían estos sistemas.

1924
- El fisiólogo neerlandés, Willem Einthoven, descubrió el galvanómetro de cuerda que daría paso al electrocardiograma, otorgándole el Premio Nobel de Fisiología o Medicina en 1924.

1921
- En 1921 tuvo lugar el primer entrenamiento formal de Ingeniería Biomédica en el Instituto Oswalt de Física Médica en Frankfurt, Alemania.

1927
- El primer respirador artificial fue creado en 1927 por Philip Drinker y Louis Agassiz Shaw Jr. Conocido como el pulmón de hierro. Se usó por primera vez en 1928 en el Children's Hospital, Boston, Massachusetts, en una niña inconsciente. Adquirió una gran relevancia a mediados del siglo XX cuando las víctimas de la polio no eran capaces de respirar debido a la parálisis del diagragma.

1939-1945
- La Segunda Guerra Mundial fue la crisis que impulsó de manera notoria los avances tecnológicos no solo en la práctica de la aniquilación humana, sino en el arte de salvar vidas entre 1939 y 1945.

1960-1970
- Tras la electricidad y la electrónica, la tecnología computacional es el campo de estudios interdisciplinario que está dotando de mayor avance a la ingeniería biomédica y cuyas contribuciones tuvieron origen entre las décadas 60 y 70 del siglo XX. Las ventajas que aporta van desde el cada vez más creciente poder de computación, pasando por el enorme almacenamiento y gestión de bases de datos, a la interconexión mundial que partió de la red ARPANET y derivó en lo que hoy se conoce como Internet.

S. XXI
- Hoy en día, las tecnologías de la información y las comunicaciones, nacidas de la tecnología computacional y las redes, otorgan al área de la salud sistemas inteligentes e interconectados. Sus bienes son diversos: la telemedicina, la digitalización de los registros clínicos, o la sofisticación de dispositivos médicos implantables, la IA y la robótica en la cirugía, entre otros.

Enlazando con el inicio de este apartado y como evolución a los bastones de madera con los que se abrió, hoy se cuenta con prótesis robóticas y provistas de inteligencia artificial que aprenden de los patrones de movimiento de las personas que los portan. Toda una evolución gracias a la unión entre la medicina y la ingeniería.

4. Marco legal español de la ciberseguridad en el entorno sanitario

Este apartado recopila en la siguiente tabla veintiocho de las normas jurídicas (primera columna) más relacionadas con la seguridad TIC del entorno sanitario español y algunas de las menciones (segunda columna) que las implica directa o indirectamente con la temática. Se efectuará de forma resumida por motivos de limitaciones de extensibilidad del TFM.

Norma Jurídica	Menciones
1. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. [24]	• El derecho a la intimidad de los datos de salud. • Las medidas de seguridad de la información que deben adoptar los centros sanitarios. • Los usos y accesos legítimos a la historia clínica. • La obligación de conservación seguridad de la documentación clínica.
2. Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. [25]	• El control que debe ejercer el Ministerio de Sanidad y las comunidades, en las entidades sanitarias no integradas en el Sistema Nacional de Salud, en relación con las actividades de salud pública y en materia de garantías de información y seguridad. • El uso tutelado de determinadas tecnologías de acuerdo con protocolos específicos destinados a garantizar su seguridad. • Las garantías de seguridad de las técnicas, tecnologías o procedimientos utilizados.
3. Ley 14/2007, de 3 de julio, de Investigación Biomédica. [26]	• El catálogo de principios y garantías para la protección de los derechos de las personas y de los bienes jurídicos implicados en la investigación biomédica. • Las medidas necesarias para garantizar la seguridad de la investigación y reducir los riesgos e incomodidades para los individuos participantes. • La regulación de manera específica el consentimiento informado y el derecho a la información, la protección de datos personales y el deber de confidencialidad de los datos utilizados con fines de investigación biomédica.
4. Ley 14/1986, de 25 de abril, General de Sanidad. [27]	• El uso interno de expedientes sancionadores y medidas administrativas por las infracciones cometidas en materia de sanidad. • La incautación o inmovilización de productos, suspensión del ejercicio de actividades, cierres de empresas o sus instalaciones, intervención de medios materiales y personales y cuantas otras se consideren sanitariamente justificadas. • La regulación general de todas las acciones que permitan hacer efectivo el derecho a la protección de la salud.

5. Ley 33/2011, de 4 de octubre, General de Salud Pública. [28]	• La adopción de las medidas necesarias para garantizar la seguridad de los datos en todos los niveles del sistema de información en salud pública. • El apoyo de las instituciones en el cumplimiento de la legislación a Autoridad Sanitaria estatal. • El auxilio de las Fuerzas y Cuerpos de Seguridad del Estado u otros agentes de la autoridad que tengan encomendadas funciones de seguridad. • La extensión del contenido de la cartera de servicios del Sistema Nacional de Salud a mutualidades garantizando la seguridad y la información.
6. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [29]	• Los criterios lícitos para el tratamiento de datos en la investigación en salud. • Las previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica. • La categoría especial de los datos de la salud. • El aseguramiento del anonimato del paciente en el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia. • La reutilización con fines de investigación en salud o biomedicina de datos personales.
7. Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización. [30]	• La actualización de la cartera de servicios comunes teniendo en cuenta la seguridad de las tecnologías. • Las estrictas medidas de seguridad en los implantes para cardioestimulación. • Los servicios de información a los usuarios del Sistema Nacional de Salud de acuerdo con la regulación de los derechos en materia de información y documentación clínica y de protección de datos de carácter personal. • El diseño e implantación de políticas de salud para la protección de riesgos para la salud. • La verificación y control del cumplimiento de la legislación, criterios y estándares sanitarios, en ejercicio de la autoridad sanitaria.
8. Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada. [31]	• La adscripción del registro a un órgano que garantiza la confidencialidad, seguridad e integridad de los datos contenidos en él. • La implementación digital del registro para intercambio de datos y explotación por medios electrónicos.

	• Las medidas oportunas para garantizar la seguridad de los procesos de envío, cesión, custodia y explotación de la información. • La aplicación de técnicas de disociación y encriptación de datos para garantizar su confidencialidad.
9. Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual. [32]	• La base de datos del sistema de intercambio de información sobre la población protegida entre las administraciones sanitarias. • El fin de mantener la seguridad de los datos y la fiabilidad de la fuente. • La necesidad de establecer los aspectos de seguridad y acceso a la información y la cesión de datos. • La garantía por parte del Ministerio de Sanidad tanto de la seguridad como de la disponibilidad de los datos de carácter personal, evitando su alteración, pérdida, tratamiento y, en especial, el acceso no autorizado a aquélla. • La responsabilidad de la base de datos por parte del Ministerio de Sanidad, que aplicará las medidas de seguridad y accesos.
10. Real Decreto 1277/2003, de 10 de octubre, por el que se establecen las bases generales sobre autorización de centros, servicios y establecimientos sanitarios. [33]	• El Registro general de centros, servicios y establecimientos sanitarios sometido a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. • Las garantías mínimas y comunes de seguridad y calidad que deberán exigir las comunidades autónomas para autorizar la apertura y puesta en funcionamiento de los centros, servicios y establecimientos sanitarios. • El asentamiento de las bases para las garantías de seguridad y calidad de la atención sanitaria.
11. Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud. [34]	• El conjunto mínimo de datos que deberán contener los documentos clínicos con soporte electrónico. • La responsabilidad de la interoperabilidad de la información clínica electrónica por parte de las entidades. • Los datos clínicos y personales que deberán contener, como mínimo, los informes referenciados y la historia clínica resumida.
12. Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se	• El establecimiento de la implantación de nuevas medidas de seguridad para las empresas europeas, los autónomos y la administración pública. • La Ley de Seguridad Cibernética de la UE que moderniza y refuerza la Agencia de la UE para la ciberseguridad (ENISA) y establece un marco de certificación de la ciberseguridad en toda la UE para productos, servicios y procesos digitales.

deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). [35]	• El responsable del tratamiento en fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad. • Las excepciones a la prohibición de tratar categorías especiales de datos personales con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. • El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado necesario por razones de interés público en el ámbito de la salud pública. • Las circunstancias de prohibición de datos personales relativos a la salud en fines distintos a los asistenciales.
13. Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) nº 178/2002 y el Reglamento (CE) nº 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo. [36]	• La evaluación clínica relativa a la seguridad. • La garantía de que los datos generados en investigaciones clínicas sean fiables y sólidos y que se proteja la seguridad de los sujetos que participen en dichas investigaciones. • La toma de medidas adecuadas por parte de la autoridad competente cuando el fabricante no colabore a fin de garantizar la protección de la salud pública y la seguridad de los pacientes. • La exigencia por parte de las autoridades competentes al fabricante de adoptar medidas pertinentes para velar por la seguridad de los pacientes. • Las disposiciones adoptadas para dar cumplimiento a las normas aplicables en materia de protección y confidencialidad de los datos personales. • Las medidas que se aplicarán en caso de filtración de la seguridad de los datos, para mitigar sus posibles efectos adversos.
14. 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. [37]	• La prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas. • La prevención ante otros sistemas de información interconectados. • El registro de las actividades de los usuarios, reteniendo la información necesaria para registrar las actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa con plenas garantías contra el derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados.
15. Norma UNE-EN 80001. Aplicación de la gestión del riesgo para las redes de tecnología de la información que incorporan dispositivos médicos. [38]	• La gestión del riesgo del ciclo de vida de los dispositivos médicos. • La responsabilidad del fabricante del dispositivo médico. • El plan de gestión del riesgo del dispositivo médico.

	• El control del riesgo del dispositivo médico. • La definición de los roles, responsabilidades y actividades requeridas para la gestión de riesgos de las redes informáticas en las que se utilizan dispositivos médicos con el fin de identificar y garantizar que los dispositivos médicos se incluyan en las redes de tecnología informática para lograr las características deseadas como interoperabilidad, eficiencia y seguridad de los datos y del sistema.
16. Normas UNE-ISO 27001. Sistemas de Gestión de la Seguridad de la Información. [39]	• Los requisitos que ha de cumplir un sistema de gestión de la seguridad de la información. • El objetivo principal de garantizar la protección de la información para evitar su pérdida o robo. • La confianza y credibilidad de la entidad. • El compromiso de la organización con la seguridad.
17. Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social. [40]	• La función de informado, deliberar e intercambiar información con los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado y que sean responsables de ficheros con datos personales para tratar y asesorar sobre las medidas de seguridad técnica aplicables en los sistemas y servicios que les afecten y que utilicen tecnologías de la información y comunicaciones. • La creación de un Comité de Seguridad de los Sistemas de Información en el ámbito de la Seguridad Social, como órgano colegiado con funciones de coordinación de aquéllos y de propuesta y aprobación de las medidas conducentes al cumplimiento de la política de seguridad a que obliga el Esquema Nacional de Seguridad.
18. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. [41]	• La definición de los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas. • La publicación de las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico por parte de las administraciones públicas especificando las condiciones de seguridad aplicables. • La conformidad a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

	• La conservación de los documentos electrónicos según lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad. • La competencia en materia de ciberseguridad y criptografía del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia. • Las medidas que se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios.
19. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. [42]	• La garantía de la confidencialidad de los datos sobre infraestructuras estratégicas y de los planes que para su protección se deriven, según la clasificación de la información almacenada. • Las especiales obligaciones que deben asumir tanto las administraciones públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas. • El servicio esencial como aquel necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. • Las infraestructuras críticas como aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
20. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. [43]	• La finalidad principal del catálogo en la valoración y gestión de los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza contra aquéllas. • El planeamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación. • El Plan Nacional de Protección de las Infraestructuras Críticas como el instrumento de programación del Estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.
21. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de	• La necesidad del diseño de una política de seguridad homogénea e integral en el seno de las organizaciones que esté específicamente dirigida al ámbito de las infraestructuras críticas, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de

Seguridad del Operador y de los Planes de Protección Específicos. [44]	impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población. • El análisis de riesgo plasmando las amenazas intencionadas, tanto de tipo físico como a la ciberseguridad, que afecten de forma específica a alguno de los activos que soportan la infraestructura crítica. • El CERT de Seguridad e Industria, en aplicación del Acuerdo Marco suscrito entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, que da apoyo directo al CNPIC en todo lo relativo a la prevención y reacción ante incidentes que puedan afectar a las redes y sistemas de los operadores de infraestructuras críticas y a la disponibilidad de los servicios que éstos prestan.
22. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. [45]	• El derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y que regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las administraciones públicas. • El uso por parte de las administraciones públicas de las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias. • El intercambio electrónico de información garantizando la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan. • La formación específica que recibirán los empleados públicos de la Administración General del Estado que garantice conocimientos actualizados de las condiciones de seguridad de la utilización de medios electrónicos en la actividad administrativa, así como de protección de los datos de carácter personal.
23. Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. [46]	• Los sistemas de información que soporten las sedes electrónicas que deberán garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. • El acceso a los documentos originales que se realizará de acuerdo con las condiciones y límites que establece la legislación de protección de datos personales u otra legislación específica. • Las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establece el Esquema Nacional de Seguridad.
24. Real Decreto 1066/2001, de 28 de	• El establecimiento de las condiciones de protección del dominio

septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas. [47]	público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas. • La precisión del procedimiento de determinación de los niveles de emisión radioeléctrica tolerables y que no supongan un peligro para la salud pública. • La coordinación de las competencias del Ministerio de Ciencia y Tecnología, en relación con los límites de emisiones y gestión y protección del dominio público radioeléctrico, con las competencias sanitarias del Ministerio de Sanidad y Consumo.
25. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. [48]	• La regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación. • La infracción por el incumplimiento deliberado de las obligaciones de protección y seguridad de los datos. • El deber de los sujetos obligados a identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados.
26. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. [11]	• La definición de servicio esencial como aquel servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información. • El deber de los operadores de servicios esenciales y los proveedores de servicios digitales de adoptar medidas adecuadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilicen, aunque su gestión esté externalizada.
27. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. [12]	• La autoridad competente en la materia respecto al sector de la salud es el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad. • El objeto es desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

28. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. [49]	• El objeto de regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. • Los procedimientos de gestión de incidentes de seguridad en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales. • La aplicación del real decreto a todo el sector público.

5. Ciberincidentes en infraestructuras y dispositivos sanitarios

Existen diversas ciberamenazas sobre infraestructuras y dispositivos sanitarios que han sido tan extendidas e inherentes al propio sector, que sería imposible hablar sobre su ciberseguridad sin mencionarlas.

Por un lado, el ransomware es la que más incidentes y pérdidas económicas ha generado en la sanidad a nivel mundial. Pese a no ser una amenaza de naturaleza sanitaria propiamente dicha, como podría ser el acceso indebido a historias clínicas, ha afectado tan cuantiosamente a la infraestructura sanitaria, que se considera ya casi inherente a este sector. Especialmente durante la crisis del COVID-19.

Por otro lado, existe una ciberamenaza de la que, si bien por diversos motivos no se han registrado, de momento, muchos casos de incidentes, afecta enormemente al sector de la salud como han constatado varios organismos oficiales. Esta es la relativa al secuestro de dispositivos médicos, denominado técnicamente “medjacking”.

Finalmente, se tratará otro de los ciberincidentes que mayor repercusión tiene en el sector de la salud dada su facilidad de perpetración, que suele ser cometido por el mismo personal interno e incluso facultativo y el carácter legal especial de los datos vulnerados. Este es el acceso ilícito a las historias clínicas de pacientes.

5.1 Ciberincidentes de ransomware

En ransomware es un tipo de malware que infecta a los equipos y dispositivos impidiendo el acceso a los datos almacenados, normalmente encriptándolos.

La diferencia con la mayoría de los virus informáticos es que su objetivo no es extraer información, sino exigir, a cambio de devolver el acceso a los datos, un rescate generalmente económico.

Una vez que ha infectado a un equipo, el ransomware intentará propagarse al resto de los sistemas conectados en red con el fin de cifrar la mayor cantidad de datos posibles de la entidad a la que pretenda extorsionar.

Las principales afectadas son medianas y grandes empresas de buen nivel adquisitivo y que manejan datos críticos, bien para su continuidad o para la propia privacidad de las personas que gestiona: empleados y usuarios.

Esencialmente, el ransomware se subdivide en dos tipos:

- El de bloqueo, que bloquea todo el equipo excepto la ventana que permite el pago del rescate.
- El de cifrado, que permite utilizar el equipo a excepción de los datos cifrados.

Una vez que el ransomware ha tomado el control del equipo o de sus datos, sus efectos podrán revertirse mediante una clave de descifrado con algoritmos cada vez más complejos y avanzados que los ciberdelincuentes prometen facilitar a cambio del rescate. Hay que destacar que el pago del rescate no siempre logra la recuperación del sistema, pero sí potencia y vivifica la acción cibercriminal, por lo que las autoridades oficiales en materia de ciberseguridad lo desaconsejan como primera opción.

El año 2020 derivó en una oleada de ataques ransomware sin precedentes y de características incontrolables debido al contexto internacional que se venía cosechando desde el año anterior.

En primer lugar, el mundo había entrado recientemente en una crisis sanitaria, la del COVID-19, que tenía saturados los servicios públicos y de salud en todo el planeta. A ello, se le sumó el aumento del teletrabajo a un ritmo apresurado y sin tiempo apenas para garantizar la seguridad de esta nueva modalidad laboral adoptada para evitar contagios.

Adicionalmente, Microsoft dejó de prestar soporte a los sistemas Windows 7 y Windows Server 2008, dejando expuestos y vulnerables a muchos de los sistemas sanitarios que funcionaban incluso en versiones más antiguas por temas de eficiencia de sistemas sanitarios, continuidad de servicios clínicos y compatibilidad con otros sistemas.

Con la mayoría de las empresas expuestas a Internet, la excesiva carga de trabajo y la criticidad de las administraciones públicas y especialmente las de los servicios de salud; los cibercriminales vieron el momento idóneo para atacar a estas infraestructuras. Se modificaron e incluso crearon ransomwares más evolucionados, dedicados a determinados sectores como el de la salud, y con mecanismos criptográficos avanzados con el fin de infectar al mayor número de entidades, públicas y privadas, cuanto más críticas, mejor.

El nuevo ransomware no solo era más eficaz, sino que reducía el tiempo de cifrado de datos y ofrecía la posibilidad de ejercer la doble o incluso triple extorsión:

1. Exigencia económica a la entidad para recuperar los datos cifrados.
2. Secuestro de datos de la empresa con el fin de publicarlos en caso de no obtener el rescate.
3. Exigencia de rescate también a los pacientes de la entidad bajo la amenaza de publicar sus datos tanto de salud como personales.

Por supuesto, los ataques a hospitales en plena crisis sanitaria terminaron con víctimas mortales. En un hospital de Dusserdorlf, Alemania, una mujer murió durante un ataque de ransomware. La paciente gravemente enferma tuvo que ser trasladada a un hospital cercano en ambulancia debido al bloqueo del centro atacado, falleciendo en el trayecto. Esta muerte se convirtió en el primer caso de fallecimiento registrado debido a un ciberataque.

Otro de los factores de mayor crecimiento de ciberataques es la reciente guerra ruso-ucraniana que si bien lleva librándose desde el año 2014, se ha intensificado durante el presente año con la invasión de Ucrania.

Uno de los más grandes y recientes incidentes de ransomware en el ámbito sanitario en España fue el ocurrido el pasado mes de octubre sobre los hospitales catalanes del Moisès Broggi de Sant Joan Despí; el Dos de Maig de Barcelona y el hospital Creu Roja de L'Hospitalet de Llobregat, además de una decena de Centros de Atención Primaria (CAP). El grupo criminal RansomExx, haciendo uso de

la doble extorsión, secuestró según informó 52,75 gigas de información y amenazó con publicarla en la dark web. Este ataque también derivó en la inoperatividad de diversos servicios imprescindibles tales como el de correo electrónico del personal hospitalario durante varios días.

5.2 Ciberincidentes de secuestro de dispositivos médicos (medjacking)

El secuestro de dispositivos médicos conocido como medjacking (medical device hijacking) es un tipo de ataque cibernético destinado a vulnerar los dispositivos médicos.

En sus inicios, los sistemas sanitarios eran grandes artefactos de ubicación fija y coste desorbitado que solo podían hallarse en algún hospital de relevancia. Poco a poco, su cada vez más extendido y valorado uso hizo que fueran activos indispensables en cualquier hospital e incluso centro de salud de atención primaria.

Los avances de la tecnología médica siempre han sido precipitados por la emergencia sanitaria de las necesidades y crisis que los propiciaron, la obsolescencia y rápida evolución y la competición económica de las grandes comercializadoras. Esto ha conllevado a que sus pasos, si bien agigantados, casi nunca han sido del todo seguros.

Otro de los factores que ha impedido gestionar en tiempo y forma la detección y corrección de vulnerabilidades ha sido el gran coste de su mantenimiento correctivo y evolutivo, o el de licencias cuando se debía solventar con renovación o sustitución del equipo.

Por otro lado, la sobrevaloración del avance clínico y funcional ha dejado siempre a la sombra el desarrollo técnico de aspectos tales como la ciberseguridad de los sistemas sanitarios.

De manera análoga, ha prevalecido la eficiencia y compatibilidad de los sistemas sanitarios sobre su propia seguridad. Se han desechado o postergado parches y actualizaciones cuando se ha previsto que podrían perjudicar a la eficacia o continuidad momentánea de un servicio hospitalario.

El conglomerado de vulnerabilidades de distintos o iguales tipos de causas ha puesto en bandeja de plata los sistemas sanitarios a los atacantes y, colateralmente, la totalidad de la infraestructura. De hecho, la intrusión a estos sistemas en muchos casos solo ha sido la puerta de entrada a los verdaderos objetivos en los hospitales, más suculentos y mejor salvaguardados, mediante ataques laterales.

Actualmente, las grandes y genéricas máquinas de electromedicina han reducido tanto su coste como su tamaño, convirtiéndose en dispositivos personales. Pueden ser así portados por el paciente, instalados en su domicilio e incluso implantados en su propio cuerpo. De esta manera, gestionan y hasta controlan funciones vitales para el paciente las 24 horas del día. En estos casos y de manera metafórica, la infraestructura sensible ante un ataque lateral es el propio paciente.

Si la reciente tercera extorsión del ransomware consiste en extorsionar al propio usuario a cambio de no publicar sus datos, en el caso del medjacking en implantes, el atacante podría exigir un rescate a una persona a cambio de no causarle la muerte a él o a un ser querido.

Además, mediante el IoMT (Internet of Medical Things), los dispositivos salen a Internet, con lo que son accesibles a nivel internacional. No sería difícil suponer que, tras el descubrimiento o la publicación de una determinada vulnerabilidad en un extendido modelo de marcapasos conectados a la IoMT, un grupo cibercriminal podría exigir el pago de un rescate a una o varias entidades (un fabricante, un gobierno, etc.) a cambio de no provocarle la muerte de forma remota a cientos o miles de usuarios de ese implante.

Sumado a esto, los implantes son dispositivos que en ocasiones requieren de una cirugía para su extracción y sustitución o parcheado tras el descubrimiento de una vulnerabilidad, por lo que tomaría bastante tiempo corregirla a nivel mundial. Tiempo que jugaría a favor de los cibercriminales.

A nivel de incidentes, el de los dispositivos médicos puede ser uno de los casos más controvertidos. Es un secreto a voces la infinidad de vulnerabilidades que contienen estos artefactos por los diversos motivos ya mencionados. Entonces, ¿por qué no trascienden apenas casos de ciberincidentes relacionados con los dispositivos médicos?

Bien es sabido que existen múltiples intereses, no solo comerciales sino también de seguridad pública, que hacen que anunciar sus vulnerabilidades pueda terminar en un exterminio a nivel internacional. Conjuntamente, desde el punto de vista reputacional, ni a un fabricante ni a su cliente le conviene que se divulgue haber suministrado, comprado e incluso implantado dispositivos que afectan a la salud pública.

Asimismo, se encuentra el hecho de que las herramientas de ciberseguridad de los centros sanitarios no están especializadas en las arquitecturas hardware y software de los dispositivos médicos, por lo que en muchas ocasiones las infecciones ni siquiera llegan a ser detectadas.

Finalmente, son reseñables desde el punto de vista criminológico varios aspectos que podrían explicar por qué no son tan frecuentes:

- Los grupos cibercriminales suelen perseguir delitos económicos de gran calibre haciendo o amenazando con hacer el mayor daño posible de forma simultáneamente y no persona a persona.
- Prefieren amenazar a grandes entidades, cuanto más pudientes mejor, en vez de a pacientes individuales.
- Los grupos cibercriminales optan por propagar sus ataques de manera automatizada para llegar al mayor número de víctimas posible. Los ataques a dispositivos médicos suelen requerir algo de gestión humana para impedir que termine en muerte antes de poder proceder al lucro.
- La pena, persecución y percepción social de un ciberdelincuente que comete delitos económicos se puede ver gravemente perjudicada si deriva en delitos contra la vida humana.

De todas formas, es demasiado improbable, de momento, que las muertes humanas sean investigadas por forenses informáticos pese a que las víctimas lleven implantados dispositivos médicos electrónicos. Con lo que los casos podrían pasar desapercibidos.

Uno de los fabricantes de dispositivos médicos peor parados en los últimos años en cuanto a vulnerabilidades detectadas es la compañía estadounidense Medtronic.

En 2019, la FDA presentó una advertencia oficial sobre las vulnerabilidades de seguridad de dispositivos de su firma tales como bombas de insulina [16]. A la FDA le preocupaba que, debido a las vulnerabilidades de seguridad cibernética identificadas en los dispositivos, un atacante pudiera conectarse de forma inalámbrica a una bomba de insulina y cambiar la configuración de esta. Esto podría permitir que una persona modifique la administración de insulina a un paciente, lo que podría provocarle una hipoglucemia, una hiperglucemia o una cetoacidosis diabética; poniendo en riesgo su vida.

Las bombas retiradas del mercado fueron la bomba de insulina MiniMed 508 y las de la serie MiniMed Paradigm.

Medtronic no podía actualizar adecuadamente las bombas de insulina MiniMed 508 y Paradigm con ningún software o parche para abordar las vulnerabilidades de los dispositivos, por lo que proporcionó

bombas de insulina alternativas a los pacientes con capacidades de ciberseguridad integradas mejoradas.

Solo en los EE. UU., Medtronic identificó al menos a 4.000 pacientes que potencialmente usaban bombas de insulina vulnerables a ese problema distribuidas de manera directa.

De inmediato, Medtronic se vio obligada a publicar una carta de notificación a sus pacientes desde su página web [17].

Podría pensarse que, dada la gravedad del asunto y las consecuencias, Medtronic tomó fuertes medidas en cuanto a la garantía de la seguridad digital en sus dispositivos médicos. Especialmente, cuando la crisis sanitaria del COVID-19 dejó patente la importancia de asegurar los sistemas sanitarios. Pues bien, el pasado 19 de octubre de 2022, durante la confección del presente TFM, la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) informa de un problema de seguridad con el método de comunicación de las bombas de insulina MiniMedTM serie 600 [18].

Esta vez ha sido la propia empresa Medtronic quien ha identificado recientemente el problema a través de unas pruebas internas, conforme a las cuales, en circunstancias específicas, la comunicación entre los componentes del sistema de bomba MiniMed™ de la serie 600 pueden verse comprometidos mediante un acceso no autorizado.

Pero las bombas de insulina no son el único dispositivo médico con vulnerabilidades inalámbricas de Medtronic. El Departamento de Seguridad Nacional (DHS) de EE. UU. lanzó un aviso desde el 4 de junio de 2020 acerca de vulnerabilidades descubiertas en varias versiones y productos de dispositivos (implantes cardíacos) que utilizan el protocolo de telemetría Conexus de este fabricante [19].

Las vulnerabilidades afectan al control de acceso inadecuado (CVE-2019-6538, puntuación base CVSS v3 de 9,3) y a la transmisión de texto en claro de información sensible (CVE-2019-6540, puntuación base CVSS v3 de 6,5).

Un atacante podría explotar este protocolo de comunicación para cambiar los valores en la memoria del dispositivo cardíaco implantado, así como interceptar la transmisión de datos confidenciales a corto alcance ya que carecen de cifrado.

Investigaciones más detalladas descubrieron que en la práctica se podían realizar modificaciones que extraerían los datos personales de los pacientes y médicos, y realizar cambios no autorizados y potencialmente fatales en las descargas eléctricas que administran los desfibriladores implantados. La prueba realizada pudo leer y reescribir el firmware del implante [20].

Estas vulnerabilidades se corregirían mediante la aplicación de parches durante las visitas regulares al centro médico y, mientras tanto, Medtronic ha informado de una serie de recomendaciones defensivas a sus usuarios.

Actualmente, y como muestra de la poca importancia que existe en torno a la relevancia de la ciberseguridad en la salud, Medtronic se sitúa a la cabeza de las compañías del sector e-Health, por encima de Fresenius Medical Care, Philips Healthcare, General Electric Healthcare y Siemens Healthineers, entre otras; y con unas ganancias al alza.

Críticas como sus pruebas en animales, su traslado fiscal a Irlanda, o su negativa de retirarse del mercado ruso ante la invasión de Ucrania han desplazado a un segundo plano a sus constantes vulnerabilidades en materia de ciberseguridad.

5.3 Ciberincidentes de acceso ilícito a historias clínicas

Como se ha abordado en los apartados relativos al ransomware y al medjacking, el robo de información puede ser un procedimiento semiautomatizado e impersonal. Persigue extraer la mayor cantidad de información clínica sin importar los sujetos de los que proviene. Generalmente centra su objetivo en las entidades, normalmente servicios de salud y centros sanitarios.

Estos ciberdelitos se consuman en su mayoría por cibercriminales no relacionados con la profesión sanitaria ni con el centro donde se perpetra el ataque, siendo la mayoría de las veces procedentes de otros países.

No obstante, los datos clínicos personales son muy suculentos también para el ciudadano de a pie que no tiene por qué tener extensos conocimientos y destrezas en informática. Este atacante en muchas ocasiones pertenece al propio gremio sanitario e incluso es profesional del centro.

El acceso a información confidencial siempre ha sido una gran tentación para el ser humano que ha visto en ella un activo suministrador de morbo y poder. Los sistemas de información de historia clínica (SSIIHC) tales como el HIS (Hospital Information System) la ponen a disposición del usuario con un simple clic y en la intimidad de su oficina o incluso de su hogar con el auge del teletrabajo.

Esta ilusoria sensación de impunidad ha acarreado a varios profesionales del ámbito diferentes penas de multa, inhabilitación y hasta prisión.

A continuación, se mostrarán una serie de artículos del Código Penal [21] utilizados para sentenciar judicialmente la mayoría de los incidentes relativos a este delito en España.

Artículo 197 del Código Penal:

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

Artículo 198 del Código Penal:

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199 del Código Penal:

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos

de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Las historias clínicas de pacientes solo deben de ser accedidas por profesionales autorizados y con un motivo asistencial que lo motive.

No obstante, los profesionales médicos y enfermeros no son los únicos que acceden a esta información. De hecho, la mayor parte de esta información se encuentra almacenada en bases de datos y es gestionada por aplicaciones. Por ello, realmente quienes tienen mayor acceso a ella son precisamente los informáticos relacionados con la administración, el soporte, el mantenimiento y el desarrollo de estos sistemas que no se rigen por el código deontológico médico.

Por otro lado, aunque la mayor parte de la sanidad en España es pública, y el código penal sanciona de especial manera a los funcionarios que cometen los delitos en el desarrollo de su actividad profesional, existe un gran número de trabajadores privados. No solo en los centros sanitarios privados, sino prestando sus servicios a organismos públicos bajo diversas metodologías, por ejemplo, en la externalización de personal o servicios.

Una vez soslayadas las fronteras deontológicas y penales más rigurosas, cabría depositar la esperanza en las medidas de seguridad de los sistemas de información sanitarios y las normativas que los protegen durante todo su ciclo de vida. No obstante, como ya hemos visto con el medjacking, los procesos de digitalización del sector sanitario son a menudo precipitados y dejan una gran cantidad de deuda técnica, actos de fe y fallos a lo largo de su implementación.

Por ejemplo, es muy común el uso de bases de datos con datos reales en entornos de prueba o preproducción. Datos reales que a menudo se envían a otras entidades y sistemas externos en pruebas de interoperabilidad.

Los sistemas también suelen tener un gran déficit en la robustez de aspectos tan relevantes como el cifrado de la información o la autenticación.

El acceso, también a personal subcontratado, se suele dar a más recursos y con más privilegios de los realmente necesarios bajo sus funciones.

En adición, las aplicaciones tienden a ser programáticamente obsoletas, repletas de bugs, sin una auditoría de seguridad y con un desarrollo atropellado puramente funcional y sin mucho reparo técnico.

Por parte del personal, es frecuente el uso de cuentas de correo electrónico personales, pendrives propios o el ordenador de casa en sus tareas laborales.

Finalmente, hay un excesivo voto de confianza tanto a personal interno, como externo. En muchas ocasiones, el personal de la entidad de salud no llega a dar soporte y mantener las aplicaciones y bases de datos de proveedores que almacenan datos relativos a los pacientes de la misma.

De poco o nada sirve que se controle eficazmente la trazabilidad de accesos a la historia clínica del paciente en la interfaz de usuario de la aplicación sanitaria, si no se garantiza desde el propio sistema de gestión de bases de datos. Más aún, cuando los técnicos que consultan y gestionan dicha base de datos suelen ser de compañías externas y con un alto índice de rotación y nueva contratación. Además, no están relacionados de forma directa con la entidad sanitaria ni se acogen al régimen sancionador de la misma que en algunos casos es el de los funcionarios públicos.

Son múltiples las sentencias en España de casos relativos a este tipo de ciberdelito. Como muestra, podemos encontrar la noticia publicada en el portal web del Poder Judicial de España [22]:

La Sala II del Tribunal Supremo ha condenado a 2 años de prisión y 6 años de inhabilitación absoluta para desempeñar su profesión a una enfermera del Servicio Aragonés de Salud como autora de un delito de descubrimiento de secretos, por haber accedido al historial médico de una antigua amiga desde el Centro de Salud de Zaragoza donde trabajaba.

En síntesis, el relato fáctico refiere que la acusada, en su condición de enfermera del Servicio Aragonés de Salud, el día 30 marzo 2017 se encontró con una mujer con la que había tenido una relación de amistad que se había deteriorado, y tras un intercambio de palabras le dijo que "su marido era un cobarde y un sinvergüenza y que sabía que su hermana tenía el VIH, y que si quería que lo dijera, y otras palabras en el sentido de que iba desvelar información médica que tenía acceso por su profesión".

Narran además los hechos probados que la perjudicada denunció lo ocurrido, y que también lo comunicó a los servicios sanitarios de Aragón, que detectaron dos accesos a las bases de datos por la acusada al historial clínico de la perjudicada.

Uno de los máximos impedimentos para poder detectar los accesos indebidos a la historia clínica de los pacientes es impuesto precisamente por el artículo 15 del RGPD sobre el derecho de acceso del interesado. Y es que de entre toda la información de la que el interesado tiene derecho a obtener del responsable del tratamiento de sus datos clínicos, no está incluida la identificación de las personas que los han consultado.

En otras palabras, el paciente necesita proporcionar una sospecha fundamentada e identificar a una persona para conocer, de manera individual, si ha accedido de forma ilegal a sus datos clínicos. Algo extremadamente enmarañado que sin duda obstaculiza enormemente el descubrimiento de delitos de revelación de datos clínicos. Y es que, aun siendo por ley dueño de sus propios datos de salud, no puede solicitar todos los accesos que ha habido a su historia clínica de forma general.

6. Mecanismos de acción e infección

En este apartado se detallarán los mecanismos de acción e infección de las ciberamenazas descritas en el apartado anterior a nivel general, ya que puede variar dependiendo de la versión del malware o de la metodología del ataque.

6.1 Acción e infección del ransomware

La infección se produce en la mayoría de los casos mediante descargas de ficheros adjuntos o enlaces externos en correos electrónicos provistos de mensajes que utilizan la ingeniería social para engañar al usuario.

Otro de los factores de infección es la visita a sitios web inseguros o maliciosos a través del navegador, aprovechando vulnerabilidades en este o en el mismo sistema operativo.

También se han descrito casos de ataque bajo diferentes protocolos tales como el RDP o servicios como FTP, SSH, TELNET, etc.

Finalmente, y de forma colateral, el ransomware puede estar embebido en otro malware o bien provenir de otro sistema de la misma red.

Una vez que el ransomware llega a un sistema, recorre los archivos de cada una de sus unidades normalmente atendiendo a aspectos tales como el tipo o la extensión de los mismos.

Usualmente, identifica los archivos que ha cifrado estableciéndoles una determinada extensión (.aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault o .petya, etc.) en dependencia del ransomware.

Cuando ha terminado su acción, ya sea encriptar datos, secuestrarlos o bloquear el equipo, muestra por pantalla una ventana con información relativa a la infección y el pago del rescate.

Las criptomonedas son las divisas preferidas por los ciberdelincuentes para exigir el rescate, especialmente el Bitcoin. La pseudoanonimización es el primordial atractivo de estas, seguido por su internacionalidad y casi nulo control por parte de los organismos públicos y bancarios.

Suelen sumársele diversos factores para aumentar el enredo a su posible rastreo, tales como utilizar ubicaciones de ataque de países opacos o con difíciles relaciones políticas. También, el uso de monedas como Ethereum y Monero, provistas de menor trazabilidad, o la utilización de servicios como CoinJoin o Coin Ninja, para entremezclar su rastro.

6.2 Acción e infección del secuestro de dispositivos médicos (medjacking)

En el apartado sobre la descripción de este ciberincidente se ha detallado en mayor medida el ataque a dispositivos sanitarios implantados en pacientes tales como los de Medtronic. No obstante, y como se demostrará en este apartado, el medjacking puede ser perpetrado sobre los equipos médicos (máquinas de diálisis, TAC, resonancias magnéticas, electrocardiogramas, etc.) e incluso servidores (de aplicaciones de historia clínica, departamentales, BBDD, almacenamiento de pruebas radiológicas, etc.) que albergan los hospitales.

El procedimiento, como norma general, comienza con la infección un sistema mediante un malware que se descarga a través de diferentes métodos (e-mail, páginas web, ingeniería social, memorias USB, tarjetas, etc.) o bien de forma colateral a través de la red. Aunque existen diversos métodos de obtención de acceso al dispositivo.

Las vulnerabilidades explotadas pueden ser tanto del propio sistema sanitario (por ejemplo, el software que lo gestiona o un protocolo propio del fabricante), el sistema operativo, etc. Se sabe que gran parte de los sistemas médicos están sobre sistemas operativos Microsoft Windows 95, 2000, XP y 7, sin soporte oficial desde hace ya varios años por parte de Microsoft.

A menudo, las herramientas de seguridad no están diseñadas para acceder al interior de los sistemas y dispositivos sanitarios (discos, memorias y procesadores internos) por su especificidad, por lo que un malware puede pasar inadvertido durante mucho tiempo e incluso de forma permanente debido a este hándicap.

Otro de los factores que obstaculiza la detección del malware es que estos sistemas suelen estar certificados oficialmente o provistos de licencias que podrían impedir el acceso al personal interno de la entidad sanitaria que lo adquirió o incluso al del mismo proveedor.

Por si esto fuera poco, en algunos países existen normativas que regulan la no manipulación de este tipo de sistemas sanitarios.

Los mecanismos de acción e infección utilizados en el medjacking son muy variados, ya que tratan de analizar y aprovecharse de una o varias vulnerabilidades del sistema y, de esta forma, conseguir uno o varios objetivos.

En muchas ocasiones, los datos de acceso a los sistemas sanitarios e incluso a las VPN de las infraestructuras hospitalarias son vendidas en la dark web. Los ciberdelincuentes pueden comprar

estos datos y acceder a su red ocultando su verdadera IP mediante diversas técnicas que además garantizan que esta no se encuentre en ninguna lista negra.

Una vez dentro del sistema, el atacante intentará escalar privilegios y deshabilitar herramientas de seguridad tales como antivirus.

Analizará tanto los datos del propio sistema, como los de los recursos compartidos mediante protocolos como SMB, robándolos mediante FTP o el propio túnel SSL.

Examinará las redes adyacentes con el fin de poder perpetrar el ataque en más sistemas o llegar al objetivo principal. Podrá utilizar protocolos como RDP o SSH para llegar a otras máquinas destino, ya sean ordenadores personales, tablets, servidores o sistemas sanitarios tales como el de resonancia magnética, TAC, etc.

Podrá descargar software malicioso especialmente diseñado para conseguir sus fines. Es frecuente el uso de exploits en este tipo de ataques, así como el movimiento lateral (pivoting) entre máquinas usando técnicas tales como Pass the hash (PtH).

El malware descargado a la máquina infectará varios archivos y se propagará a través de diferentes medios como unidades locales y extraíbles, emails y recursos compartidos. Realizará las modificaciones pertinentes sobre el sistema (entre otras cosas para evitar su detección y neutralización) y sus cuentas de usuario. De esta forma, ganará privilegios y conferirá más eficacia al ataque. Se mantendrá en memoria RAM, infectando procesos en ejecución, pero también en otros recursos no volátiles para poder resistir a un reinicio.

Una vez culminada la infección y habiéndose afianzado en el sistema, estará en condiciones de consumar el/los objetivo/s del ataque, ya sea controlar uno o varios equipos electromédicos, robar información médica o financiera de servidores, alterar el comportamiento de un sistema automatizado mediante IA, falsear datos de interoperabilidad entre sistemas, etc.

Cuando haya concluido, el atacante intentará borrar las huellas y permanecer desapercibido dentro de la infraestructura sanitaria para garantizar seguir delinquiendo o vender nuevos datos en la dark web.

Cabe recordar y adicionar una serie de factores que propician la efectividad de los mecanismos de acción e infección en medjacking:

- Los dispositivos médicos son cerrados en cumplimiento de algunas normativas gubernamentales, por lo que no hay demasiada visibilidad sobre lo que ocurre en su interior y con ello se dificulta la monitorización de los mismos. En otras muchas ocasiones, son sistemas protegidos que, por razones de propiedad intelectual o de licencia comercial, no permite el acceso de los técnicos de la entidad sanitaria e incluso del proveedor.

- Además, aunque a nivel de plataforma suelen compartir características comunes con otros sistemas sanitarios, poseen características de arquitectura propias e incluso obsoletas, tales como determinados procesadores integrados que en ocasiones son desconocidos por las herramientas de seguridad utilizadas por el departamento de informática de la entidad.

- El creciente uso del IoMT en los dispositivos médicos también complica la monitorización y la protección de estos por parte del personal técnico de la infraestructura sanitaria dada su alta conectividad, el alto número de dispositivos o la diversidad de tecnologías que implementan.

- Los centros deben mantener ciertos sistemas electromédicos en continuo funcionamiento para no ocasionar el corte de un servicio sanitario esencial.

- Las tareas de corrección de vulnerabilidades o desinfección de los equipos a menudo deben de ser realizadas o cubiertas económicamente por la propia entidad hospitalaria.

- Normalmente, la infección afecta a varios dispositivos conectados a la red de la infraestructura sanitaria, por lo que comúnmente hay que desinfectarlos a todos para evitar la reinfección una vez se vuelvan a conectar los que habían sido restaurados.

6.3 Acción e infección del acceso ilícito a historias clínicas

Como se ha visto en el apartado descriptivo de este ciberdelito, puede perpetrarse bajo diferentes procedimientos y, de hecho, el más usual es mediante el normal acceso al sistema de información de historia clínica al que el atacante tiene acceso. Obviamente, tener acceso al sistema de información de historia clínica (SIHC) no implica tener acceso legítimo a las historias clínicas de todos los pacientes. Pero la carencia de medidas de seguridad hace que lo facilite en gran medida. Y es que la incorrecta segregación de roles o privilegios en los usuarios de los SSIIHC hace posible que puedan acceder a módulos y secciones que no corresponden a sus funciones profesionales.

Por ejemplo, un profesional administrativo no tendría por qué poder acceder a la historia clínica de un paciente y, de hacerlo, estaría infringiendo un delito.

Otro de los procedimientos se da cuando el atacante sí es personal de medicina o enfermería, pero el paciente no pertenece a su cupo asistencial ni hay razones asistenciales que motiven el acceso, por lo que, de acceder a sus datos de salud, violaría la confidencialidad de estos.

Hasta el momento, se han descrito dos mecanismos de acción para los que no se precisan de grandes habilidades ni conocimientos informáticos a través del normal acceso al aplicativo que muestra los datos de historia clínica. Sin embargo, existen mecanismos que, directa o indirectamente, también vulneran la confidencialidad de los datos.

Sin ahondar en procedimientos demasiado ambiciosos desde el punto de vista de la ciberseguridad, existe el caso del personal que en el corriente ejercicio de su labor debe visualizar cotidianamente datos de salud reales. Estas labores suelen ser funcionales, estadísticas, de investigación científica, de desarrollo de software sanitario, etc. Cuando sus funciones requieran trabajar con datos clínicos, se le debe imposibilitar la identificación del paciente. Pese a todo, en varias ocasiones no se suele acudir a medidas que lo garanticen tales como la anonimización de los datos.

Las propias BBDD productivas son utilizadas para realizar pruebas no solo OSAT (pruebas de aceptación en sitio), sino también de aceptación del sitio (SAT) o incluso de aceptación de fábrica (FAT). Esto supone el almacenamiento y la utilización de datos reales personales y clínicos de pacientes en entornos sin control de ningún tipo y por personal técnico que en la mayoría de las ocasiones es externo a la entidad sanitaria.

A veces, pese a su buena intención, las medidas de seguridad no están correctamente analizadas en todo su contexto y puede tenerse la errónea percepción de que la confidencialidad de los datos personales y de salud de los pacientes está asegurada cuando realmente no es así.

Caso de ejemplo:

Eve ha sido contratada como especialista estadístico de una gerencia de atención primaria. Su función es realizar análisis estadísticos clínicos para el control de la diabetes.

Para ello, cuenta con un perfil en el aplicativo SaludEstadistica, que muestra datos clínicos, pero que oculta los personales de los pacientes garantizando que no puedan ser identificados. Estos datos de

salud solo se encuentran enlazados a un código interno. De hecho, se decide que la trazabilidad del aplicativo SaludEstadistica no tiene que ser registrada.

Recientemente y debido a la baja laboral de un compañero, le ha sido asignada la nueva tarea de realizar también análisis estadísticos demográficos de pacientes para concluir si normalmente acuden al servicio de Urgencias del centro de salud de su zona o al de otro.

Para esta nueva tarea, se le da acceso al aplicativo DemograficoEstadistica, con los datos personales y domiciliares de los pacientes (pero sin sus datos clínicos) y ejecutada de forma aislada de SaludEstadistica. En este caso, los pacientes también poseen su código interno.

Así pues, Eve, con acceso a ambas aplicaciones, podría identificar a un paciente en el aplicativo DemograficoEstadistica y, mediante su código interno, encontrar y acceder a su historial clínico en el aplicativo SaludEstadistica. Esta actividad, además, no sería registrada.

Uno de los profesionales con más privilegios y perfiles diferentes en los aplicativos, y que, por lo tanto, mayor trazabilidad y cautela por parte la entidad ha de tener, es el de soporte. Por comodidad, con frecuencia el personal de soporte pertenece a la empresa externa desarrolladores o proveedora del sistema sanitario. No obstante, es recomendable usar para estar labores a personal interno, ya que a menudo requieren visualizar datos reales para auxiliar a usuarios o validar incidencias.

Para evitar la descontextualización en la definición de las medidas de seguridad, tal y como se ha hecho hincapié a lo largo del TFM en la importancia del personal técnico, los conocimientos del personal funcional clínico también son fundamentales para establecer las reglas usuario-rol-operación de los sistemas, además de otras cuestiones.

Pese a que se ha recurrido a mecanismos simples para demostrar la facilidad con la que se vulneran día a día los datos clínicos en los centros sanitarios, existen ataques más sofisticados que permiten acceder a la información clínica de los sistemas de manera indebida.

Un ejemplo de ello es el ataque MITM (Man-in-the-Middle). En la comunicación entre dos sistemas (por ejemplo, el cliente y el servidor de un HIS (Hospital Information System)), un atacante puede hacerse pasar por la dirección de destino e interceptar las comunicaciones con técnicas como el Spoofing de IP, ARP o DNS. Tras la obtención de los datos, podrá utilizar métodos para desencriptarlos como el HTTPS Spoofing, el Secuestro de SSL o el SSL Stripping.

Existen hechos que aumentan su facilidad, como el de que en muchos sistemas sanitarios los datos ni siquiera se transmiten cifrados. Además, es muy común encontrar puntos de red en los pasillos de los hospitales o poner a disposición de los pacientes y el personal una Wi-Fi sin tener la red debidamente aislada ni segmentada.

7. Medidas de prevención

El propósito de este apartado no es abarcar las medidas genéricas de prevención de ciberincidentes sino la de centrarse específicamente y con mayor ahondamiento en las de mayor implicación en la protección ante los principales ciberincidentes sanitarios tratados en el proyecto.

Por supuesto, algunas de las medidas tienen sentido en cualesquiera de las tres ciberamenazas, pero se ubicarán en la de relación más directa para evitar la redundancia. La diferenciación en los tres grupos se hace útil en beneficio del análisis unitario. No obstante, en la práctica es de interés reunir todas las medidas para proporcionar una mejor y más integral protección a la infraestructura sanitaria. Estas medidas prevendrán incluso de otras ciberamenazas no analizadas en este trabajo.

Prevención del ransomware	Prevención del medjacking	Prevención del acceso ilícito a HHCC
Organizativas/procedimentales: • Respaldo frecuente, completo y aislado de la información. • Crear puntos de restauración bien clasificados. • Prácticas y medidas de navegación segura. • Contratación de un ciberseguro. • Políticas de seguridad de directorios como App Data, Local App Data o directorios temporales. • Mantener listas de control de acceso para las unidades mapeadas en red. • Identificar cuáles son los ficheros ejecutables. • Medidas antispam. • Promover el uso de máquinas virtuales. • Mantener una reputación de no ceder ante extorsiones económicas. • Medidas contra la ingeniería social. • Mantener vías de contacto ágiles con los usuarios de la red ante incidentes. • Fomentar la colaboración en materia de ciberseguridad entre los diferentes centros de la red sanitaria. • Constante actualización en las últimas estrategias y versiones de ransomware. **Técnicas:** • Herramientas anti-ransomware específicas. • Herramientas antivirus. • Segmentación de red de la infraestructura. • Bloqueadores de código script. • Mantener actualizadas las aplicaciones y el sistema operativo. • Utilizar versiones de sistemas operativos y aplicativos actuales y con soporte oficial. • Control de correos sospechosos.	**Organizativas/procedimentales:** • Medidas eficientes de control de acceso físico. • Prácticas y medidas de descarga segura. • Medidas de detección de malware. • Evaluar la seguridad y la necesidad de los protocolos y servicios. • Políticas de seguridad de contraseñas. • Reducir el uso de cuentas de administrador cuando no sean necesarias. • Cambiar las contraseñas por defecto de los sistemas. • Utilizar puertos no predeterminados. • Usar políticas White Lists. • Establecer un máximo de intentos de acceso relativamente bajo. • Utilizar comunicaciones seguras en los dispositivos. • Evitar dejar puertos de entrada y accesos desprotegidos. • Evitar contratar sistemas cerrados u opacos. • Contratación de personal y dispositivos de vigilancia y seguridad integral. • Evaluar la seguridad de los sistemas adquiridos a terceros: acceso, transmisión de datos, etc. • Seguimiento de las últimas noticias de seguridad de los fabricantes. • Análisis continuo de vulnerabilidades. **Técnicas:** • Uso de estándares de cifrado avanzado en redes y autenticación. • Actualizaciones y parcheado de los sistemas. • Técnicas de autenticación robusta. • Sistemas de detección de intrusiones (IDS).	**Organizativas/procedimentales:** • Trazabilidad profunda y eficiente. • Auditorías continuas. • Procedimiento de mejora continua de software. • Correcta definición de roles y niveles de acceso. • Evitar los medios externos de almacenamiento. • Evitar el uso de equipos y correos personales en el trabajo. • Formación en seguridad de la información. • Campañas de concienciación y sensibilización. • Definir políticas y procedimientos del ciclo de vida de los datos. • Constante actualización en normativa de protección de datos personales. • Cláusulas contractuales con empleados y proveedores. • Proteger especialmente el almacenamiento de datos clínicos o personales, principalmente en la nube. • Proteger especialmente la interoperabilidad de datos clínicos o personales, principalmente a través de Internet. • Evitar la externalización para puestos en los que se manejen datos clínicos o personales. • Evitar el teletrabajo con aplicaciones que gestionen datos sensibles. • Buenas prácticas en desarrollo de software. • Modularizar de forma independiente las plataformas de software. • Impedir extraer BBDD productivas para fines de pruebas y preproducción.

• Control de carga y uso de los recursos CPU, RAM, HD, etc. • Control del aumento del tráfico de red.	• Sistema de prevención de intrusiones (IPS). • Pruebas desafío-respuesta para evitar autómatas. • Factores adicionales de autenticación. • Firewalls. • Implementación de un Acceso a la red Zero Trust (ZTNA).	• Anonimización y seudoanonimización de datos sensibles. • Asesoramiento funcional sobre las actividades pertinentes de cada rol. • Evitar los accesos desprotegidos a la red. **Técnicas:** • Protocolos de cifrado de transmisión de datos. • Dispositivos de control de acceso y videovigilancia. • Herramientas de análisis de vulnerabilidades de software.

8. Gestión de incidentes: medidas de contención y contramedidas

Cuando la prevención no ha sido suficiente y el ataque ha conseguido llegar al interior de la infraestructura sanitaria (ya sea un centro de salud, una gerencia hospitalaria, un servicio de salud, el sistema nacional o incluso a nivel comunitario europeo), la mejor defensa es una buena gestión de incidentes. Este apartado se centrará en esta área de procesos que abarcará, entre otras prácticas, la aplicación de medidas de contención y contramedidas.

La parte de prevención de ciberincidentes se ha separado de este apartado con el fin de enumerar de manera específica y holgada varias medidas para cada una de las amenazas estudiadas.

No obstante, este apartado centrará su esfuerzo en la correcta realización de un plan de gestión de incidentes completo, que no dejará de contener las medidas de contención y las contramedidas, pero a un nivel más genérico. Esto es debido a la importancia no solo de estas, sino de todo el plan. De nada serán útiles las más sofisticadas medidas de contención y contramedidas si no hay detrás una buena metodología y un eficiente procedimiento que certifique el óptimo orden y las actividades precisas de todas las demás fases en su conjunto.

De todas maneras, las medidas de contención y contramedidas específicas para cada una de las tres ciberamenazas serán, normalmente, la puesta en marcha y adecuación de las medidas de prevención que se han visto en el apartado anterior. Dichas medidas deberán ser implantadas de manera activa y ajustándose a las conclusiones, decisiones y datos recogidos en las fases estudiadas en este apartado que preceden a la fase de contención y que dependerán del ciberincidente acontecido y su contexto.

Se conoce como gestión de incidentes de seguridad de la información a un conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible [22].

El coste de la recuperación del control y el servicio afecta a factores tales como el tiempo dedicado, los recursos necesarios o los daños sufridos.

Existen seis fases bien diferenciadas:

8.1 Preparación

Es la adecuación de los pilares fundamentales en cualquier entidad sanitaria:

- Las personas: especialmente los empleados internos y externos con acceso a los sistemas de la infraestructura sanitaria. Pero siempre que sea posible, también los usuarios y pacientes, sobre todo si están ingresados, utilizan aplicaciones tales como el portal del paciente o acuden con asiduidad a realizarse tratamientos, por ejemplo, de hemodiálisis.

- Los procedimientos: todas las políticas, estándares, protocolos, medidas y demás procedimientos adoptados en beneficio de garantizar la seguridad de las instalaciones y la integridad, confidencialidad y disponibilidad de los datos tratados.

- La tecnología: los sistemas de información de historia clínica tales como el HIS, los departamentales como el RIS, los de almacenamiento como el PACS o el VNA, los implantados en los pacientes, los provistos de IoMT, los dispositivos y máquinas de electromedicina tales como las de diálisis; o las aplicaciones de pacientes tales como las de visualización de HC, acceso a pruebas e informes, solicitud de cita, etc. En general, todas aquellas tecnologías que estén conectadas o puedan ser conectadas de manera potencial a cualquier red (interna o externa) o se pueda acceder a ella, por ejemplo, mediante puertos de entrada.

En la fase de preparación se debe contar con todos los recursos técnicos y contactos personales necesarios, así como las instrucciones efectivas y los protocolos establecidos para cualquier tipo de adversidad.

Cobra especial importancia garantizar las comunicaciones ante cualquier tipo de ciberincidente. Pero, además:

- Disponer de una agenda de contactos ante incidentes clara y concisa.
- Estar en disposición de captar la trazabilidad de las evidencias.
- Tener actualizados los catálogos y diagramas de la infraestructura sanitaria.
- Mantener los procedimientos actualizados.
- Mantener formado y concienciado al equipo humano.
- Mantener protegidos los puestos de trabajo.
- Definir y actualizar cíclicamente un análisis de riesgos.
- Realizar ciberentrenamientos y simulacros periódicos.

8.2 Identificación

Solo conociendo el correcto funcionamiento de cada sistema sanitario de la infraestructura se pueden hallar aquellos eventos que se salen de la normalidad de este y, con ello, identificar sucesos anormales probablemente debidos a amenazas anticipadamente que, de materializarse, concluirían en incidentes. Por ello, es óptimo conocer qué se debe esperar de un sistema específico en todo momento e identificar inequívocamente los eventos, aplicando reglas si es posible para mantenerlos controlados.

En esta fase se deberá prestar especial atención a eventos funcionalmente desconocidos o de dudosa procedencia. Cualquier pequeño proceso puede llegar a producir un resultado desastroso en nuestro sistema cuando se le suman otras magnitudes tales como el tiempo, por ejemplo, en una fuga de memoria. Por lo tanto, la eficiencia, conjunción de eficacia y rapidez, se convierte en

imprescindible.

Se hace vital en esta fase:

- Recolectar información del estado y la situación de cada tecnología de la infraestructura sanitaria.
- Registrar y monitorizar los eventos esperados e inesperados.
- Registrar una óptima trazabilidad que identifique en todo momento: quién y cuándo hizo qué.
- Almacenar evidencias y trazabilidad que garanticen el no repudio.
- Detectar información fuera de lo normal.
- Auditar recurrentemente.

Como ya se ha visto en los ciberincidentes de este trabajo, existe una serie de vectores que se deben tener bajo control. Entre otros, estos son:

- **Correo electrónico**. Pueden contener enlaces o ficheros adjuntos maliciosos.

- **Vulnerabilidades conocidas**. Se ha descrito un auge en el sector sanitario del uso de microprocesadores y sistemas operativos obsoletos, falta de parches y actualizaciones en software y dispositivos médicos, etc.

- **Dispositivos de almacenamiento externo**. Hay que tener un gran cuidado no solo del malware que puede inocular al sistema sanitario. También de la información que puede extraer de él (técnica del sistema, clínica o personal de pacientes o empleados, de la organización, etc.).

- **Equipos de trabajo**. Ya sea por acción o por omisión, aquí se concentra la mayor entrada de software malicioso y operaciones indebidas. Y no solo hay que garantizar la seguridad en los equipos de trabajo de los empleados internos, sino de cualquier usuario que se conecte a la red de la infraestructura sanitaria: consultores externos, proveedores, etc.

- **Documentos**. Tales como historias clínicas de pacientes, nóminas, contratos con proveedores o protocolos de actuación ante incidentes.

- **Vectores externos**. Garantizar la seguridad interna es esencial, pero sin descuidar las amenazas externas que podrían comprometer los sistemas en los contextos menos prolíficos como demostró la crisis del COVID-19 o la guerra ruso-ucraniana en la ciberseguridad del sistema sanitario a nivel mundial.

8.3 Contención

Contener un ataque es impedir que se propague o haga mayor daño del ya provocado. Evitar que trascienda a otras redes o sistemas, que infecte más archivos, que extraiga más información o que logre perpetuarse en el sistema, entre otros objetivos. Para ello es clave conocer la infraestructura sanitaria y los medios puestos a disposición de su seguridad obedeciendo al protocolo establecido.

Pero no todo está escrito ni protocolizado y siempre hay decisiones que dependen del tipo de amenaza y sus magnitudes que deben ser tomadas de forma ágil ya que el tiempo es determinante en lograr lo explicado en el párrafo anterior. Cuanto mejor documentado se encuentre el plan de contención, mejor, pues se minimizarán las decisiones en caliente. Debería de ser versátil teniendo en cuenta, al menos, las ciberamenazas que, a día de hoy, se conocen. Pero a la hora de priorizar, se hace indispensable indagar en qué tipo de ciberamenazas suelen afectar más al sector de la

salud, de las cuales, ya se han estudiado tres de ellas en este trabajo.

Como se verá en la fase de actuaciones post-incidente, una bitácora que reúna cada decisión y paso tomado y en relación a qué hallazgos o razones, será de esencial interés. Este detalle también podría añadirse a la herramienta de gestión de incidentes de la organización sanitaria. Describir el proceso de acciones realizadas es transcendental sobre todo en situaciones que no se rigen por el procedimiento establecido, ya que puede requerirse más adelante tener que indagar sobre un paso dado o incluso revertirlo y que quizá ya no se recuerde.

Con todo, se puede concluir un análisis de situación que permita clasificar el ciberincidente para así determinar cómo gestionarlo, esclareciendo además algunas directrices para su posible resolución. Gracias a una taxonomía de ciberincidentes como la utilizada por INCIBE-CERT [23] basada en las mejores prácticas y en las recomendaciones de organismos internacionales relevantes en la materia, se podrán priorizar en dependencia de su tipo y peligrosidad.

Sin embargo, la evaluación del impacto producido no será tan concreta desde el principio como el en el caso del tipo y la peligrosidad, ya que dependerá de múltiples factores inherentes a las circunstancias y al suceso acaecido. Tampoco podrá ser calculada de forma inmediata ya que precisará de una investigación más minuciosa de todos los elementos afectados pudiendo estos ser no solo físicos o económicos, sino también morales, penales, reputacionales, etc.

Los equipos de respuesta ante incidentes se valdrán de la clasificación de los mismos para asignar una prioridad a cada problema, por lo que esta debe de ser precisa. La priorización de los inconvenientes producidos resultará en la elección del orden y los recursos destinados a la resolución de cada uno de ellos.

El ciberincidente se debería registrar y documentar en una herramienta de gestión de incidentes o, en su ausencia, de ticketing; incluyendo la información obtenida durante la fase de identificación, así como los valores de clasificación, peligrosidad e impacto inicial.

Sería recomendable valorar, llegados a este momento, la necesidad de informar este incidente de seguridad a un nivel superior en la estructura organizativa y dependiendo de dónde haya tenido lugar el ciberincidente (la jefatura del departamento de ciberseguridad de la entidad sanitaria, la dirección del centro de salud, la jefatura de informática de la gerencia de AP o AE, la dirección del servicio de salud, etc.) o al comité de crisis, en función de los procedimientos definidos por la entidad.

También sería preciso avisar a los responsables de las entidades interconectadas con la infraestructura afectada independientemente del nivel y naturaleza orgánica, ya que podría evitarse su propagación fuera de esta. Por ejemplo, si se ha descubierto una infección mediante un estándar de interoperabilidad sanitaria que está siendo usado con clínicas concertadas, estas deberían ser alertadas para activar su protocolo de actuación.

Además, en un ambiente tan multidisciplinar y con tantos servicios como el del sector sanitario, el incidente afectará a la continuidad de múltiples y muy diversas actividades a través sus respectivos servicios.

Los mejores conocedores de la criticidad y la actividad funcional de estos servicios clínicos serán los integrantes del equipo humano específicamente dedicado a ellos en su día a día. Cualquier trabajo sobre los servidores y demás sistemas implicados en cada servicio debería de ser coordinado, en la medida de lo posible, con el área implicada para poseer más información y producir el menor impacto posible al menos en los más esenciales, por ejemplo, los de la UCI, Urgencias, etc.

Pueden ayudar diagramas de red, correladores de eventos, sistemas de detección, etc. a comprender la magnitud del suceso.

Con el apremio del tiempo, se podrían definir estrategias de unificación de soluciones y de medidas de aislamiento que se apliquen bajo patrones tales como características comunes entre dispositivos médicos. Esto debería de hacerse solo en primera instancia y con el compromiso de ser revisadas una vez pasado el episodio de emergencia. Toma especial interés en los hospitales, ya que cuentan con miles de dispositivos de electromedicina sensibles en algunos de los casos.

A continuación, se citan algunas medidas de contención a nivel general que podrían ayudar a retener un incidente:

- Desconectar el sistema o el segmento de red afectado del resto de sistemas y redes de la infraestructura sanitaria.
- Cuando no sea posible desconectar el sistema o segmento afectado, o el servicio de este sea esencial e irremplazable, se puede proceder a filtrar el tráfico y permitir únicamente aquello que sea estrictamente necesario para la prestación del servicio mediante la colocación de un cortafuegos intermedio.
- Aislar el sistema comprometido en otra VLAN sellada.
- Implementar un agujero negro de DNS (DNS Sinkhole) para contener, interrumpir o impedir tráfico malicioso procedente de malwares, botnets, DDoS, etc.
- Bloquear vectores de ataque con determinadas direcciones sospechosas, remitentes u otros patrones comunes a los ya identificados.
- Aplicar reglas específicas en los firewalls perimetrales.
- Bloquear el acceso a unidades compartidas.
- Deshabilitar determinados servicios en ejecución.
- Solicitar soporte a los proveedores de servicio de Internet a fin de que puedan aplicar filtros o activar medidas de protección.
- Recurrir a entidades públicas o privadas especializadas en la materia, tal como un Equipo de Respuesta ante Emergencias Informáticas (CERT), que podría ofrecer información adicional y coordinación a nivel nacional e internacional con otros posibles implicados en el incidente.
- Eliminar cuentas de usuario y procesos sospechosos posiblemente provenientes del ataque.

De momento, la fase se ha centrado en contener el incidente respetando en la medida de lo posible la continuidad del servicio clínico y los datos a preservar. Es el momento de comenzar con la gestión de evidencias para poder analizarlo más sosegada y pormenorizadamente a posteriori o incluso aportar pruebas ante un organismo oficial de ciberseguridad o judicial.

El análisis de la memoria volátil es de gran utilidad en la investigación forense, especialmente cuando algunas pruebas pudieran perderse al apagar el sistema sanitario. Sería interesante realizar una adquisición de memoria volátil mediante herramientas especiales en la rama forense para evitar variar los datos y el estado del sistema y evitar alterar o perder evidencias.

Si los sistemas se encuentran sobre máquinas virtuales, se puede extraer el fichero correspondiente a la memoria RAM (*.sav si VirtualBox, *.vmem si VMware, etc.).

Para evitar que el software malicioso detecte que se intenta apagar el sistema, una vez que se ha realizado la adquisición de datos volátiles de la memoria, se podría apagar de manera súbita cortándole el suministro de electricidad. De esta forma, nos aseguramos de que el malware no ejecute ninguna acción contra el apagado, active alguna medida para intentar perpetuarse, ocasione daños en represalia o actuando a la desesperada, etc.

Se puede hacer uso de clonadoras físicas o herramientas software para hacer copias bit a bit de los datos no volátiles verificando que el medio original no sufrirá ninguna alteración empleando elementos que bloqueen la escritura en ellos (write-block) durante la ejecución del clonado.

El medio de almacenamiento de destino debería de tener un tamaño algo mayor al de origen para posibilitar procedimientos que necesiten de espacio adicional tal como el borrado seguro que garantizará que no traiga consigo información infectada.

El análisis forense en vivo es una alternativa a sopesar cuando por cualquier motivo no ha sido posible ejecutar una copia completa del sistema y su memoria.

Una vez copiados los datos, corresponde emplear métodos adicionales que certifiquen la integridad de los mismos. Por ejemplo, mediante la aplicación de funciones criptográficas o hash. Convenientemente funciones de tipo SHA2, sin despreciar MD5 y SHA1 cuando la primera no ha sido posible por la versión del sistema. Estas funciones aplicadas tanto en el origen como en el destino de los datos comprobarán que el valor obtenido en ambos casos es el mismo, correspondiéndose ambas informaciones de manera equivalente.

Antes de finalizar y continuar con la fase de mitigación, conviene realizar las acciones de análisis de los datos copiados con el fin de tratar de obtener la máxima información para proceder en ella de la forma más eficiente.

No obstante, y solo en el caso de que el sistema deba seguir prestando el servicio por ser esencial e irremplazable, se hace necesario aplicar medidas correctivas temporales hasta su reemplazo para poder aplicar las medidas de mitigación que logren neutralizar el incidente permanentemente.

8.4 Mitigación

Pese a parecer una solución razonablemente eficaz, el borrado de los medios de almacenamiento y posterior reinstalación del sistema afectado no siempre es la mejor opción para mitigar un ciberincidente. Esto puede ser desaconsejable en muchos casos. Entre ellos:

- No se cuenta con una copia de seguridad completa.
- La copia de seguridad no es reciente.
- No se dispone del instalador, la fuente o el proveedor de algún software necesario.
- No se cuenta con las licencias de programas necesarios.
- La vulnerabilidad atacada se encuentra en el software a ser reinstalado.
- Se precisa someter el equipo a la conexión de la red para instalar ciertos programas que podría provocar la reinfección o volver a sufrir un ataque.

No obstante, también hay casos en los que es la única opción viable. Como, por ejemplo, cuando la eliminación automática a través de herramientas no es posible, principalmente cuando se trata de algún tipo de rootkit o amenazas más avanzadas. En el mejor de los casos se podrá restaurar el sistema con una copia de seguridad anterior al ciberincidente o incluso a la aparición de la vulnerabilidad que lo incitó.

Cuando la única o mejor solución sea extraer manualmente la información del sistema porque, por

ejemplo, no existe una copia de seguridad, se debe de hacer con extrema cautela para no transferir también algún fichero infectado.

Es difícil encontrar una solución genérica para mitigar cualquier tipo de ciberincidente sanitario. Por ello, la solución dependerá intrínsecamente del tipo de ataque sufrido y aún más específicamente de la vulnerabilidad que lo propició, ya que deberá de ser corregida en última instancia.

Además del departamento interno de informática o electromedicina, o incluso de ciberseguridad cuando exista, hay empresas que pueden ofrecer un servicio externalizado de ciberseguridad integral. Aunque si lo que se desea es atajar el problema de forma específica, también hay empresas especializadas en ciberamenazas concretas, como el DDoS (denegación de servicio distribuidas), que pueden contratarse.

Asimismo, se puede contar con un CSIRT nacional, como INCIBE-CERT, que puede apoyar en el análisis y la definición de la estrategia de mitigación del problema.

Hay que recordar la necesidad de mantener siempre una fluida comunicación e información con los distintos proveedores tanto de software, hardware y equipos. Ya que estos productos que en el área sanitario suelen ser cerrados o restringidos comercialmente, pueden precisar de acciones adicionales del fabricante o el proveedor para ser desinfectados. Además, no hay que descartar que pudieran albergar la propia vulnerabilidad y pueda precisarse de un upgrade o parcheado oficial.

Por supuesto, las herramientas de seguridad tales como antivirus pueden eliminar ciertas infecciones si son conocidas por sus bases de datos y demás procedimientos de inteligencia artificial, heurísticos, etc.

En cualquier caso, será preciso aplicar las medidas de seguridad necesarias en la infraestructura: parches, updates, upgrades, firewall, antivirus, etc. para minimizar la posibilidad de reinfección una vez reconectado.

El incidente deberá ser comprendido como una evaluación y mejora continua. De él, siempre se deberá aprender y evolucionar. Por eso es necesario restudiar un análisis sobre el grado de exposición del activo, los servicios informáticos mal configurados o innecesarios y demás cuestiones que no solo pueden dar lugar a vulnerabilidades, sino que generan una infraestructura sanitaria cada vez más compleja y confusa, que entorpece en gran medida su control si no se delimita. A su vez, será un buen momento para cambiar las contraseñas de usuarios e interoperabilidad sanitaria entre sistemas, revisar las reglas de seguridad perimetral, etc.

La infraestructura sanitaria no debería de ponerse nuevamente en producción sin realizar antes una auditoría de seguridad para garantizar la correcta consecución de las fases anteriores. De la misma forma, hay que tener en cuenta que un parche, upgrade o update, también podría arrastrar un nuevo tipo de fallo o vulnerabilidad, con lo que nunca hay que confiar ciegamente en las medidas adoptadas.

Como punto final y respondiendo a una posible suspicacia del atacante, es conveniente revisar que las configuraciones no hayan sido modificadas. A veces se considera que se ha mitigado un ciberincidente cuando realmente no ha sido así ya que quizá el ciberatacante ha conseguido su propósito final alterando alguna configuración que pueda continuar proporcionándole beneficios cuando las aguas parezcan calmadas. Por ejemplo, creando un superusuario, abriendo una puerta trasera, cambiando un número de cuenta bancaria de ingresos por la suya, etc.

8.5 Recuperación

En esta fase, todos los servicios que proporcionaba la infraestructura sanitaria deben de volver a la normalidad recuperando la funcionalidad y operatividad necesaria para su carga ordinaria de trabajo que podría verse incrementada debido al corte del mismo.

Es un error pensar que una vez restablecido productivamente el sistema se puede dar por solventada la incidencia. Se hace necesario examinar en profundidad la infraestructura sanitaria no solo para impedir que pueda caer ante nuevas amenazas, sino para garantizar que no haya puertas traseras o software malicioso oculto que pueda reactivar el incidente que se creía resuelto. Especialmente una vez que se procede a la reconexión de todos los sistemas y dispositivos tanto entre ellos como a través de Internet.

Se debe atender a cualquier actividad sospechosa como si de la fase de identificación se tratara. Además, conviene atender a las instrucciones de fabricantes y proveedores de los sistemas sanitarios para restaurar y reinstalar los productos en las mejores garantías.

Será de gran ayuda la colaboración del personal funcional especializado (clínico, administrativo, etc.) para verificar y validar los sistemas desde el punto de vista práctico y operativo. Como normalmente este personal suele encuadrarse en un horario laboral de mañana y cuando coexiste una mayor carga de trabajo clínico, los tests automatizados que prueben y validen la funcionalidad de los sistemas para sus puestas a punto antes de la próxima jornada de trabajo serán de gran valor.

8.6 Post-incidente

Una vez que la puesta en producción de los sistemas de la infraestructura sanitaria ha sido exitosa y el ciberincidente está bajo control, dando como resultado el funcionamiento normal del servicio, es momento del aprendizaje y, de ser necesario, de la autocrítica.

Casi todas las organizaciones dan por culminado el proceso de gestión del incidente en la fase anterior. No obstante, esta fase es la más instructiva y comprometida fundamentalmente a nivel humano. Guarda una gran compatibilidad con eventos de tipo Agile tal como el Sprint Retrospective de Scrum si se deseara añadir a la metodología de trabajo.

Es un punto de encuentro. Un enclave donde no solamente debe de participar el equipo técnico, sino representativamente cualquier área afectada: personal clínico, administrativo, etc. Se podría incluso incorporar a externos y proveedores ligados intrínsecamente con la actividad de la entidad.

El objetivo es reflexionar sobre lo acontecido: cómo y por qué ha sucedido el incidente. Qué se ha hecho bien y qué puede mejorarse. Cómo podría prevenirse. Etcétera.

Será bienvenida cualquier información acerca del procedimiento llevado a cabo y los hitos de actuación de manera cronológica con el fin de analizar el ciberincidente con perspectiva general e imparcial.

Toda la información recabada, así como los puntos reseñables del debate dialéctico, servirán para la mejora de las personas, procedimientos y tecnologías que se enfrentarán a un posible futuro ciberincidente.

A su vez, este detalle podrá incorporarse a un informe general post-incidente que pueda servir a los altos cargos de la organización a tomar las decisiones ejecutivas pertinentes, entre ellas, la creación de un departamento de ciberseguridad cuando no exista en la entidad sanitaria afectada.

9. Ciberataques en estándares propios de la interoperabilidad sanitaria: HL7 y DICOM

Como ya se ha visto en anteriores apartados, uno de los mayores riesgos de la tecnología sanitaria es precisamente su universalidad. Cuando una vulnerabilidad es descubierta, con total seguridad se encuentra en dispositivos de múltiples hospitales a lo largo del mundo debido a la amplia comercialización y a los pocos fabricantes existentes en el sector. Esto permite no solo explotar la misma vulnerabilidad en múltiples organizaciones distintas, sino que los grupos cibercriminales puedan perpetrar sus ataques a nivel internacional, lo que dificulta aún más su persecución.

Pero existe algo todavía más universal que un determinado modelo de dispositivo y esta es precisamente su intencionalidad: un estándar.

Los estándares de interoperabilidad, en este caso entre sistemas de información del ámbito de la salud, definen el uso de características comunes tales como la estructura de datos, la codificación, las especificaciones técnicas y los protocolos que aseguran que la mensajería cumpla con su propósito y sea transmitida de forma compatible entre todos los sistemas que interactúan entre sí.

Los estándares sanitarios están presentes en casi todos los sistemas del sector a nivel internacional, por lo que una vulnerabilidad en ellos se convierte, de facto, en una vulnerabilidad en casi cualquier centro sanitario del mundo.

Dada la importancia y la repercusión de este hecho se abordarán las ciberamenazas existentes en dos de los principales estándares sanitarios utilizados hoy en día: HL7 y DICOM.

9.1. HL7

Fundada en 1987, Health Level Seven International (HL7) es una organización de desarrollo de estándares acreditada por ANSI sin fines de lucro dedicada a proporcionar un marco integral y estándares relacionados para el intercambio, la integración y la recuperación de información electrónica de salud que respalda la práctica clínica y la gestión, prestación y evaluación de los servicios de salud. HL7 cuenta con el respaldo de más de 1600 miembros de más de 50 países, incluidos más de 500 miembros corporativos que representan a proveedores de atención médica, partes interesadas gubernamentales, pagadores, compañías farmacéuticas, vendedores/proveedores y empresas de consultoría [50].

La comunicación HL7 es utilizada no solamente entre sistemas de un mismo centro sanitario, sino entre diferentes centros sanitarios de una misma organización, entre los centros de una organización y los de otra (por ejemplo, un hospital público y una clínica privada concertada). A su vez, se usa entre diferentes sistemas a nivel internacional (por ejemplo, a lo largo de Europa en el contexto de la eHDSI (eHealth Digital Service Infrastructure)).

En la mayoría de los casos, el mensaje HL7 contendrá los datos personales del paciente (nombre, apellidos, documentos de identificación, dirección, teléfono, etc.) y los datos de su salud (citas médicas, ingresos hospitalarios, resultados de analíticas, informes médicos, etc.).

A continuación, se detallarán algunas vulnerabilidades de HL7 y los ciberataques a los que pueden dar lugar en caso de no protegerse adecuadamente mediante las medidas precisadas posteriormente [52].

Vulnerabilidades:

1. HL7 asume que el **cifrado** se ha dado bajo la capa donde opera, la de aplicación (por ejemplo, mediante TLS/SSL o IPSec), y no la requiere. Este descuido por parte de HL7 International hace que la mayoría de las veces el mensaje se transmita en texto claro pese a la sensibilidad de los datos que transmite.

2. El estándar tampoco se preocupa de la **autenticación**, de forma que cualquier sistema podría comunicarse con un puerto de recepción HL7.

3. Las interfaces de **comunicación** HL7 funcionan bajo la relación de muchos a uno (N:1). De esta forma, varios clientes carentes de autenticación pueden comunicarse a un mismo puerto abierto puesto a disposición para este propósito.

4. La responsabilidad de **verificación** del mensaje recibido depende de la implementación del sistema de destino. De hecho, la validación de si se recibió desde el sistema adecuado, o si son datos válidos; a menudo no es implementado. Y es que el sistema destino no cuenta apenas con posibilidad de contraste de información o de saber si no le llegó un mensaje que sí le tuvo que llegar. Con lo cual, bajo una equivocación de diagnóstico, podría no recibir la corrección de esta y, además, desconocer su existencia, con lo que no solicitaría su reenvío para poder procesarla y registrarla adecuadamente. Un fallo de verificación de datos podría dar como resultado, por ejemplo, el poder asignarle un diagnóstico negativo de cáncer a un paciente que sí lo padece.

Ciberataques:

- Las vulnerabilidades 2 y 3 son escenario perfecto para perpetrar un ataque **Denial of Service (DoS)**.

  La conexión HL7 estándar es a demanda. Un sistema origen se comunica a otro destino mediante el puerto abierto para la comunicación. Una vez que el sistema de origen ha terminado el envío de mensajes se desconectará y el sistema de destino tendrá disponible ese canal para nuevas conexiones de otros sistemas. El sistema de destino tendrá un máximo de conexiones de escucha.

  Debido a que HL7 carece de autenticación, cualquier sistema puede conectarse al puerto abierto de escucha. Incluso un simple Telnet.

  A esto se le suma que, por defecto, en los motores de integración el tiempo de espera de recepción suele estar desactivado, y en cambio, la opción de mantener las conexiones abiertas suele estar activada, por lo que lo estará hasta que el sistema origen decida cerrarla.

  De esta forma, lanzando tantos Telnet como número máximo de conexiones tenga establecido el sistema de destino, se ocuparán todos los canales y se impedirá que ningún otro sistema legítimo pueda comunicarse con él, provocando una denegación de servicio.

  Con este procedimiento, un ciberatacante podría bloquear un sistema médico vital para los pacientes de un hospital.

- Las vulnerabilidades 2 y 4 podrían propiciar un ataque de **envío de información falsa**.

  La configuración de interfaz estándar de HL7 permite que un sistema ficticio pueda conectarse como sistema origen sin autenticación y enviar mensajes con datos falsos debido a la baja capacidad de verificación del sistema destino. Este hecho podría poner en riesgo la

operatividad del centro sanitario (por ejemplo, enviando mensajes de cancelación de todas las citas) o la vida de los pacientes (por ejemplo, enviando mensajes de modificación que anulen todas las alergias a medicamentos de los pacientes ingresados).

Mientras que el mensaje falso sea sintácticamente correcto, el sistema destino lo procesará, registrará y enviará un acuse de recibo (HL7 ACK) correcto.

- Las vulnerabilidades 1, 2 y 4 son el caldo de cultivo ideal para un ataque **Man-in-the-Middle (MITM)** con **envenenamiento ARP.**

  Mediante diversas herramientas de ARP Spoofing (Arpspoof, Arpoison, Cain & Abel, Ettercap, etc.), el atacante suplantará la identidad en la red de la infraestructura sanitaria de uno de los sistemas HL7 que están manteniendo una comunicación. Esto lo realizará enviando respuestas ARP falsas con la IP de un sistema HL7 legítimo, de manera que los demás sistemas reconozcan la dirección MAC del atacante como la de dicho sistema y pasen a comunicarse con él.

  Una vez dentro de la comunicación, se podrá leer en texto claro la información sensible transmitida entre los sistemas e incluso modificarla intermediariamente para que el sistema destino reciba la variación en vez del mensaje original.

  De esta forma, por ejemplo, se podrán falsificar signos vitales o parámetros corporales como el peso que podrá influir en la cantidad de medicamento que se administrará a un paciente, pudiéndole provocar una sobredosis.

- La vulnerabilidad 4 permite la **inyección de código SQL**.

  La mayoría de los datos recibidos en mensajería HL7 son almacenados en BBDD. Un atacante podría introducir una inyección de código SQL de tal forma que cuando se guarde en la base de datos se deseche el resto del texto a excepción de la instrucción, que será interpretada y procesada por el sistema de base de datos y la ejecutará.

  De esta forma, un atacante podría, por ejemplo, introducir en un campo de un formulario de una aplicación una inyección SQL con una sentencia de borrado (delete) que al ser interpretada en la BBDD eliminara todas las alergias a medicamentos de los pacientes, pudiéndoles ocasionar una anafilaxia.

Medidas para segurizar HL7:

- La **validación** de la mensajería y el **recuento** de mensajes enviados versus mensajes recibidos mediante sus identificadores para asegurarse de que no se hayan recibido mensajes adicionales.
- Un **cortafuegos basado en host** podría evitar que los sistemas no autorizados se comuniquen con las interfaces HL7 y envíen mensajes o ataques DoS desde sistemas aleatorios.
- La **segmentación de la red** puede limitar la visibilidad de las interfaces HL7 (y el motor de interfaz), lo que resultaría ventajoso en la transmisión de datos sensibles.
- Las **medidas contra la falsificación de ARP** como las entradas ARP estáticas evitan con éxito los ataques de suplantación de ARP.
- Las **redes privadas virtuales** (VPN) también se deben usar en comunicaciones internas para proporcionar cifrado en ellas.
- Con la **tunelización SSH** se puede lograr que los datos sin cifrar nunca sean visibles desde fuera de los dos sistemas finales de la comunicación HL7.
- El uso de declaraciones prediseñadas, consultas parametrizadas, validaciones de entradas

de usuarios o procedimientos almacenados que verifiquen los datos introducidos en los sistemas de información son **medidas efectivas contra los ataques SQL**.

9.2. DICOM

DICOM ® (Digital Imaging and Communication In Medicine) es el estándar internacional para imágenes médicas e información relacionada. Define los formatos de imágenes médicas que se pueden intercambiar con los datos y la calidad necesarios para su uso clínico.

DICOM ® se implementa en casi todos los dispositivos de radiología, imágenes de cardiología y radioterapia (rayos X, tomografía computarizada, resonancia magnética, ultrasonido, etc.), y cada vez más en dispositivos de otros dominios médicos como la oftalmología y la odontología. Con cientos de miles de dispositivos de imágenes médicas en uso, DICOM ® es uno de los estándares de mensajería de atención médica más implementados en el mundo. Hay literalmente miles de millones de imágenes DICOM ® actualmente en uso para la atención clínica.

DICOM ® está reconocido por la Organización Internacional de Normalización como el estándar ISO 12052 [51].

Vulnerabilidad:

El estándar de formato de archivo DICOM define un encabezado que consiste en una sección de 128 bytes al principio del archivo, llamada preámbulo, que se puede usar para facilitar el acceso a las imágenes y metadatos dentro de la imagen DICOM.

Si bien el estándar DICOM pretende que el campo se use para permitir la compatibilidad con visores de imágenes que no son DICOM, el estándar no impone ningún requisito estructural sobre los datos insertados en el preámbulo.

El 02/05/2019 se publicó bajo el CVE-2019-11687 [53] una vulnerabilidad relacionada con el preámbulo. Tiene un puntaje CVSS de 9.3 y un impacto completo en la confidencialidad, integridad y disponibilidad de la información y los sistemas afectados. Su complejidad de acceso es media, aunque no se requiere autenticación. Este tipo de vulnerabilidad permite la ejecución de código malicioso.

El problema se detectó en el formato de archivo DICOM Part 10 dentro del estándar NEMA DICOM versión 1995 hasta 2019b. El espacio del preámbulo de un archivo DICOM que cumple con esta especificación puede contener el encabezado de un archivo ejecutable.

Antes de nada, conviene saber que Portable Executable (PE) es una estructura de datos que encapsula la información necesaria para que el cargador del sistema operativo Windows administre el código ejecutable empaquetado. Si el PE/DICOM se ejecuta con un lector DICOM, se interpreta como un DICOM. Pero si se ejecuta desde la COMMAND.COM de Windows, se ejecutará como PE, incluso si su extensión es .dcm.

Las configuraciones antimalware en las instalaciones sanitarias a menudo ignoran las imágenes médicas DICOM. Se piensa erróneamente que no pueden ser o contener ejecutables. Además, el número de pruebas almacenadas es cuantioso y en algunos casos son gigantescas, como en el de las resonancias magnéticas, PET-TAC, etc., cuyo análisis continuo podría repercutir negativamente en el rendimiento de los sistemas.

Del mismo modo, las herramientas antimalware podrían infringir acuerdos regulatorios y comerciales al procesar archivos DICOM debido a su carácter clínico.

Esto permite que un atacante pueda **enmascarar un archivo ejecutable (por ejemplo, un malware Portable Executable (PE)) como una imagen DICOM** (por ejemplo, una radiografía), aprovechando su intención inicial, que es poder enmascarar imágenes de pruebas médicas no DICOM (tal como una dermatoscopia en JPEG) como un archivo DICOM.

Ciberataques:

La vulnerabilidad descrita permite la **infección por malware** embebido en un fichero DICOM que debería de contener una imagen médica.

El atacante crea un archivo PE/DICOM utilizando un archivo DICOM prexistente y el malware elegido para el ataque. Como el archivo puede tener la extensión .dcm en vez de .exe, el malware quedará camuflado en un archivo DICOM como los que están familiarizados a emplear en las estaciones de trabajo de radiología o medicina nuclear.

A continuación, le hace llegar el estudio radiológico ficticio a su especialista médico en el hospital en un pendrive, indicando que necesita que valore una prueba que se realizó en otra clínica privada. Para asegurar la infección, el atacante podría agregar un visor open source modificado que garantice la correcta ejecución del PE.

Cuando el archivo es abierto, el malware se ejecutará, buscando llegar a través de la red al PACS (almacenamiento de imágenes DICOM) donde pueda infectar a cientos de miles de imágenes médicas sin ser percibido. De esta forma, al ser abiertas desde diferentes sistemas, perpetrará su objetivo a lo largo y ancho de la infraestructura sanitaria.
Dependiendo del tipo de malware, podría provocar los siguientes ciberincidentes:

- Replicarse y moverse a través de la red de la infraestructura sanitaria, como en el caso del **gusano**.
- Alterar el funcionamiento de los dispositivos médicos perjudicando la salud de los pacientes, como en el caso del **virus**.
- Controlar remotamente los sistemas médicos, como en el caso del **troyano**.
- Espiar la actividad médica y robar datos de historias clínicas, como en el caso del **spyware**.
- Bloquear con publicidades o realizar compras no autorizadas desde los ordenadores del personal clínico, como en el caso del **adware**.
- Cifrar los datos de servidores esenciales de la infraestructura de un hospital para exigir rescates económicos, como en el caso del **ransomware**.

Pero esta no es la única vulnerabilidad que se ha descrito sobre el estándar DICOM. Existen otros estudios, como el realizado en base a CT-GAN [54] acerca de cómo un atacante puede usar el aprendizaje profundo (deep learning) para agregar o eliminar evidencias médicas de escáneres volumétricos en 3D. Esta investigación logró interceptar comunicaciones DICOM entre sistemas (por ejemplo, una máquina de resonancia magnética o de TAC y el PACS) y modificar las imágenes, generando o eliminando evidencias patológicas mediante machine learning. Más concretamente, en la evaluación del ataque se enfocaron en crear y suprimir evidencias de un cáncer de pulmón en unas tomografías computarizadas.

Esta vulnerabilidad podría suponer amenazas tales como sabotaje a investigaciones médicas, fraudes a seguros médicos y de vida, atentados contra la vida de las personas, etc.

Se podrá indagar más en la teoría y práctica de este estudio mediante el vídeo [55] y el repositorio de código fuente [56] anexados en la bibliografía de este trabajo.

Medidas para segurizar DICOM:

- Sobreescritura del preámbulo de los ficheros DICOM.
- Actualizaciones y parches de seguridad contra el uso de exploits.
- Políticas de contraseñas seguras.
- Ajuste de las funciones de los usuarios según sus roles.
- Monitorización y registro de actividades sospechosas.
- Uso de firewall y antimalware para aplicar reglas de detección estática y heurística.
- Uso de SIEM (Security Information and Event Management).
- Uso de analizadores de comportamientos anómalos.
- Segmentación de la red.
- Uso de servidores Unix resistentes a los ataques mediante PE.
- Técnicas CDR/CDNR (Content Disarm and Reconstruction/Content Deconstruction Neutralization and Reconstruction).

10. Riesgos y amenazas del futuro de la tecnología sanitaria

No solo la sanidad privada está apostando fuertemente en la tecnologización del sector, sino que también se están destinando grandes partidas presupuestarias por parte de la pública. Prueba de ello es la reciente aprobación del Plan INVEAT (Inversión en Equipos de Alta Tecnología del Ministerio de Sanidad del Gobierno de España) con una dotación de 796.100.000 € entre 2021 y 2022 [57].

Si bien no se puede predecir con exactitud cuál será el futuro de la tecnología sanitaria a largo plazo, sí se conocen las incorporaciones de varias disciplinas tecnológicas con un gran potencial en el avance del sector y que marcarán la tendencia de su progreso de forma inminente. Algunas de ellas, así como los riesgos y amenazas que podrían acarrear son:

Telemedicina:

La telemedicina ha proporcionado dos ventajas clave para el sector en la lucha contra el COVID en los últimos años. Por un lado, permitía mantener una relación y comunicación segura entre el personal sanitario y el paciente al no existir posibilidad de contagio. Por otro, permitía una reducción de costos y un mejor aprovechamiento del cada vez más limitado personal clínico gracias al carácter online de las consultas.

La telemedicina va teniendo mejor acogida no solo entre las aseguradoras médicas y sus pacientes por la comodidad y rapidez que suministra, sino también por algunas consejerías de sanidad públicas que están sufriendo una cada vez mayor falta de personal médico.

La telemedicina utiliza en muchas ocasiones los equipos personales al menos del paciente (smartphone, PC o tablet) y la red de su hogar o incluso una red pública, por lo que no cuenta en la mayoría de los casos con las suficientes medidas de seguridad.

Otros factores que podrían afectar a la confidencialidad de los datos son el ambiente en el que se dé la consulta, que en determinadas ocasiones puede ser ante otras personas, incluso desconocidas; o la reducida capacidad de identificar al paciente.

IoMT:

El Internet of Medical Things lo componen dispositivos médicos conectados al *Internet de las Cosas* y cumplen misiones tales como la de monitorizar de forma constante los datos del paciente: signos vitales, pasos, glucosa, etc.

Existen ya en proyectos tales como marcapasos, bombas de insulina o algunos más novedosos como los inhaladores inteligentes o las pastillas sensorizadas. No obstante, las funcionalidades que pueden realizar dentro del mundo de la salud, y con ello, las ventajas que pueden llegar a proporcionar tanto al sector como al paciente son innumerables.

Los dispositivos IoMT pueden presentar vulnerabilidades en materia de ciberseguridad, por ejemplo, en el método de autenticación, que propicie ataques medjacking comprometiendo incluso la salud del propio paciente. Del mismo modo, pueden sufrir ataques de denegación del servicio o de interceptación de sus comunicaciones como el MITM, afectando a su operatividad y confidencialidad respectivamente, sobre todo cuando los datos no están correctamente cifrados.

Big data:

La recolección de datos médicos y su análisis es parte esencial de los modelos predictivos. Estos modelos aportan beneficios a diferentes ámbitos, ya que podrían:

- Predecir el número de ingresos hospitalarios en un día determinado.
- Pronosticar gastos sanitarios.
- Conocer la dosis exacta de un medicamento de gran coste que se debe administrar a un determinado paciente.
- Diagnosticar tempranamente enfermedades a pacientes según su perfil.
- Controlar epidemias.

El big data gestiona varias y diversas BBDD en la mayoría de los casos de diferentes entidades que deben garantizar el contar, en su conjunto, con las medidas óptimas de seguridad que garanticen la disponibilidad, confidencialidad e integridad de los datos. En caso contrario, pueden ser susceptibles a ataques de inyección de código, gestión inadecuada de permisos, vulnerabilidades de DBMS, etc.

Si la custodia de la integridad de los datos no es la correcta, podría hacer fracasar el trabajo de varios años de investigación médica.

IA:

La Inteligencia Artificial no solo ayuda a procesar los datos recolectados por el Big Data a fin de crear los modelos predictivos vistos en el apartado anterior. Es una disciplina imprescindible en la agilización de tiempos de investigación para el desarrollo de nuevas vacunas, como lo demostró con la del COVID-19.

Además, ayuda al personal médico en el hallazgo de enfermedades analizando pruebas médicas DICOM o auxilia a la disciplina robótica a la hora de memorizar los patrones de movimiento de pacientes provistos de prótesis inteligentes.

Aunque disciplinas tales como el Big Data y la IA son más conocidas como buenas aliadas de la ciberseguridad que por las vulnerabilidades en sus propios dispositivos, estas también cuentan con ellas. Normalmente, la mayor ciberamenaza para la IA es otra IA. Como se ha visto con anterioridad en el análisis del estándar DICOM, las imágenes pueden ser sometidas a creaciones de tumores maliciosos mediante IA para engañar a otro sistema de IA encargado de diagnosticarlos.

Esto se consigue mediante el uso de la ingeniería inversa. El sistema IA atacante se nutre del conocimiento de cómo funciona un sistema IA sanitario para confundirlo mediante técnicas inversas.

Uno de los casos más sonados de ataque a la IA fue el de Tay, un bot de charla dotado de inteligencia artificial lanzado por Microsoft a través de Twitter en el 2016 y que, tras enviar mensajes ofensivos a los usuarios, fue dado de baja a las 16 horas de su lanzamiento.

Realidad virtual:

Esta disciplina provee de escenarios ficticios pero dotados de un gran realismo a estudiantes, profesionales e investigadores médicos. Permite, por ejemplo, el entrenamiento de forma masiva en casos prácticos de cirugía, sin necesidad de contar con quirófanos o cuerpos humanos para aplicar las técnicas en las que se les están formando. Con ello, se consigue un abaratamiento de costes, una perfección continua de la técnica y una fuente inagotable de recursos necesarios para la simulación de los escenarios.

Algunos organismos sanitarios ya están estudiando qué papel podría tener Metaverso en sus actividades y cómo podría ayudarles.

La realidad virtual ofrece un entorno práctico que aísla los riesgos de la realidad física. No obstante, al estar provista de múltiples dispositivos para su implementación, las vulnerabilidades aumentan, y con ello, la posibilidad de ciberamenazas. Estas ciberamenazas podrían traducirse en el envío de datos falsos en la formación de cientos de profesionales que podrían terminar efectuando mal la minuciosa operación para la que fueron formados y que creían verse desenvueltos en un quirófano real.

Chips implantables:

Según Elon Musk, propietario de la empresa Neuralink, que fabrica chips implantables en el cerebro, en 2023 podría realizar su primera prueba con humanos tras haber terminado los trámites con la FDA (Food and Drug Administration), organismo encargado también del uso de implantes y procedimientos quirúrgicos para el público en EE. UU.

La implantación de chips en el cuerpo humano podría suponer beneficios en la detección temprana de enfermedades o en el tratamiento de algunas discapacidades tales como la ceguera.

La conexión inalámbrica de la que están provistos estos chips aumenta significativamente la posibilidad de acceso no autorizado a ellos y, de esta forma, su ataque. Un atacante podría aprovechar un fallo en la autenticación para acceder al dispositivo y modificar su comportamiento. A su vez, propicia la interceptación de sus datos, especialmente si carecen de un mecanismo de cifrado óptimo.

Robótica:

La robótica ha brindado la posibilidad de realización de diversas tareas dentro del sector de la salud de manera automatizada y precisa. Uno de los campos que más se ha nutrido de sus beneficios ha sido la cirugía, aportándole poder realizar operaciones a distancia y con mayor precisión que minimizan los errores humanos. Otro de los campos es la rehabilitación en procesos de rehabilitación motora, prótesis y exoesqueletos inteligentes y en la recuperación de los sentidos como en el caso del ojo biónico.

Los robots se encuentran presentes en otras actividades tales como la logística, gestionando el almacenamiento y la distribución de medicamentos en hospitales y farmacias; o la clínica, prestando su servicio como auxiliares médicos en zonas altamente contaminadas por virus.

Los robots, al igual que los humanos, son vulnerables a los virus, en este caso, informáticos. Un virus podría hacer que el robot tuviera un comportamiento inesperado. Los robots, de hecho, podrían ser vulnerables a todo tipo de malware.

Conjuntamente, pueden ser sometidos a ataques DoS, bloqueando su operatividad. Por otro lado, y dado que están provistos de conexión inalámbrica en la mayoría de los casos, son susceptibles a accesos no autorizados con el fin de controlarlos.

Finalmente, al estar provistos de IA, pueden aplicárseles ataques de ingeniería inversa desde otros sistemas inteligentes con el fin de distorsionar su comprensión o decisión.

Cloud:

Son diversos los factores que propician la utilización de la nube dentro del ámbito sanitario. El uso cada vez mayor de las tecnologías de la información, la escasez de personal, la centralización, el trabajo a distancia, el crecimiento del ecosistema de aplicaciones, entre otros.

Algunos casos de éxito actuales de la nube en el sector son la infraestructura de salud pública, las aseguradoras, la telemedicina, el uso secundario de datos clínicos, el almacenamiento y visualización de imágenes médicas, etc.

Las amenazas y los riesgos que pueden afectar al sistema sanitario en la nube son varios dada la fusión de tecnologías que intervienen. Entre ellos, destaca la violación de los datos que alberga, la configuración incorrecta dada su complejidad y gestión compartida, los fallos en la autenticación, el secuestro de cuentas, el abuso y uso indebido de servicios en la nube, las interfaces y API inseguras, etc.

Estas cuestiones podrían suponer, por ejemplo, el robo de información relativa a pruebas médicas e historias clínicas de pacientes y la extorsión a las organizaciones sanitarias responsables de los datos.

11. Conclusión

Desde los primeros usos de las materias primas por parte de los homos, los instrumentos siempre han estado presentes a la hora mejorar su salud y bienestar. Los avances tecnológicos dentro del área sanitaria han sido innumerables y cada vez más apresurados.

La cuestión que propició este trabajo de fin de máster fue si la veloz tecnologización del sector sanitario se estaba realizando de una manera garante, es decir, de la mano de las medidas técnicas de seguridad adecuadas que protegiesen cada avance.

Tal y como se ha podido comprobar en el apartado de revisión del arte, en España los servicios necesarios para el mantenimiento de la salud de la población son definidos como esenciales para la nación. Estos servicios esenciales contarían con altas medidas de protección al encuadrarse como infraestructuras críticas y una regulación especial en cuanto a la seguridad de sus redes y sistemas de información.

No obstante, la declaración de infraestructura crítica corresponde al Ministerio del Interior y el Catálogo Nacional de Infraestructuras Estratégicas no es público. Este catálogo recoge un total de 12 sectores y 600 infraestructuras, entre las que se estima que no fue hasta la pandemia del 2020 del COVID-19 bajo el virus SARS-CoV-2 que se tomó la decisión de incluir a los más relevantes hospitales. De haberse tomado antes la decisión, la respuesta y resiliencia ante el incidente pandémico en los centros hospitalarios habría sido notablemente superior.

Por otro lado, y como especifica el ENISA Report del 2021, es necesario un CSIRT central y concreto del sector de la sanidad a nivel nacional a causa de su especificidad, dimensión y criticidad. Pero más aún en España debido a su fundamental pertenencia al sector público, autonomía a nivel regional y dispersión.

En materia de ciberseguridad en el sector de la salud existe poca documentación rigurosa y de fuentes neutrales u oficiales, muestra de la poca especialización y concienciación a la que se está viendo sometida pese a su crecimiento exponencial digital.

El estudio del marco legal concluye que pese a existir una amplia gama de normas que intervienen en garantizar la seguridad de las instalaciones de salud en España, apoyadas por la Unión Europea; se echa en falta regulaciones específicas, como específico y autónomo es el sector de la sanidad en el país. Regulaciones que lideren y centralicen las políticas regionales que cada consejería y servicio de salud adoptan de manera unilateral, ya que de ello depende la garantía y protección del sistema nacional de salud.

El sector es visto por los ciberatacantes como una víctima que cuenta con cuatro debilidades principales: sus centros comparten vulnerabilidades a nivel global, almacena datos sensibles y de gran valor, gestiona mucho dinero y es altamente extorsionable debido a su criticidad.

De esta forma, la principal ciberamenaza que acecha al sector, el ransomware, consigue su objetivo económico al cifrar e incluso amenazar con publicar datos personales y clínicos o bloquear servicios indispensables para la continuidad del servicio de los hospitales.

A lo largo del TFM se han nombrado diversas medidas para reducir los riesgos desde un punto de vista técnico, con algunas menciones a medidas procedimentales y organizativas. Sin embargo, las herramientas técnicas ya existen y donde realmente hay que llegar es a las personas, profesionales y pacientes, que componen las organizaciones sanitarias. De ahí, que el resto de las conclusiones del proyecto adquieran un tono más social.

Este proyecto propone una mayor difusión de los ciberincidentes al menos entre las entidades sanitarias a nivel internacional. La compartición de la información recabada en los procedimientos de gestión de incidentes llevados a cabo será de gran ayuda para la gestión de los mismos incidentes en otras organizaciones. Por lo tanto, la difusión se hace vital y más en la era de las tecnologías de la información. Es por ello, que dejando a un lado los temores reputacionales, la competitividad y la opacidad comercial; conviene una mayor coordinación entre todas las entidades no solo nacionales, sino internacionales. Tanto del ámbito público, como del privado. Estas amenazas perjudican a todos por igual y el bien común es también el bien propio.

Se sugiere, por lo tanto, la creación de una asociación internacional de todas las entidades en materia de ciberseguridad sanitaria (que el proyecto denominará, de forma ficticia, *IHESEC*) el cual debe proveer de un canal de comunicación e información entre estas organizaciones sanitarias a escala mundial. Su fin debe de ser la publicación de riesgos, vulnerabilidades, amenazas y medidas de seguridad. Pero, también, el de reclamar el papel fundamental de la seguridad TIC en el área sanitaria, así como de exigir la adecuación de las normas, estándares y proveedores, entre otros, a la calidad exigida para garantizar dicha seguridad en todas las infraestructuras sanitarias.

Por otro lado, hay que romper clichés. El personal tecnológico también tiene un papel vital en las infraestructuras sanitarias y debe de tener la misma consideración y valoración que el personal médico. Su motivación es esencial tanto en el día a día como ante ciberincidentes. Por ello, es imprescindible invertir también en su contratación, estabilidad, mejoras salariales, formación y concienciación en materia de ciberseguridad.

Es normal pensar, y más en un sector con tanta competencia y que mueve tanto dinero, que la

vanguardia e inversión debe de estar en la sofisticación de aparatos médicos. Sin embargo, cualquier activo valioso debe de estar bien custodiado y salvaguardado. Por lo que también hay que invertir en la renovación, licenciamiento, actualización y parcheado de estos sistemas sanitarios.

En la infraestructura sanitaria actual, los técnicos y la tecnología también curan y salvan vidas. Sería imposible concebir la medicina moderna sin la tecnología.

Reincidiendo en el tema de los sistemas sanitarios, el *IHESEC* debe mediar con los gobiernos en la adecuación de aquellas regulaciones que impidan acceder para desarrollar con eficacia las tareas de seguridad en los sistemas médicos incorporados a la infraestructura sanitaria.

Asimismo, el *IHESEC* debe concienciar a sus miembros en la evitación de la compra de sistemas que incorporen licencias y/o contratos comerciales que impidan acceder a los mismos con fines de ciberseguridad desde la misma redacción del contrato privado o pliego público que la suscite.

En estos contratos y pliegos de suministro de sistemas sanitarios por parte de proveedores, es vital establecer aquellas cláusulas que permitan un control eficaz de las medidas de seguridad por parte de la entidad sanitaria, así como las penalizaciones pertinentes en caso de incumplimiento.

Una de las medidas de seguridad exigibles del párrafo anterior debe de ser el poder someter a los sistemas a una auditoría de seguridad por parte de la propia entidad sanitaria antes del compromiso de adquisición.

Igualmente, sería valorable para las entidades sanitarias la contratación de empresas externas de pentesting y realizar los análisis de manera continua, pero alternando la empresa.

Es eficiente que la propia entidad realice sus propias auditorías de seguridad, pero es óptimo que lo hagan sus órganos superiores, públicos e independientes de esta. De esta forma, el servicio de la salud debe de ser competente en la realización de auditorías de seguridad en las gerencias hospitalarias, así como la consejería o incluso el Ministerio de Sanidad debe de ser competente en la auditoría de seguridad del servicio de la salud (por ejemplo, en la auditoría de accesos a su Sistemas de Información de Historia Clínica (SIHC)).

Estas auditorías no deben recaer sobre empresas privadas, aunque sí pueden formar parte de ellas, recayendo la autoridad y responsabilidad final en el organismo oficial que la ejecute.

En relación a los accesos indebidos a las HHCC, la Agencia Española de Protección de Datos debe de permitir que cualquier paciente, como titular de sus propios datos clínicos, pueda requerir la identificación de todo el personal que haya accedido a su historia clínica sin más argumentación. Debería de ser una petición automatizada y sin coste para el paciente, ya que podría esclarecer delitos de los que es garante la propia AEPD.

Las administraciones públicas dedicadas a la sanidad deberían minimizar la contratación de personal externo para cubrir puestos que puedan afectar directamente a la integridad, confidencialidad o disponibilidad de los datos personales y de la salud de los pacientes. De la misma forma, para estas funciones deberían utilizar personal funcionariado, pues es más estable contractualmente, está mejor implicado con la institución, está mejor y más íntimamente identificado por la entidad y recaen sobre él sanciones únicamente aplicables a los funcionarios públicos. La sanción disciplinaria de separación del servicio de manera firme debe de ser de aplicabilidad en estos tipos de infracciones.

Respecto a este personal que entre sus funciones tiene la gestión de datos sensibles, se debe minimizar que estas actividades se desarrollen físicamente fuera de la organización, por ejemplo, mediante teletrabajo. De la misma forma, se debe impedir o al menos registrar la extracción de los datos fuera de la organización: a través de pendrives, correos electrónicos, clientes VPN, etc.

La inversión en la seguridad de la infraestructura sanitaria no es solo virtual. Se hace vital también la inversión en seguridad física: videovigilancia, control de accesos, vigilantes de seguridad, etc.

La infraestructura de sanidad debe de contar siempre con réplica de sistemas sanitarios exigibles mediante el pliego o el contrato al proveedor. La misión de estas réplicas no es solo de interés cuando hay que realizar un trabajo sobre el sistema primitivo sin perjudicar a la continuidad de su servicio esencial, como puede ser durante su desinfección, actualización o parcheado. También lo es para tareas de preproducción o pruebas sin afectar a su servicio. No se deben utilizar los sistemas productivos para este cometido.

Ya se ha incidido en que es necesaria la creación de un CSIRT o un órgano oficial en materia de ciberseguridad del sector sanitario público y privado a nivel nacional. Pero también es vital la creación de un departamento de ciberseguridad específico en cada entidad sanitaria, también pública o privada.

El departamento de ciberseguridad con el que debe de contar cada entidad sanitaria debería de mantener una comunicación fluida y ágil con los usuarios: personal y pacientes.

Al personal interno y externo le debería de ser exigible el entrenamiento, participación en simulacros y formación en materia de ciberseguridad, cuya rigurosa evaluación debería de ser penalizable en caso de no ser realizada o superada.

La digitalización de las organizaciones públicas y privadas de la salud involucran al paciente y facilitan sus trámites mediante la creación de aplicaciones usualmente móviles. Sería idóneo requerir que los dispositivos informáticos de los pacientes reúnan ciertas características de seguridad antes de conectarse a los aplicativos y datos de la infraestructura sanitaria. Por supuesto, dichos aplicativos deberían estar lo suficientemente aislados de la red de la infraestructura sanitaria, así como deben garantizar no mostrar en ningún caso los datos de otro paciente, ni los mínimos requeridos de los profesionales asistenciales del paciente autenticado. Las medidas técnicas de autenticación y cifrado de la información en estas aplicaciones deben de ser robustas.

Del mismo modo, debe de ser requerido estar plataformados y/o bastionados por la organización todos los equipos profesionales que sean conectados a la red de la infraestructura sanitaria. Sean internos o externos. Así como impedir la conexión de dispositivos personales: tales como portátiles o móviles. De hecho, no debería de existir Wi-Fi abierta a pacientes ni proveedores sin estar plenamente aislada. A su vez, todos los puertos de transferencia de datos o de conexión a la red o a los sistemas sanitarios no custodiados e inutilizados deben de estar capados. También deberían de ser inaccesibles los cables de red que puedan ser crimpados para fijar clavijas LAN como la RJ. Y, por supuesto, gestionar adecuadamente el alta e identificación de los dispositivos conectados a la red previamente a su consentimiento de transmisión de datos.

La ingeniería biomédica debe desarrollarse también en el ámbito de la seguridad ofreciendo, en cada avance que proporcione, las medidas técnicas, procedimentales y organizativas que permitan beneficiarse de él bajo las mejores garantías. Hay que ser cautos con los nuevos avances y calibrar siempre las ventajas *versus* los riesgos.

Parece lo más sensato, cómodo y económico contratar al mismo proveedor de un sistema (por ejemplo, un HIS) para su soporte en producción. No obstante, los privilegios y accesos de los que goza un técnico de soporte con datos productivos no deben recaer en un empleado externo. Todas las actividades, especialmente si gestionan datos reales y sensibles, deben de recaer sobre personal interno. Aunque haya contratos de confidencialidad de por medio.

Este proyecto ha realzado en varias ocasiones el papel fundamental del personal técnico en el ámbito

sanitario. Pero, del mismo modo, hace hincapié en que es vital para este personal contar con el apoyo del personal funcional clínico. El aprendizaje y la colaboración debe de ser mutua en todo momento. De forma paralela, el personal técnico debe de tener formación e inquietudes funcionales y conocer aspectos como qué prioridad y funciones tiene cada sistema y servicio de la infraestructura sanitaria.

La competitividad y los presupuestos de la organización no siempre permiten contar con el mismo proveedor y sistemas en las renovaciones contractuales. No obstante, se recomienda evitar su continuo cambio en pro de la confianza, estabilidad y noción del sistema por parte del personal interno que ofrece mantenerlos, siempre y cuando cumplan con los propósitos de la entidad.

De la misma forma que es inevitable hoy día el uso de proveedores y externalizaciones, lo es para la sanidad pública el contar con clínicas concertadas. La interoperabilidad con estas clínicas debe de ser meticulosa y cautelosamente ejecutada, pues no solo es una vía de salida de datos de la organización, sino una posible vía de entrada de inoculaciones: malwares, exploits, inyecciones de código, etc.

Por muy bien y seguras que suenen las palabras International Health Standards, no hay que confiarse plenamente de su ejecución dentro de la infraestructura sanitaria. Como se ha visto en el trabajo, es usual que los estándares contengan vulnerabilidades. El *IHESEC* debe presionar a las entidades responsables para que las corrijan. Mientras tanto, hay que analizarlas, informarlas y mantenerse al tanto de ellas, corrigiéndolas on-site en los sistemas que los implementen.

Es desaconsejable dejar toda la responsabilidad de la seguridad en manos de autómatas. Las personas siguen siendo clave en los procedimientos y no deberían de ser completamente relevadas en ellos tras la adquisición de autómatas.

Asimismo, en la interoperabilidad entre varios sistemas, es un error dejar toda la responsabilidad de la seguridad en manos de uno solo de ellos. Cada sistema tiene un papel fundamental en la implementación conjunta de las medidas que garanticen la integridad, confidencialidad y disponibilidad de los datos transmitidos.

Es altamente recomendable contar con personal funcional activo en momentos de ciberincidentes para comprobar la correcta restauración de los sistemas y sus funciones. En el excepcional caso de no contar con ellos en un horario determinado, se debe contar con tests funcionales que prueben los sistemas tras un ciberincidente para dejar las instalaciones operativas ante la próxima jornada de trabajo.

Nunca hay descuidar las vulnerabilidades antiguas, pues los atacantes suelen volver a convertirlas en tendencia una vez que las entidades sanitarias las dan por superadas. De la misma forma, no hay que dar por mitigado ningún ciberincidente sin analizar todos los registros y eventos durante un tiempo prudencial y examinar concienzudamente todas las posibles afectaciones incluso indirectas.

El *IHESEC* debe presionar al Ministerio del Interior en la exigencia de que los centros sanitarios se mantengan siempre dentro del Catálogo Nacional de Infraestructuras Estratégicas.

A la par, es importante que las reivindicaciones en sanidad, como las de la llamada *Marea Blanca*, vayan acompañadas de las demandas en tecnología sanitaria y ciberseguridad, pues el sector ya depende íntimamente de la tecnología.

Debido precisamente a esta fusión entre medicina y tecnología, hace tiempo que la ciencia forense médica debería ir de la mano de la ciencia forense tecnológica en las lesiones y muertes de pacientes. Especialmente de aquellos que las hayan sufrido tras haberse sometido a un tratamiento mediante tecnología, por ejemplo, un ingresado en UCI, un paciente de diálisis, etc. O que llevase incorporado algún tipo de implante electrónico tal como una bomba de insulina o un marcapasos. Los

peritos forenses informáticos deben incorporarse a los procedimientos de evaluación de lesiones y autopsias de este tipo de pacientes. Estos especialistas forenses deben analizar si los dispositivos influyeron en la lesión o la muerte, ya sea de forma pasiva (mediante un mal funcionamiento debido a un bug, incompatibilidad con otro artefacto o cualquier fallo de fábrica), o de forma activa (mediante un ataque intencionado).

Por último, se recomienda informar siempre a los ciberatacantes de la calidad sanitaria de la infraestructura que han atacado y las posibles consecuencias para los pacientes y ellos mismos en materia penal si causaran muertes u otros perjuicios contra la salud de las personas. Se han dado casos en los que los ciberatacantes han cesado en el ataque o cedido la clave de descrifrado del ransomware cuando han sido informados de que la entidad infectada era hospitalaria.

12. Bibliografía

- [1] "Sofisticación en el antiguo Egipto: una prótesis de hace 3.000 años" [en línea]. [fecha de consulta: 06/10/2022]. Disponible en: https://historia.nationalgeographic.com.es/a/sofisticacion-antiguo-egipto-protesis-hace-3000-anos_11639

- [2] "Nueva sección sobre salud y protección de datos" [en línea]. [fecha de consulta: 06/10/2022]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/nueva-seccion-sobre-salud-y-proteccion-de-datos

- [3] "Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again" [en línea]. [fecha de consulta: 07/10/2022]. Disponible en: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

- [4] "El sector sanitario, entre los más desprotegidos contra los ciberataques avanzados" [en línea]. [fecha de consulta: 07/10/2022]. Disponible en: https://www.checkpoint.com/es/press/2018/el-sector-sanitario-entre-los-mas-desprotegidos-contra-los-ciberataques-avanzados/

- [5] "Investigation: WannaCry cyber attack and the NHS" [en línea]. [fecha de consulta: 07/10/2022]. Disponible en: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/#:~:text=On%20Friday%2012%20May%202017,been%20attacked%20before%2012%20May.

- [6] "Ransomware attacks on US healthcare organizations cost $7.8bn in 2021" [en línea]. [fecha de consulta: 08/10/2022]. Disponible en: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

- [7] "Cynerio. The State of Healthcare IoT Device Security 2022" [en línea]. [fecha de consulta: 08/10/2022]. Disponible en: https://www.cynerio.com/landing-pages/the-state-of-healthcare-iot-device-security-2022

- [8] "Survey Research Report - The Insecurity of Connected Devices in Healthcare 2022" [en línea]. [fecha de consulta: 09/10/2022]. Disponible en: https://www.cynerio.com/ponemon-survey-insecurity-of-connected-devices-in-healthcare-2022#ponemon-report

- [9] "Cybersecurity" [en línea]. [fecha de consulta: 09/10/2022]. Disponible en: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

- [10] "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas." https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

- [11] "Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información." [en línea]. [fecha de consulta: 02/11/2022]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

- [12] "Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información." [en línea]. [fecha de consulta: 02/11/2022]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

- [13] "Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección

de las infraestructuras críticas." [en línea]. [fecha de consulta: 02/11/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

- [14] "CSIRT Capabilities in Healthcare Sector" [en línea]. [fecha de consulta: 10/10/2022]. Disponible en: https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector
- [15] "Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed" [en línea]. [fecha de consulta: 10/10/2022]. Disponible en: https://pages.checkpoint.com/cyber-security-report-2022.html
- [16] "FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps" [en línea]. [fecha de consulta: 07/11/2022]. Disponible en: https://www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain
- [17] "MiniMed™ 508 Insulin Pump and MiniMed™ Paradigm™ Series Insulin Pumps" [en línea]. [fecha de consulta: 07/11/2022]. Disponible en: https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice11-letter
- [18] "La AEMPS informa de un posible problema de seguridad con el método de comunicación de las bombas de insulina MiniMedTM serie 600" [en línea]. [fecha de consulta: 07/11/2022]. Disponible en: https://www.aemps.gob.es/informa/la-aemps-informa-de-un-posible-problema-de-seguridad-con-el-metodo-de-comunicacion-de-las-bombas-de-insulina-minimedtm-serie-600/
- [19] "ICS Medical Advisory (ICSMA-19-080-01)" [en línea]. [fecha de consulta: 07/11/2022]. Disponible en: https://www.cisa.gov/uscert/ics/advisories/ICSMA-19-080-01
- [20] "Critical flaw lets hackers control lifesaving devices implanted inside patients" [en línea]. [fecha de consulta: 07/11/2022]. Disponible en: https://arstechnica.com/information-technology/2019/03/critical-flaw-lets-hackers-control-lifesaving-devices-implanted-inside-patients/
- [21] "Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal." [en línea]. [fecha de consulta: 08/11/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
- [22] "Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía" [en línea]. [fecha de consulta: 25/11/2022]. Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf
- [23] "REFERENCE TAXONOMY INCIDENT Taxonomy (human readable version)" [en línea]. [fecha de consulta: 03/12/2022]. Disponible en: https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md
- [24] "Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2002-22188
- [25] "Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2003-10715https://www.boe.es/buscar/act.php?id=BOE-A-2003-10715

- [26] “Ley 14/2007, de 3 de julio, de Investigación Biomédica” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12945
- [27] “Ley 14/1986, de 25 de abril, General de Sanidad” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1986-10499
- [28] “Ley 33/2011, de 4 de octubre, General de Salud Pública” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-15623
- [29] “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
- [30] “Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2006-16212
- [31] “Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-1235
- [32] “Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2004-2591
- [33] “Real Decreto 1277/2003, de 10 de octubre, por el que se establecen las bases generales sobre autorización de centros, servicios y establecimientos sanitarios” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2003-19572
- [34] “Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14199
- [35] “Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf
- [36] “Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) nº 178/2002 y el Reglamento (CE) nº 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R0745&from=DA
- [37] “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” [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330
- [38] “Norma UNE-EN 80001. Aplicación de la gestión del riesgo para las redes de tecnología de

la información que incorporan dispositivos médicos" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.en.aenor.com/_layouts/15/r.aspx?c=N0050043

- [39] "Normas UNE-ISO 27001. Sistemas de Gestión de la Seguridad de la Información" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://ll-c.es/certificacion/iso-27001/?http://ll-c.cz/www/home_page.asp?Domain=cz&gclid=Cj0KCQiAvqGcBhCJARIsAFQ5ke4m79igIsOZyT88VCDqHDaSydPuQI5tNf0rx9aNjkP2IzzXX7tAk1QaAr2mEALw_wcB

- [40] "Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2014-5111

- [41] "Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1331

- [42] "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

- [43] "Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

- [44] "Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10060

- [45] "Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352

- [46] "Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2009-18358

- [47] "Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2001-18256

- [48] "Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones" [en línea]. [fecha de consulta: 05/12/2022]. Disponible en: https://www.boe.es/buscar/pdf/2007/BOE-A-2007-18243-consolidado.pdf

- [49] "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad" [en línea]. [fecha de consulta: 20/12/2022]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

- [50] "About HL7" [en línea]. [fecha de consulta: 21/12/2022]. Disponible en:

https://www.hl7.org/about/index.cfm?ref=nav

- [51] ”About DICOM: Overview” [en línea]. [fecha de consulta: 22/12/2022]. Disponible en: https://www.dicomstandard.org/about
- [52] “HL7 Data Interfaces in Medical Environments: Attacking and Defending the Achille's Heel of Healthcare” [en línea]. [fecha de consulta: 23/12/2022]. Disponible en: https://www.sans.org/white-papers/38010/
- [53] “Vulnerability Details : CVE-2019-11687” [en línea]. [fecha de consulta: 24/12/2022]. Disponible en: https://www.cvedetails.com/cve/CVE-2019-11687/
- [54] “CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning” [en línea]. [fecha de consulta: 25/12/2022]. Disponible en: https://www.usenix.org/system/files/sec19-mirsky_0.pdf
- [55] “Injecting and Removing Cancer from CT Scans” [en línea]. [fecha de consulta: 26/12/2022]. Disponible en: https://www.youtube.com/watch?v=_mkRAArj-x0
- [56] “ymirsky/CT-GAN Public” [en línea]. [fecha de consulta: 27/12/2022]. Disponible en: https://github.com/ymirsky/CT-GAN
- [57] “Consejo Interterritorial SISTEMA NACIONAL DE SALUD Acuerdo nº: 1369” [en línea]. [fecha de consulta: 28/12/2022]. Disponible en: https://www.sanidad.gob.es/organizacion/consejoInterterri/docs/1369.pdf