UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola d'Enginyeria de Barcelona Est

TRABAJO DE FINAL DE GRADO

Grado en Ingeniería Biomédica

CIBERSEGURIDAD EN EL ÁMBITO SANITARIO

Memoria y Anexos

Autor/a:	Carmen Galán Lucerón
Tutor:	Víctor Manuel Santiago Praderas
Co-tutor externo:	Javier Farreres De La Morena
Director experimental:	Luis Taroncher Pellicer
Convocatoria:	Junio 2023

Resumen

El sector sanitario es uno de los más vulnerables y afectados por los incidentes cibernéticos, que pueden poner en riesgo la seguridad de los pacientes, la confidencialidad de los datos y la continuidad de los servicios. Por esta razón, es necesario sensibilizar sobre la importancia de la ciberseguridad en este ámbito y adoptar medidas preventivas y correctivas para mitigar y reducir los posibles daños.

En este trabajo de fin de estudios se pretende realizar un análisis multidisciplinar del estado actual de la ciberseguridad en el sector sanitario, a partir de una revisión bibliográfica exhaustiva que abarca los siguientes aspectos: los costos asociados a los incidentes cibernéticos, la discusión sobre la conciliación de los fundamentos de la deontología médica y la aplicación de las TIC en el sector, la normativa vigente a nivel nacional e internacional, los riesgos más comunes y las buenas prácticas para evitarlos, y dos casos reales recientes de hospitales que han sido víctimas de ataques cibernéticos, en los que se mostraran las lecciones aprendidas.

Con ello, se pretende alcanzar el objetivo principal de este trabajo, que es concienciar sobre el impacto que los incidentes cibernéticos presentan en la actualidad sobre el sector sanitario y ofrecer recomendaciones para mejorar la protección y la resiliencia de las organizaciones sanitarias frente a las amenazas cibernéticas.

Resum

El sector sanitari és un dels més vulnerables i afectats pels incidents cibernètics, que poden posar en risc la seguretat dels pacients, la confidencialitat de les dades i la continuïtat dels serveis. Per aquesta raó, cal sensibilitzar sobre la importància de la ciberseguretat en aquest àmbit i adoptar mesures preventives i correctives per mitigar i reduir els possibles danys.

En aquest treball de fi d'estudis es pretén fer una anàlisi multidisciplinària de l'estat actual de la ciberseguretat al sector sanitari, a partir d'una revisió bibliogràfica exhaustiva que abasta els aspectes següents: els costos associats als incidents cibernètics, la discussió sobre la conciliació dels fonaments de la deontologia mèdica i l'aplicació de les TIC al sector, la normativa vigent a nivell nacional i internacional, els riscos més comuns i les bones pràctiques per evitar-los, i dos casos reals recents d'hospitals que han estat víctimes d'atacs cibernètics, en què es mostren les lliçons apreses.

Amb això, es pretén assolir l'objectiu principal d'aquest treball, que és conscienciar sobre l'impacte que els incidents cibernètics presenten actualment sobre el sector sanitari i oferir recomanacions per millorar la protecció i la resiliència de les organitzacions sanitàries davant de les amenaces cibernètiques .

Abstract

The healthcare sector is one of the most vulnerable and affected by cyber incidents, which can jeopardise patient safety, data confidentiality and continuity of services. For this reason, it is necessary to raise awareness of the importance of cybersecurity in this area and to adopt preventive and corrective measures to mitigate and reduce potential damage.

The aim of this thesis is to carry out a multidisciplinary analysis of the current state of cybersecurity in the healthcare sector, based on a comprehensive literature review covering the following aspects: the costs associated with cyber incidents, the discussion on the reconciliation of the fundamentals of medical ethics and the application of ICT in the sector, the current national and international regulations, the most common risks and good practices to avoid them, and two recent real cases of hospitals that have been victims of cyber attacks, in which the lessons learned will be shown.

This is intended to achieve the main objective of this work, which is to raise awareness of the impact that cyber incidents currently have on the healthcare sector and to offer recommendations to improve the protection and resilience of healthcare organisations in the face of cyber threats.

Agradecimientos

Me gustaría expresar mi más sincero agradecimiento a las personas que han hecho posible la realización de este trabajo. En primer lugar, a mi tutor Javier Farreres De La Morena, por confiar en mí y guiarme en el desarrollo del proyecto, así como sugerirme el interesante caso del Hospital Clínic como objeto de estudio.

En segundo lugar, a Xavier Pastor, jefe del departamento de informática médica por concederme la oportunidad de entrevistarle y compartir conmigo sus experiencias sobre el incidente ocurrido en el centro.

Por último, a Nerea Palacios, secretaria del Doctor Pastor, por facilitarme la gestión y coordinación de la entrevista, atendiendo a las indicaciones que he ido requiriendo.

A todos ellos, les estoy profundamente agradecida por su colaboración y apoyo.

Glosario

Término	Siglas	Descrición
Agencia de Ciberseguridad de Cataluña	ACC	Organismo encargado de garantizar la seguridad cibernética en Cataluña.
Agencia Europea de Ciberseguridad	ENISA	Agencia de la Unión Europea que tiene como objetivo fomentar la ciberseguridad en Europa.
Autentificación de dos factores	2FA	Método de autentificación que requiere de dos formas diferentes de identificación.
Centre Hospitalier Universitaire	CHU	Hospital universitario en Francia que también puede referirse a otros hospitales en países francófonos.
Centro Criptológico Nacional	CCN	Centro español encargado de la criptografía y la seguridad informática.
Centro Nacional de Protección de Infraestructuras Críticas	CNPIC	Organismo español encargado de proteger las infraestructuras críticas del país.
Centro de proceso de datos	CPD	Instalación que alberga los servidores y los sistemas de almacenamiento de una organización.
Control de acceso basado en roles	RBAC	Sistema de control de acceso que otorga permisos de acuerdo con el rol del usuario.
Departamento de Seguridad Nacional	DNS	Organismo estadounidense encargado de proteger el país de amenazas externas.
Electronic Health Record	EHR	Registro electrónico de una información médica de un paciente.
Electronic Medical Record	EMR	Registro electrónico de la información médica de un paciente en un solo centro de salud.
Equipo de respuesta a incidentes de ciberseguridad de la Unión Europea	CERT-UE	Equipo de respuesta a incidentes de ciberseguridad de la Unión Europea.
Equipo de respuesta a incidentes de seguridad informática	CSIRT	Equipo encargado de responder a incidentes de seguridad informática en una organización.
Historia clínica electrónica	HCE	Registro electrónico de la información médica de un paciente en un hospital.
Instituto Nacional de Ciberseguridad	INCIBE	Centro español encargado de la ciberseguridad en el país.
Planificación de Recursos Empresariales	ERP	Sistema de gestión empresarial que integra procesos y datos en una sola plataforma.
Reglamento General de Protección de Datos	RGPD	Regulación de la Unión Europea que protege los datos personales de los ciudadanos.
Sistema de Emergencias Médicas	SEM	Servicio encargado de responder a emergencias médicas y de transporte sanitario.
Sistema de Información Sanitaria	HIS	Sistema de gestión de la información médica de un hospital.
Sistema Operativo	SO	Software que controla el hardware y permite que otros programas se ejecuten en un ordenador.

Sistemas de administración de información y eventos de seguridad	SIEM	Herramienta de ciberseguridad que recopila y analiza información de eventos en tiempo real.
Tecnología de la Información	TI	Conjunto de herramientas, procesos y técnicas utilizados para procesar y transmitir información.
Tecnologías de la información y la comunicación	TIC	Conjunto de tecnologías utilizadas para procesar, almacernar, transmitir y recibir información.

Índice

Introducción

Según la empresa tecnológica multinacional IBM, "la ciberseguridad es la práctica de proteger los sistemas críticos y la información confidencial de los ataques digitales. También conocidas como seguridad de la Tecnología de la Información (TI), las medidas de seguridad cibernética están diseñadas para combatir las amenazas contra los sistemas y aplicaciones en red, ya sea que esas amenazas se originen desde dentro o fuera de una organización".*[1]*

En la actualidad, la seguridad cibernética se ha convertido en una preocupación creciente a nivel mundial, sobre todo en el sector sanitario, pues a medida que la tecnología avanza, las organizaciones sanitarias dependen cada vez más tanto de los sistemas digitales para almacenar, gestionar y transmitir los datos médicos, como de los dispositivos médicos, indispensables para el tratamiento y mejora de los pacientes.

La Seguridad Hospitalaria se define según el artículo *[2]* como: "la condición que garantiza que los trabajadores, pacientes, visitantes, infraestructura y equipos dentro de un centro de atención en salud, estén libres de riesgo o peligro de accidentes". Sin embargo, la responsabilidad de proteger la privacidad y seguridad en los servicios sanitarios se ha dificultado con la progresiva adopción de la tecnología en la atención médica, que ha advertido el problema de las vulnerabilidades del sector con respecto a ciberataques cada vez más sofisticados.

Generalmente, los sistemas de TI en el sector sanitario suelen ser vulnerables a los ataques cibernéticos debido a la falta de seguridad en la infraestructura de TI y la falta de concienciación en cuanto a las amenazas cibernéticas. Además, las vulnerabilidades presentes en los dispositivos médicos pueden poner en riesgo la propia salud del paciente.

Por lo que, la identificación y mitigación de vulnerabilidades en sector es fundamental para que se garanticen la disponibilidad, integridad y confidencialidad de la información médica, así como la seguridad del paciente.

La evolución de los ciberataques se hizo notable con la llegada de la pandemia COVID-19, como se anunció en el informe de la Agencia Europea de Ciberseguridad (ENISA),*[3]* donde se indica que hubo "304 ciberataques significativos y maliciosos contra sectores críticos en 2020, más del doble de los 146 registrados el año anterior". De hecho, los hospitales fueron uno de los principales sectores, pues el número de incidentes se incrementó en un 42% en 2020.*[4]*

Asimismo, en el reciente informe del segundo cuatrimestre de 2022 del Observatorio de Ciberseguridad de Exprivia *[5]* se ha señalado un incremento del 77% respecto a las amenazas informáticas del cuatrimestre anterior. También se espera que el 68% de los equipos médicos estén conectados a Internet en 2025, lo que establece aún más la vulnerabilidad del sector salud a los ciberataques.*[6]*

Por tanto, la ciberseguridad se ha convertido en una preocupación fundamental en el sector sanitario debido a la creciente dependencia de la tecnología digital en la atención médica, pues a medida que los sistemas de TI y los dispositivos médicos se vuelven más sofisticados, también lo hacen los ciberataques, aumentando así el riesgo de violaciones de seguridad y privacidad en el sector.

Es crucial que las organizaciones sanitarias identifiquen y mitiguen las vulnerabilidades en sus sistemas y dispositivos médicos para garantizar la seguridad del paciente y la confidencialidad de la información médica. Dado el aumento constante de las amenazas informáticas en el sector de la salud, es esencial que se tomen medidas efectivas y continuas para proteger a las organizaciones sanitarias de los ciberataques.

1.1. Objetivos

El principal objetivo de este Trabajo de Fin de Estudios es concienciar sobre el impacto que los incidentes cibernéticos presentan en la actualidad sobre el sector sanitario. Para ello, se han establecido objetivos más concretos que complementarán el proceso de estudio:

- Analizar el impacto financiero y ético-social de los incidentes de ciberseguridad en el sector sanitario.
- Evaluar las políticas y regulaciones españolas en relación con la privacidad y seguridad de los datos médicos.
- Sensibilizar sobre las vulnerabilidades y amenazas más habituales dentro de las organizaciones sanitarias.
- Analizar casos específicos y recientes de ciberataques en hospitales, así como la forma en que fueron gestionados y resueltos para extraer las lecciones aprendidas y recomendaciones para futuros incidentes.
- Estudiar las medidas de seguridad existentes en las organizaciones sanitarias y evaluar su eficacia para prevenir, detectar y responder a los incidentes de seguridad cibernética.
- Estudiar las posibles medidas de seguridad futuras para mejorar la seguridad y la resiliencia del sector ante las amenazas cibernéticas.

1.2. Planificación

La distribución temporal del Trabajo de Fin de Estudios se ha llevado a cabo mediante el programa GanttPRO, que permite crear un Diagrama de Gantt, en el que se muestran las tareas a realizar, su duración y su dependencia. En la Ilustración 1 se presentael diagrama de Gantt para la planificación global del proyecto.

Dentro de la planificación global, que abarca desde el 13/02/2023 hasta el 07/07/2023, se han dividido cinco partes diferenciadas o hitos en los que se han incluido como tareas los apartados a tratar en el trabajo, así como la búsqueda bibliográfica, la elaboración del índice provisional, la revisión general, el depósito, la preparación de la presentación y la defensa.

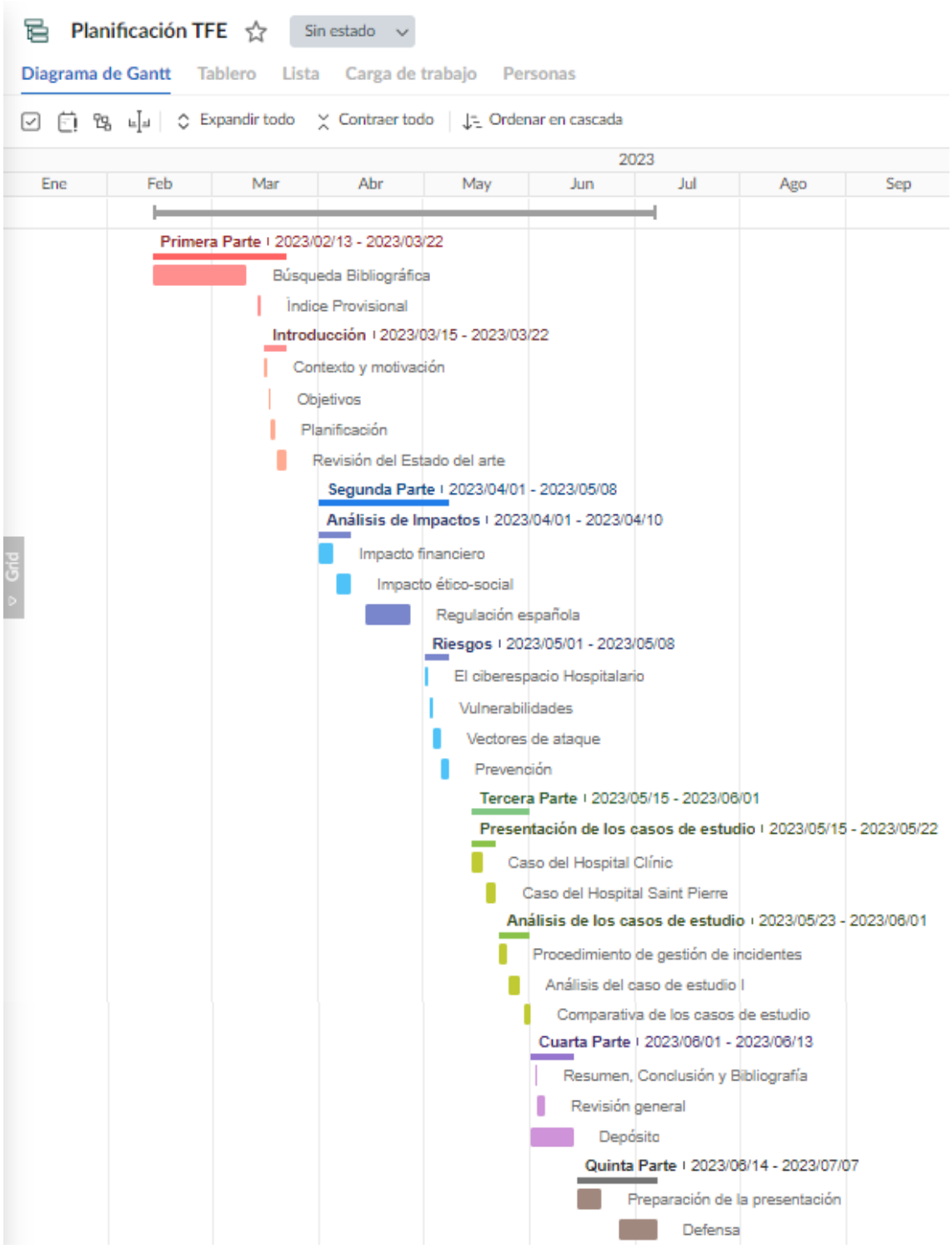

Ilustración 1. Diagrama de Gantt para la planificación global del proyecto. Realizado con GanttPRO.

En la primera parte o hito se incluyen las tareas relacionadas con la organización de la información y la puesta en marcha del proyecto. Estas tareas se han planificado para que sean realizadas en el periodo de tiempo comprendido entre el 13/02/2023 y el 22/02/2023.

Nombre de tarea	Fecha de inicio	Fecha final
	2023/02/13	2023/07/07
⊟ **Primera Parte**	**2023/02/13**	2023/03/22
Búsqueda Bibliográfica	2023/02/13	2023/03/10
Índice Provisional	2023/03/14	2023/03/14
⊟ **Introducción**	**2023/03/15**	2023/03/22
Contexto y motivación	2023/03/15	2023/03/17
Objetivos	2023/03/17	2023/03/17
Planificación	2023/03/18	2023/03/19
Revisión del Estado del arte	2023/03/19	2023/03/22

Ilustración 2. Listado de tareas y subtareas para la planificación de la primera parte del proyecto.

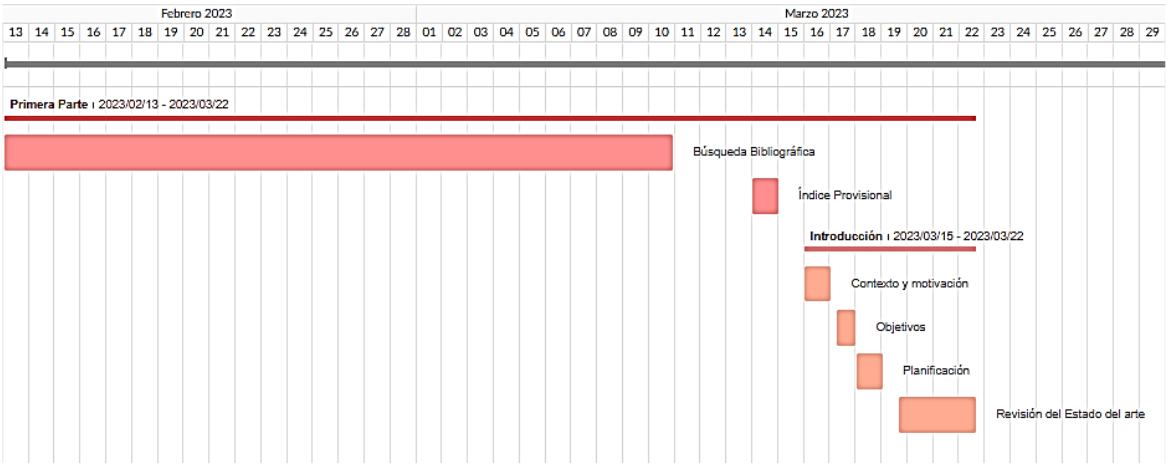

Ilustración 3. Diagrama de Gantt de las tareas y subtareas de la primera parte del proyecto. Realizado con GanttPRO.

En la segunda parte o hito se incluyen las tareas relacionadas con el desarrollo de la información teórica, que sirve para comprender los conceptos básicos de la materia. Estas tareas se han planificado para que sean realizadas en el periodo de tiempo comprendido entre el 01/04/2023 y el 08/05/2023.

Segunda Parte	**2023/04/01**	2023/05/08
Análisis de Impactos	**2023/04/01**	2023/04/10
Impacto financiero	2023/04/01	2023/04/05
Impacto ético-social	2023/04/06	2023/04/10
Regulación española	2023/04/14	2023/04/27
Riesgos	**2023/05/01**	2023/05/08
El ciberespacio Hospitalario	2023/05/01	2023/05/02
Vulnerabilidades	2023/05/02	2023/05/03
Vectores de ataque	2023/05/03	2023/05/05
Prevención	2023/05/06	2023/05/08

Ilustración 4. Listado de tareas y subtareas para la planificación de la segunda parte del proyecto.

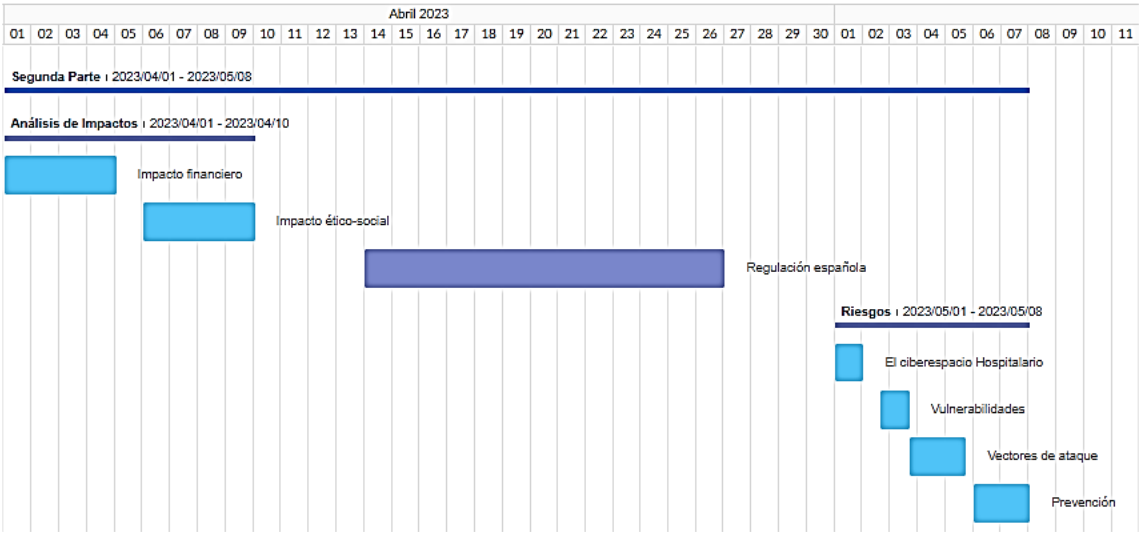

Ilustración 5. Diagrama de Gantt de las tareas y subtareas de la segunda parte del proyecto. Realizado con GanttPRO.

En la tercera parte o hito se incluyen las tareas relacionadas con el desarrollo y análisis de dos casos reales, lo que sirve para poner en práctica los conocimientos teóricos adquiridos. Estas tareas se han planificado para que sean realizadas en el periodo de tiempo comprendido entre el 15/05/2023 y el 01/06/2023.

Tercera Parte	**2023/05/15**	2023/06/01
Presentación de los casos de estudio	**2023/05/15**	2023/05/22
Caso del Hospital Clínic	2023/05/15	2023/05/18
Caso del Hospital Saint Pierre	2023/05/19	2023/05/22
Análisis de los casos de estudio	**2023/05/23**	2023/06/01
Procedimiento de gestión de incidentes	2023/05/23	2023/05/25
Análisis del caso de estudio I	2023/05/26	2023/05/29
Comparativa de los casos de estudio	2023/05/30	2023/06/01

Ilustración 6. Listado de tareas y subtareas para la planificación de la tercera parte del proyecto.

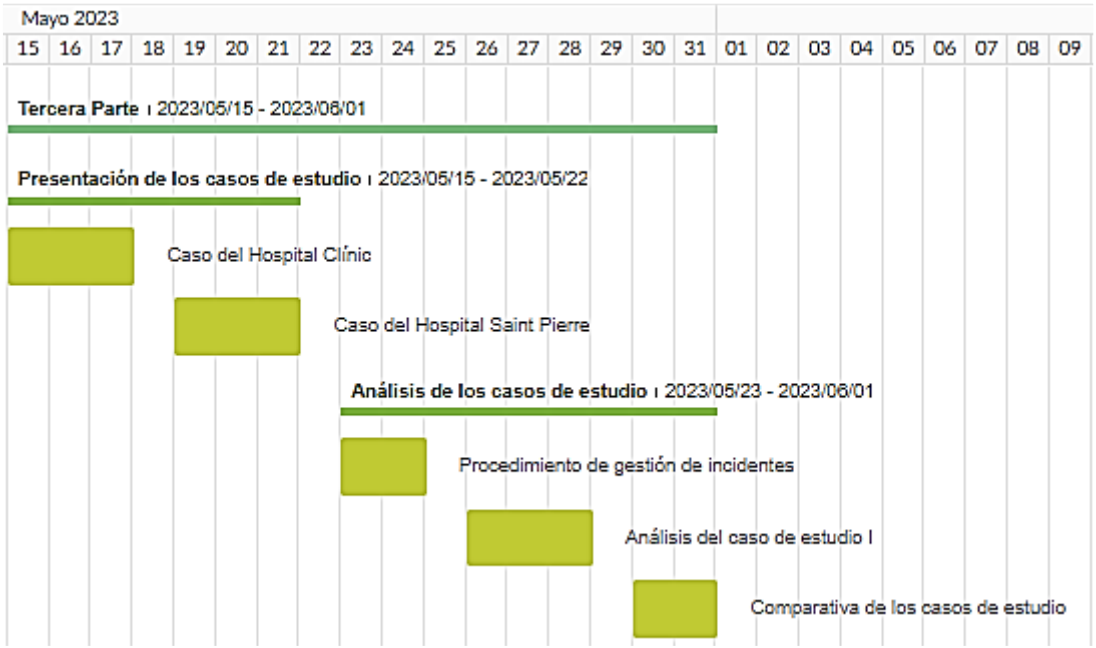

Ilustración 7. Diagrama de Gantt de las tareas y subtareas de la tercera parte del proyecto. Realizado con GanttPRO.

En la cuarta parte o hito se incluyen las tareas relacionadas con la finalización y la entrega del proyecto. Estas tareas se han planificado para que sean realizadas en el periodo de tiempo comprendido entre el 01/06/2023 y el 13/06/2023.

Cuarta Parte	**2023/06/01**	2023/06/13
Resumen, Conclusión y Bibliografía	2023/06/02	2023/06/02
Revisión general	2023/06/03	2023/06/05
Depósito	2023/06/01	2023/06/13

Ilustración 8. Listado de tareas y subtareas para la planificación de la cuarta parte del proyecto.

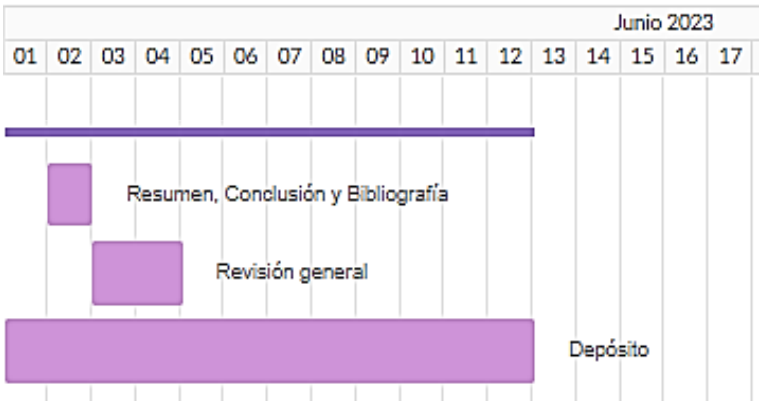

Ilustración 9. Diagrama de Gantt de las tareas y subtareas de la cuarta parte del proyecto. Realizado con GanttPRO.

En la quinta parte o hito se incluyen las tareas relacionadas con la organización y realización de la presentación oral del proyecto. Estas tareas se han planificado para que sean realizadas en el periodo de tiempo comprendido entre el 14/06/2023 y el 07/07/2023.

Quinta Parte	2023/06/14	2023/07/07
Preparación de la presentación	2023/06/14	2023/06/21
Defensa	2023/06/26	2023/07/07

Ilustración 10. Listado de tareas y subtareas para la planificación de la quinta parte del proyecto.

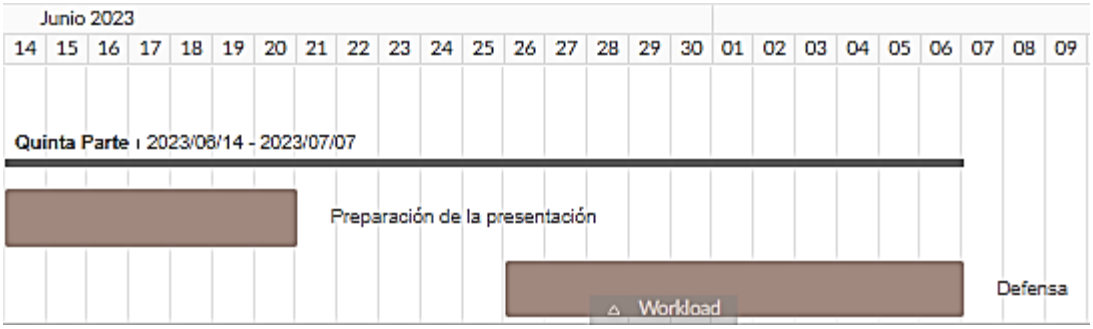

Ilustración 11. Diagrama de Gantt de las tareas y subtareas de la quinta parte del proyecto. Realizado con GanttPRO

1.3. Revisión del Estado del arte

El sector sanitario es un sector crítico que maneja la información personal y sensible de los pacientes, por lo que la ciberseguridad es de vital importancia para garantizar la privacidad y seguridad de la información confidencial. En el presente apartado se ha realizado un análisis del estado del arte en cuanto a la ciberseguridad en el ámbito de la salud, tratando el marco regulador de la Unión Europea (UE) así como el mecanismo de certificación actual de los productos y servicios digitales en el sector de estudio.

En la actualidad, la Unión Europea ha adoptado un marco reglamentario para la ciberseguridad que está conformado por varias normativas y entidades que buscan garantizar la fiabilidad de los sistemas críticos así como una respuesta rápida y coordinada frente a incidentes de seguridad.

El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, *[7]* se trata de un aspecto relevante en cuanto a la normativa en materia ya que tiene como objetivo reforzar la ciberseguridad en la Unión Europea. El Reglamento establece dos elementos principales: una Agencia de la Unión Europea para la Ciberseguridad (ENISA) con un mandato permanente y un marco para la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (TIC).

ENISA es una agencia descentralizada que apoya a las autoridades nacionales y a las instituciones de la UE en el desarrollo y la aplicación de políticas y medidas de ciberseguridad. Se encarga de contribuir a la prevención, detección y respuesta a las ciberamenazas; fomentar la cooperación y el intercambio de información entre los Estados miembros; ofrecer asesoramiento científico y técnico sobre cuestiones de ciberseguridad; y promover la sensibilización y la formación en materia de ciberseguridad.*[8]*

El marco de certificación de la ciberseguridad de la UE para los productos de TIC proporciona sistemas de certificación adaptados y basados en el nivel de riesgo. La certificación juega un papel fundamental para afianzar la seguridad de los productos y servicios digitales. De hecho, en la actualidad existen varios sistemas de certificación diferentes en la UE para los productos TIC, lo que puede generar fragmentación y barreras entre los Estados miembros. *[9]*

Para abordar esta situación, se ha propuesto un marco formado por el conjunto completo de normas, requisitos técnicos y procedimientos de certificación. El marco

se basa en un acuerdo a escala de la UE sobre la evaluación de las propiedades de seguridad de un producto o servicio TIC, lo que demuestra que los productos y servicios que han sido certificados cumplen con los requisitos especificados. Los niveles de garantía utilizados informarán a los usuarios del riego de ciberseguridad de un producto ya que vendrán clasificados como básicos, sustanciales o altos. Así, este certificado será reconocido en todos los Estados miembros de la UE, lo que facilitará a las empresas comerciar y a los compradores entender las características de seguridad del producto o servicio. *[9]*

Como primer mecanismo de certificación se ha creado Europrivacy,*[10]* para asegurar el cumplimiento del Reglamento General de Protección de Datos (RGPD). El RGPD es de especial relevancia en el sector de estudio, ya que se establecen las bases legales para el tratamiento de datos personales en las organizaciones sanitarias que incluyen el consentimiento del paciente, la obligación legal y el interés público en la protección de la salud pública. Concretamente, Europrivacy puede utilizarse para:

- Evaluar el cumplimiento de las actividades de procesamiento de datos.
- Seleccionar procesadores de datos.
- Evaluar la idoneidad de las transferencias de datos transfronterizas.
- Garantizar a los ciudadanos y clientes el tratamiento adecuado de los datos personales.

Por lo tanto, el sello puede ayudar a mejorar la protección de datos en el sector sanitario y garantizar el cumplimento de las normas de protección de datos ya que permite identificar y reducir sus riesgos, demostrar y evaluar su conformidad con las normas nacionales complementarias de protección de datos.

Por otro lado, cabe destacar la propuesta sobre el proyecto del Reglamento de la Comisión de marzo de 2022,*[11]* destinado a garantizar un elevado nivel común de ciberseguridad en todas las instituciones, órganos y organismos de la UE. Para ello, incluye el fortalecimiento del mandato y la financiación del Equipo de Respuesta a Emergencias Informáticas de las instituciones de la Unión Europea (CERT-UE), la creación de un Consejo Interinstitucional de Ciberseguridad para guiar y supervisar la implementación del nuevo reglamento y la promoción de la coordinación y cooperación en la respuesta a incidentes cibernéticos.

El CERT-UE, se trata de un equipo de expertos en seguridad informática de las instituciones y los órganos de la UE. El equipo recopila, gestiona, analiza y comparte información con las instituciones, los órganos y las agencias de la UE sobre amenazas, vulnerabilidades e incidentes relacionados con infraestructuras de TIC no clasificadas.*[12]*

En el Reglamento también se incluye la actualización del marco legal sobre la seguridad de las redes y sistemas de información (Directiva NIS 2) o Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la UE.*[13]*

Tiene como objetivo reforzar la resiliencia y la capacidad de respuesta de los Estados miembros y de la UE ante amenazas y los incidentes cibernéticos. Para ello, establece una serie de disposiciones que abarcan los siguientes aspectos:

- **Artículo 7.** La cooperación entre los Estados miembros y la UE en materia de ciberseguridad, mediante la coordinación entre las autoridades competentes nacionales y europeas, así como el desarrollo de planes nacionales y europeos de gestión de crisis cibernéticas.

- **Artículo 4.** La identificación y el establecimiento de requisitos de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales que prestan servicios en el mercado interior, así como para los productos, servicios y procesos TIC que se consideren críticos para la seguridad de la UE.

Análisis financiero y ético-social

2.1. Análisis financiero

En este subapartado se lleva a cabo un análisis del impacto financiero de los incidentes cibernéticos en función de los diferentes tipos de costes que pueden afectar a las organizaciones hospitalarias. En concreto, se examinan los costes de detección y escalado, los costes de pérdida de negocio, costes de notificación y respuesta y otros costes adicionales. Además, para proporcionar una evaluación rigurosa del estudio, se aportan datos extraídos del informe de 2022 sobre el coste de la filtración de datos realizado por IBM en colaboración con el Instituto Ponemon.*[14]*

Las brechas de seguridad en el sector sanitario se han convertido en una preocupación grave a nivel financiero, pues se trata del sector crítico más caro donde el coste medio por infracción ha alcanzado los 10,10 millones de dólares.

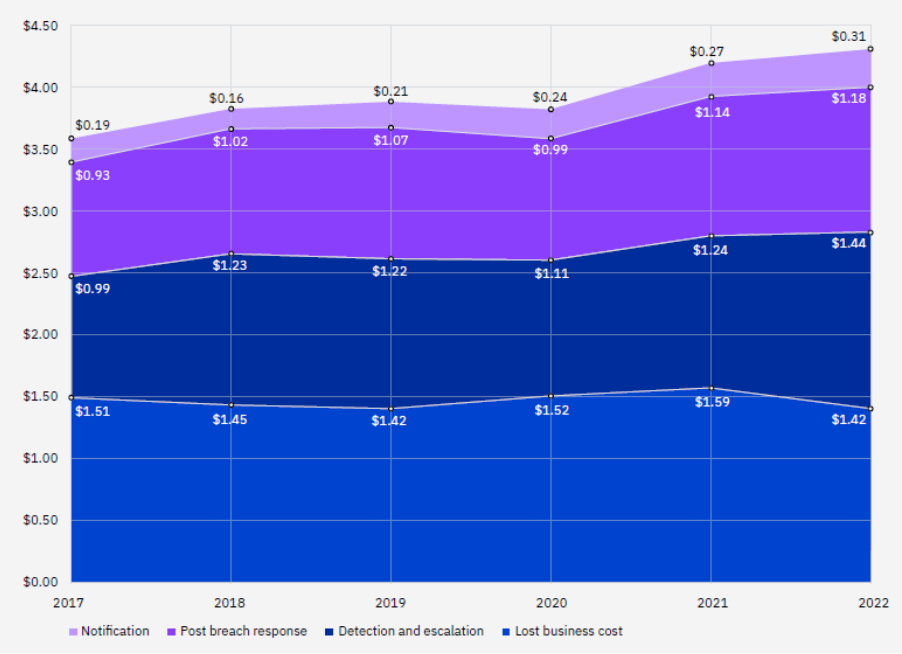

Gráfico 1. Coste medio de una violación de datos dividido en cuatro segmentos. [14]

Como se muestra en el Gráfico 1 la mayor parte de los costes por violación de datos en 2022 se corresponde a la fase de detección y escalado, pues han ascendido a 1,44 millones de dólares, lo que representa un aumento del 16,1% con respecto al año anterior. En este tipo de costes se incluyen actividades que permiten la

identificación temprana de la infracción como la implementación de tecnologías de seguridad avanzadas, la contratación de expertos en ciberseguridad y la realización de auditorías de seguridad regulares.

En el informe, se demuestra como el establecimiento de tecnologías de inteligencia artificial y automatización de seguridad supone un ahorro del 65,2% frente a organizaciones que carecen de dichos sistemas. Además, contar con un CERT que lleve a cabo un plan de respuesta ante incidentes también presenta un ahorro significativo de 2,66 millones de dólares.

Respecto a los costes por pérdida de negocio, se refieren a los daños financieros que una organización puede sufrir debido a la disminución de productividad, a la pérdida de ingresos por la caída del sistema y a la pérdida de clientes por reputación. En el Gráfico 1 se aprecia como este tipo de costes han descendido con respecto al año anterior pero aún suponen 1,42 millones de dólares.

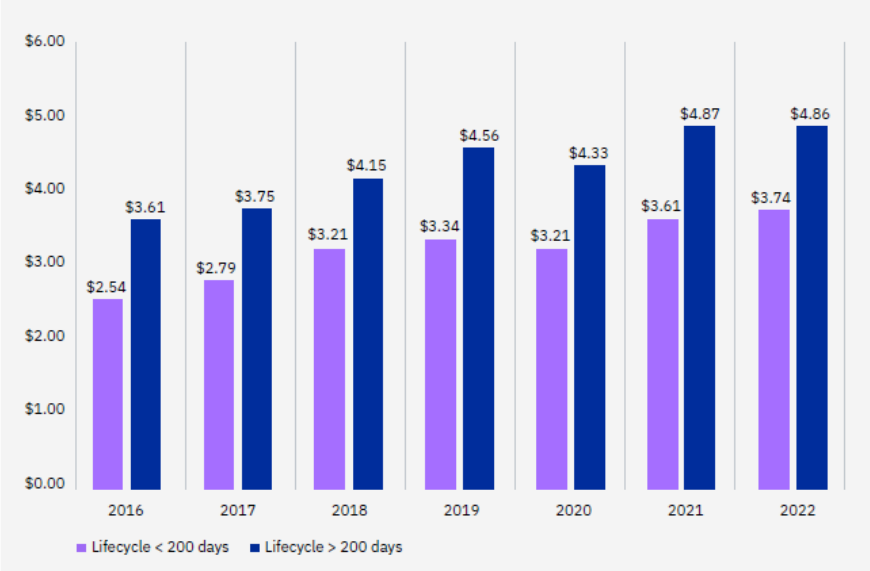

Gráfico 2. Coste medio de una violación de datos según el ciclo de vida. IBM Security. (2022).[14]

En el Gráfico 2 se hace evidente como un ciclo de vida más corto de la violación de datos se asocia a unos costes más bajos. Concretamente se refleja un ahorro de costes del 26,5% en ciclos de vida inferiores a 200 días frente a ciclos de vida superiores a 200 días. Por tanto, en los costes por pérdida de negocio también influye la disposición de tecnología de seguridad avanzada, así como la presencia de un equipo experto, pues si las organizaciones se encuentran mejor preparadas, el tiempo de actuación será más temprano y como consecuencia, el impacto financiero será menos agresivo. De hecho, en las organizaciones con IA y automatización de la seguridad se tarda una media de 181 días en identificar la

filtración de datos y 68 días en contenerla, lo que supone un ciclo de vida total de 249 días, mientras que las organizaciones que no cuentan con los sistemas mencionados tardan una media de 235 días en identificar la filtración y 88 días en contenerla, lo que supone un ciclo de 323 días.

Entre los costes de notificación y respuesta, se encuentran la reparación o reemplazo de los dispositivos infectados y los costes de restauración y comunicación de los datos perdidos o dañados. Estos tipos de costes pueden variar en función del impacto del ataque, así como el tipo y la cantidad de dispositivos afectados, ya que no es lo mismo reemplazar un hardware costoso de equipos de imagen médica, que ordenadores de escritorio. Sin embargo el conjunto de coste promedio de estos gastos oscila entre los 1.49 millones de dólares.

Respecto a los costes adicionales derivados de una infracción de ciberseguridad, se muestra las organizaciones con altos niveles de incumplimiento de normativa pueden enfrentarse a un coste medio de 5,57 millones de dólares. Por otro lado, contar con personal insuficiente en materia de ciberseguridad puede suponer un ahorro medio de 550.000 dólares.

A partir de los resultados actualizados y extraídos del informe se concluye que es indispensable realizar inversiones tanto para la adopción de tecnología avanzada en seguridad, como en el desarrollo de un equipo altamente competente en la materia. De esta manera se podrán mitigar los impactos derivados de una violación de datos y reducir el conjunto de costes tan elevados que este incidente conlleva. La aplicación de medidas preventivas y correctivas también ayudará a aumentar la eficiencia y calidad de los servicios sanitarios y con ello, se mejorará la reputación del sector.

2.2. Análisis ético-social

La implementación de las TIC en el sector sanitario ha incorporado la protección de los datos personales, la protección de los sistemas de información y la protección de los dispositivos médicos. No obstante, su despliegue en la asistencia sanitaria plantea preocupaciones éticas, pues los ataques cibernéticos suponen amenazas que pueden poner en peligro la calidad y eficiencia de los servicios, la protección de la confidencialidad y seguridad de los pacientes y la usabilidad de los sistemas y dispositivos.

Por esta razón, es fundamental garantizar la fiabilidad de las TIC a través de medidas de ciberseguridad, ya que permiten asegurar la protección de la privacidad y seguridad de los pacientes. Sin embargo, la implementación de estas medidas puede afectar a la usabilidad de los sistemas y dispositivos médicos, lo que a su vez puede comprometer la calidad y eficiencia de los servicios. Por tanto, es esencial encontrar un equilibrio entre la ciberseguridad y la usabilidad, para garantizar la seguridad y privacidad de los pacientes sin comprometer la calidad y eficiencia de los servicios sanitarios.

En este subapartado se lleva a cabo un análisis ético-social de la ciberseguridad en el sector sanitario apoyado en las conclusiones del artículo *[15],* para conocer la relación existente entre los principios de la ética médica con la desiderata resultante de la implementación de las TIC y las funcionalidades clave de la ciberseguridad en el entorno de estudio. Con ello, se pretende comprender los desafíos éticos y sociales que surgen de la implementación de medidas de ciberseguridad en la asistencia sanitaria.

Los principios de la ética médica son cuatro, se definen a continuación y se relacionan con la desiderata de la implementación de las TIC y las funcionalidades de la ciberseguridad en el entorno de estudio como se muestra en la Ilustración 12.

- **Beneficencia**, entendido como la manera de actuar en beneficio del paciente.
- **No maleficencia**, o no hacer daño al paciente y velar por su salud.
- **Autonomía,** se trata del derecho del paciente a la toma de decisiones sobre su salud previamente informadas.
- **Justicia**, entendido como el trato equitativo e imparcial del médico hacia los pacientes.

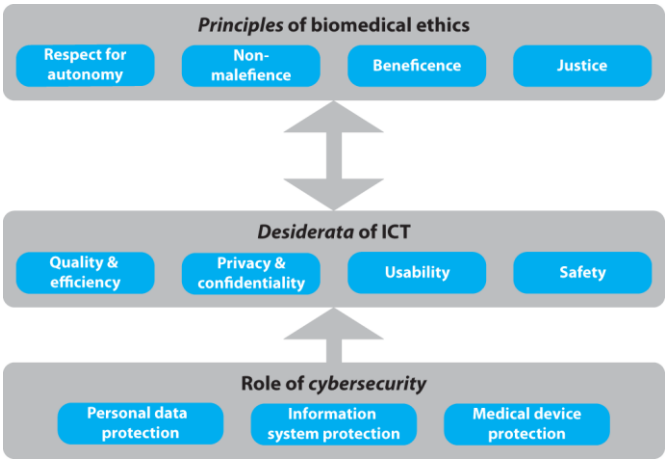

Ilustración 12. Esquema de la relación entre los principios de la ética médica con la desiderata resultante de la implementación de las TIC y las funcionalidades de la ciberseguridad en el entorno sanitario.[15]

En primer lugar, la beneficencia implica mejorar la calidad y eficiencia de los servicios de atención médica que se ofrecen a los pacientes. Para ello, es fundamental la implementación de las TIC, que permiten optimizar los procesos y recursos sanitarios.

En el sentido de la no maleficencia, la protección de la confidencialidad y seguridad de los pacientes es importante ya que el principio garantiza que los datos del paciente no sean compartidos con terceros no autorizados, pues de lo contrario el individuo podría ser sujeto de chantaje.

En términos de autonomía, la mejora de la usabilidad de los sistemas y dispositivos TIC puede ayudar a los pacientes a tomar decisiones informadas y controlar su atención médica. Para este principio, la protección de la confidencialidad y seguridad de los pacientes también es importante ya que garantiza que los pacientes tendrán control sobre la divulgación de su información médica.

Por último, la justicia está relacionada sobre todo con la usabilidad, pero también con la no maleficencia y la autonomía. El diseño de los sistemas tecnológicos puede aumentar la autonomía de los usuarios con conocimiento de la salud y buen manejo de la tecnología, pero reducir la de aquellos con menos habilidades tecnológicas, como las personas de edad avanzada. Además, una mala usabilidad también puede comprometer la seguridad; por ejemplo, la información de un implante médico puede ser más difícil de recuperar en situaciones de emergencia.

Por lo que se hace necesario garantizar que los beneficios de la ciberseguridad sean equitativamente distribuidos para todos los usuarios del sector sanitario. Sin

embargo, existen conflictos entre los cuatro principios de la ética médica en función del diseño del sistema sanitario.

Por un lado, si se prioriza la beneficencia y el diseño del sistema se hace más complejo pero altamente interconectado, evidentemente se mejora la calidad y eficiencia de los servicios. No obstante, se reduce la usabilidad además de generar mayor exposición de la información confidencial a los atacantes, afectando a la privacidad de los usuarios y por tanto, al principio de no maleficencia.

Por otro lado, si se da preferencia al principio de autonomía y no maleficencia, en el diseño se minimiza el intercambio de datos y la comunicación y creación de redes, velando así por la privacidad y seguridad de los usuarios. En cambio, se sacrifica la calidad y eficacia de los servicios, ya que se evita la monitorización inalámbrica.

Finalmente, si se prioriza el principio de la justicia, el diseño se conforma por un sistema uniforme de autentificación sencillo con una única configuración de privacidad. Lo que lo hace adecuado para todo tipo de usuarios, otorgándoles una mayor usabilidad y autonomía. Aunque, en este diseño, la no maleficencia se ve afectada ya que la seguridad de la información y por tanto, la del paciente, está en riesgo debido a una autentificación débil. También sacrifica la beneficencia porque reduce el nivel de calidad y eficiencia de los servicios.

Los sistemas del mundo real no presentan casos tan extremos ya que los diseñadores intentan acomodar parcialmente todos los principios. No obstante, es evidente que equilibrar los cuatro principios de la ética biomédica es una tarea difícil, lo que dificulta la minimización de los efectos sociales producidos por los incidentes cibernéticos en el sector sanitario.

Regulación española de la ciberseguridad en entornos hospitalarios

La ciberseguridad es un aspecto fundamental para garantizar la protección de los datos personales y la confidencialidad de la información sanitaria. En este sentido, se ha establecido un marco normativo nacional para cumplir con el RGPD y así regular la ciberseguridad en el área de la salud.

En este apartado, se aborda la importancia del cumplimiento y sanción del RGPD así como la necesidad de realizar auditorías de ciberseguridad en el ámbito de la industria médica, en relación con el propósito de adoptar medidas preventivas, reactivas y correctivas en materia de ciberseguridad en el sector sanitario. Además, se han clasificado según su finalidad y se han descrito algunas de las leyes más relevantes que afectan al sector de estudio atendiendo al Código de Derecho de la Ciberseguridad de 2023. *[16]*

El sector sanitario es uno de los que maneja una mayor cantidad y sensibilidad de datos personales, que requieren una especial protección para garantizar el derecho fundamental de las personas físicas a la privacidad y de la seguridad de su información. Por ello, el cumplimiento del RGPD es una obligación legal y ética para los responsables y encargados del tratamiento de datos sanitarios en España, que deben aplicar medidas técnicas y organizativas adecuadas para asegurar que el tratamiento es conforme con el reglamento y con los principios de responsabilidad proactiva, protección de datos desde el diseño y por defecto, transparencia e información, y garantía de los derechos de los interesados. *[17]*

Asimismo, el cumplimiento del RGPD implica la adopción de medidas preventivas, reactivas y correctivas en materia de ciberseguridad, pues incluye:

- **Finalidad preventiva**. La imposición de nuevas medidas de seguridad para las empresas, autónomos y administraciones públicas que tratan datos personales.

- **Finalidad reactiva**. La imposición a los responsables y encargados del tratamiento de datos personales el deber de notificar a la autoridad de control competente y a los interesados las violaciones de seguridad que pueden suponer un riesgo para los derechos y libertades de las personas; así como el deber de adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. *[18]*

- **Finalidad correctiva**. La imposición de multas administrativas de hasta 20 millones de euros o el 4% del volumen de negocio anual global para las infracciones graves relacionadas con la protección de datos personales. *[19]*

El marco normativo español, que regula la ciberseguridad del sector sanitario, está compuesto por diversas leyes que establecen medidas para garantizar la seguridad de los sistemas de información y las redes de comunicación que se utilizan en el ámbito sanitario. Como se ha mencionado, estas medidas pueden tener una finalidad preventiva, reactiva o correctiva según busquen evitar, responder o reparar los incidentes cibernéticos que puedan afectar a la protección de los datos o la continuidad del servicio sanitario. A continuación se presentan clasificadas algunas de las leyes más relevantes para la ciberseguridad del sector en la siguiente tabla:

Finalidad	Ley	Descripción	Artículos clave
Preventiva	La Ley 41/2002 de 14 de noviembre.*[20]*	Se regula la autonomía del paciente, así como los derechos y obligaciones en materia de información y documentación clínica.	- Art.18. Protección de datos clínicos y sus respectivas garantías.
	El Real Decreto 3/2010, de 8 de enero.*[21]*	Se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.	- Art.13. Análisis y gestión de riesgos. - Art.10.Asignación de responsabilidades. - Art.25. Seguridad operativa. - Art.21. Seguridad lógica.
	La Ley 36/2015 de Seguridad Nacional.*[22]*	Regula los principios y organismos clave para la defensa de seguridad nacional, incluyendo la ciberseguridad.	- Art.25. Regulación del CNPIC. - Art.22. Gestión de crisis en el marco del DSN.
Reactiva	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.*[23]*	Se tipifican como delitos informáticos el acceso ilícito a sistemas o datos, el daño o sabotaje informático, la interceptación ilegal de comunicaciones, la falsedad informática o el uso fraudulento de dispositivos o programas informáticos.	- Art.197. Delito de descubrimiento y revelación de secretos. - Art.197 bis. Delito de facilitación ilegítima de dispositivos y programas informáticos. - Art.264. Delito de daños informáticos.
	El Real Decreto 12/2018, del 7 de septiembre.*[24]*	Se establecen las obligaciones de los operadores de servicios esenciales y los proveedores de servicios digitales en materia de gestión del riesgo, notificación de incidentes y cooperación con las autoridades competentes.	- Art. 18-27. Notificación de incidentes de seguridad. - Art.14. Colaboración entre las autoridades competentes y los CSIRT. - Art.30-35. Penalización por infracciones cometidas por los operadores de servicios esenciales y los proveedores de servicios digitales.
	La Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.*[25]*	Se establecen las infracciones y sanciones por conductas que atenten contra la seguridad ciudadana, como aquellas que afecten al funcionamiento o disponibilidad de infraestructuras críticas o servicios esenciales para la comunidad.	- Art.36. Penalización por infracción grave. - Art.37. Penalización por infracción leve.
Correctiva	La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.*[26]*	Se establecen las medidas correctoras que puede imponer la Agencia Española de Protección de Datos (AEPD) a los infractores en materia de protección de datos.	- Art.69. Imposición de advertencias, requerimientos, órdenes o limitaciones del tratamiento. - Art.76. Imposición de multas o inhabilitaciones.

Tabla 1. Clasificación de algunas de las leyes que regulan la ciberseguridad en el sector sanitario en función de su finalidad, destacando algunos de sus artículos clave.

Para llevar a cabo los procesos de evaluación y verificación del nivel de seguridad de los sistemas de información y las redes de comunicación de las organizaciones sanitarias, se realizan auditorias.

Las auditorías de ciberseguridad dedicadas al sector sanitario siguen las normas y estándares nacionales e internacionales aplicables, así como las recomendaciones y buenas prácticas del sector para identificar las vulnerabilidades, los riesgos y las medidas de mejora necesarias. De esta forma, se garantiza la protección de los datos y la continuidad del servicio sanitario, así como el cumplimiento del marco normativo español. Por ello, las auditorias también se basan en establecer medidas preventivas, reactivas y correctivas:

- **Finalidad preventiva**. Las auditorias permiten detectar y prevenir posibles incidentes o ataques cibernéticos que puedan afectar a la seguridad de los datos o servicios sanitarios, así como establecer planes de contingencia y protocolos de actuación ante posibles escenarios de crisis.

- **Finalidad reactiva**. Las auditorias responden y gestionan adecuadamente los incidentes o ataques cibernéticos que se produzcan, minimizando su impacto y restableciendo la normalidad lo antes posible, así como notificar y cooperar con las autoridades competentes y los equipos CERT según lo establecido en el marco normativo.

- **Finalidad correctiva**. Las auditorias analizan y evalúan las causas y consecuencias de los incidentes o ataques cibernéticos, así como implementar las acciones o mejoras necesarias para evitar que se repitan en el futuro, cumpliendo con las medidas correctoras o sanciones que pueda imponer la autoridad de control competente según lo establecido en el marco normativo.

Algunas de las empresas de mayor relevancia en España que realizan auditorías de ciberseguridad para el sector sanitario son Igaleno, Hiscox y Deloitte.

La protección de datos es un derecho fundamental que afecta a todos los sectores, pero especialmente al sanitario, donde se tratan datos sensibles de la salud de las personas. Por tanto, el cumplimiento del RGPD es imprescindible para garantizar la confidencialidad, la seguridad y los derechos de los pacientes y los profesionales sanitarios. Además, su cumplimiento también contribuye a mejorar el nivel de seguridad y confianza en el ámbito sanitario digital, así como a prevenir y mitigar los riesgos y amenazas que puedan afectar a la continuidad o calidad del servicio prestado.

Por lo tanto, se hace imprescindible realizar auditorías periódicas que permitan evaluar el nivel de cumplimiento y detectar posibles riesgos o incumplimientos que puedan derivar en sanciones o brechas de seguridad, pues las auditorías de protección de datos en el sector sanitario son una herramienta eficaz para mejorar la ciberseguridad y la confianza de los usuarios, así como para adaptarse a las exigencias legales y éticas que rigen el ámbito de estudio.

Riesgos de ciberseguridad en entornos hospitalarios

La pandemia de la COVID-19 ha impulsado la transformación digital del sector sanitario, que ha tenido que responder a las nuevas necesidades y expectativas de pacientes y profesionales. Esta evolución ha supuesto una mejora para el diagnóstico y tratamiento de enfermedades, gracias al uso de tecnologías como la IA, el Big Data o la telemedicina, que aportan mayor precisión, rapidez y personalización. Asimismo, se ha mejorado la asistencia sanitaria, al ofrecerse canales más flexibles, accesibles y eficientes para la comunicación y la gestión clínica.

No obstante, la interconexión de los sistemas y dispositivos médicos los hace más vulnerables a las ciberamenazas, comprometiendo la integridad y confidencialidad de la información. Además, los datos médicos son un objetivo atractivo para los ciberdelincuentes debido a su alto valor en el mercado negro y la posibilidad de utilizarlos para fines ilícitos como el fraude, el chantaje o la extorsión. Por ello, la garantía de la ciberseguridad en el sector sanitario requiere una base técnica sólida, respaldada por criterios éticos y legales.

El objetivo de este apartado es comprender el funcionamiento del ciberespacio hospitalario propuesto en el capítulo Cyber Security in Healthcare Systems procedente del libro Cyber Security *[27]*, con el fin de entender su funcionamiento y sus implicaciones para la seguridad de los sistemas sanitarios. Asimismo, se hará una tipología de las amenazas cibernéticas según las vulnerabilidades y se describirán los vectores de ataque más relevantes en el sector de estudio. Para ello, se ha de comprender que amenaza, vulnerabilidad y riesgo forman un todo entrelazado en el mundo cibernético. En primer lugar, existe un objeto físico valioso, una competencia o algún otro derecho inmaterial que necesita protección y salvaguarda. En segundo, se identifica:

- **Amenaza**, como un acontecimiento cibernético perjudicial que puede ocurrir y su valor numérico representa su grado de probabilidad.

- **Vulnerabilidad**, como la debilidad inherente al sistema o dispositivo, que aumenta la probabilidad de que se produzca o agrave el acontecimiento. Puede estar relacionada con las actividades humanas, los procesos o las tecnologías.

- **Riesgo**, como el valor del daño esperado y es igual a la probabilidad multiplicada por la pérdida. Puede evaluarse en función de sus consecuencias económicas o de su pérdida.

Finalmente, se entiende por vector de ataque la vía que utiliza un atacante para acceder de forma no autorizada a una infraestructura de información para ejecutar una acción o un resultado malicioso. Con ello, los atacantes aprovechan las vulnerabilidades del sistema o dispositivo para llevar a cabo el incidente cibernético.

4.1. El ciberespacio Hospitalario

El ciberespacio hospitalario es un entorno complejo que se compone de varias capas que interactúan entre sí. En el Esquema 7 se muestra el desglosamiento de cada nivel.

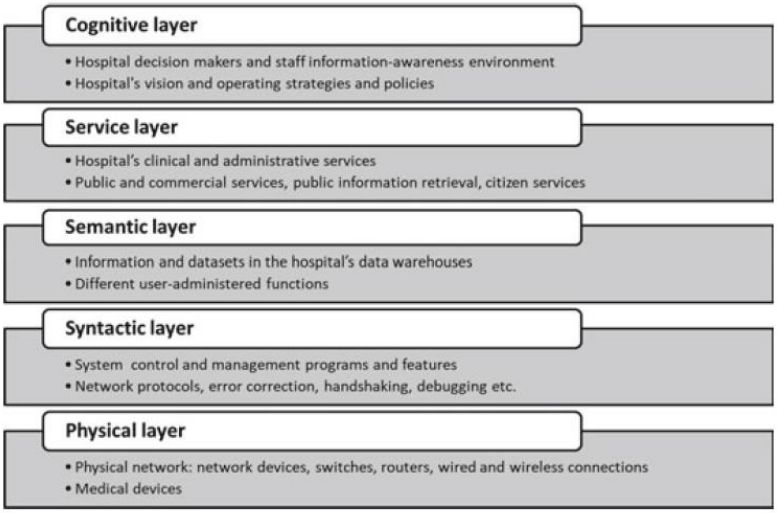

Ilustración 13. Capas del cibermundo en perspectiva hospitalaria. [27]

En la capa más externa o capa física, se encuentra la red de internet que conecta al hospital con el mundo exterior. La siguiente capa o la capa sintáctica, corresponde a la de la red interna del hospital, que conecta todos los dispositivos y sistemas del hospital. La siguiente capa o capa semántica es la del sistema de información hospitalaria, en la que se gestiona toda la información clínica y administrativa del hospital. La siguiente capa corresponde a los servicios públicos

y comerciales y la capa cognitiva es el entorno de conciencia del personal del hospital.

Es importante entender que el sistema de información sanitaria (HIS) se compone a su vez de varios procesos interconectados que se encargan de recopilar, almacenar y procesar la historia clínica electrónica (HCE). Además, también se ha de tener en cuenta que una persona genera alrededor de 1100 terabytes de datos sanitarios, 6 terabytes de datos genómicos y 0,4 terabytes de datos clínicos a lo largo de su vida.

Los datos clínicos se encuentran dispersos, lo que dificulta su análisis e intercambio, especialmente considerando el ciclo de vida que sigue este tipo de dato desde su generación hasta su eliminación.

El dato clínico se captura mediante una interfaz de usuario que permite al profesional de la salud introducir la información relevante sobre el paciente. Luego, el dato clínico se valida y codifica según los estándares y normativas vigentes. Después, el dato clínico se transmite a través de la red segura y cifrada a un sistema de gestión de bases de datos, donde se almacena en la base de datos EMR/EHR, que mantiene el historial del paciente y se organiza en registros. Finalmente, el dato se puede consultar y analizar mediante herramientas de visualización y minería de datos que permite extraer conocimiento e insights para mejorar la calidad asistencial y la toma de decisiones.

Ilustración 14. Ciclo de vida de un dato clínico.

Los dispositivos médicos son otro conjunto crítico del ciberespacio hospitalario. Estos dispositivos están conectados a la red interna del hospital y se utilizan para monitorizar a los pacientes y realizar pruebas médicas. Sin embargo, también pueden ser vulnerables a ciberataques, lo que podría tener consecuencias graves, como la manipulación de los resultados de las pruebas médicas o la alteración de los dispositivos médicos implantables. Además, un dispositivo infectado con malware tiene el potencial, en el peor de los casos, de paralizar las operaciones del hospital, exponer información sensible de los pacientes, comprometer el funcionamiento de otros dispositivos y dañar a los pacientes.

4.2. Vulnerabilidades en el sector sanitario

Las vulnerabilidades en el sector de estudio son una preocupación que cada vez está cobrando mayor relevancia en la seguridad cibernética debido a la creciente dependencia de la conexión entre los dispositivos y sistemas, así como el surgimiento de vectores de ataque cada vez más sofisticados. En el ciberentorno hospitalario las vulnerabilidades pueden surgir en cualquiera de las 5 capas y un error en una de ellas puede afectar directamente al resto. Por lo que es fundamental que se implementen medidas de seguridad en cada una de estas capas. La Ilustración 15 muestra las principales vulnerabilidades que presentan las distintas capas del entorno cibernético hospitalario.

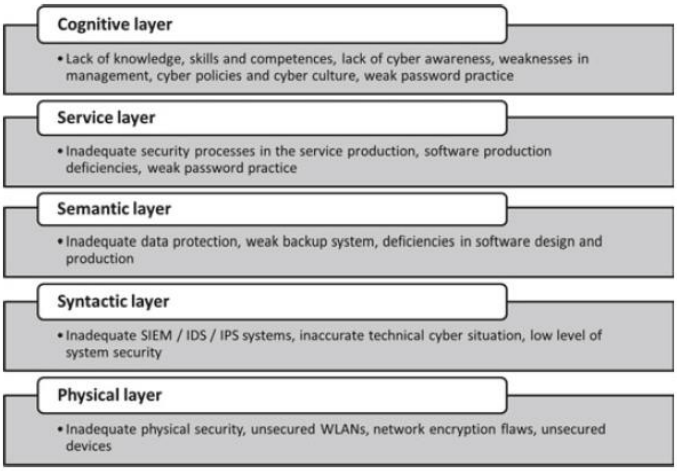

Ilustración 15. Vulnerabilidades en el ciberentorno hospitalario.[27]

En la capa física, las vulnerabilidades están relacionadas con fallos de cifrado de la red y dispositivos inseguros. Las vulnerabilidades de la capa sintáctica se asocian a un nivel bajo de seguridad del sistema o una situación cibernética técnica imprecisa. Las vulnerabilidades de la capa semántica se corresponden con un sistema de copias de seguridad deficiente y una protección de datos inadecuada. Entre las vulnerabilidades de servicio, se encuentra la práctica de contraseñas débiles y en la capa cognitiva, las vulnerabilidades generalmente se producen por falta de conocimiento, concienciación, ciberpolíticas y cibercultura.

Las vulnerabilidades a las que se presenta el sector sanitario durante la recopilación, almacenamiento y procesamiento de la historia clínica electrónica son diversas y pueden afectar a la calidad y la seguridad de la asistencia sanitaria.

Durante la generación del dato clínico, es importante garantizar que el dato sea veraz, completo y preciso, e identifique correctamente al paciente y al profesional

que lo genera. También es necesario asegurar que el dato se registre en el sistema de información adecuado y que se cumplan los requisitos legales y éticos sobre el consentimiento informado y la protección de datos personales.

Cuando se transmite la información, es fundamental utilizar canales seguros y cifrados que eviten la interceptación, la alteración o la pérdida de los datos durante su envío. También es imprescindible verificar la identidad y la autorización de los emisores y receptores de los datos, así como respetar el principio de minimización de datos; es decir, enviar solo los datos estrictamente necesarios para el fin previsto.

En el almacenamiento, es clave proteger los soportes del propio almacenamiento frente a posibles daños, robos o accesos no autorizados, mediante medidas técnicas (como copias de seguridad, antivirus o cortafuegos) y organizativas (como políticas de seguridad, control de accesos o auditorías). También es vital cumplir con las normativas vigentes sobre el plazo y el modo de conservación y eliminación de los datos.

Finalmente, cuando el dato se usa ya sea para fines asistenciales, administrativos, docentes o de investigación, es esencial garantizar que el dato sea accesible y comprensible para los usuarios autorizados, y que se respete el derecho del paciente a la información, a la rectificación y a la oposición sobre sus datos. También es necesario asegurar que el uso del dato se ajuste a los fines para los que fue recabado y que se cumplan las obligaciones de confidencialidad y secreto profesional.

Por otro lado, los dispositivos médicos son potencialmente vulnerables y fáciles de explotar, por lo que los ciberataques son posibles y factibles. La finalidad de estos ataques puede ser desde la intención de dañar a un paciente concreto, pasando por un ataque a un proveedor sanitario específico (cibervandalismo, delincuencia) hasta un ataque al sistema sanitario en su conjunto (ciberterrorismo, sabotaje), o una operación militar de apoyo a un ataque convencional o biológico. Se trata de situaciones graves. Además, como ya se ha mencionado, los dispositivos médicos se presentan cada vez más susceptibles debido a la adopción del Internet de las Cosas (IoT).

Una de las principales vulnerabilidades es la distribución incontrolada de contraseñas, que permite que cualquier persona pueda acceder a los sistemas sin la debida autorización. Asimismo, la falta de actualización y parches de software de seguridad para los servicios médicos, dispositivos y redes los hace susceptibles a ataques externos. Los puertos mal configurados o abiertos también son un riesgo,

ya que pueden ser utilizados por ciberdelincuentes para acceder a los dispositivos médicos. Asimismo, la falta de cifrado y autentificación en los dispositivos médicos puede permitir que personas no autorizadas accedan a la información del paciente, lo que pone en peligro la privacidad y la integridad de los datos clínicos, así como la vida del paciente.

4.3. Vectores de ataque en el sector sanitario

Un atacante emplea los vectores de ataque para acceder ilícitamente a un sistema de información y obtener datos confidenciales, generalmente con fines económicos. Para ello, explota una vulnerabilidad en la red, el sistema o en algún dispositivo médico. Estas amenazas suponen un riesgo para el sector sanitario tales como la pérdida de confianza en el centro, el incumplimiento de la normativa de protección de datos, el aumento de los costes operativos y la disminución de la calidad asistencial.

En la Tabla 2 se muestra la relación entre los vectores de ataque y las vulnerabilidades anteriormente mencionadas. Además, se detalla el método de infección y propagación que llevan a cabo cada uno de los vectores seleccionados, así como su objetivo. Por último, también se especifica a qué capas del ciberentorno hospitalario afecta la explotación de cada conjunto de vulnerabilidades.

Vector de ataque	Método de infección y propagación	Objetivo	Vulnerabilidades	Capa del ciberentorno hospitalario
Denegación de Servicios (DoS)	Ataque mediante el envío de un gran número de solicitudes a un servidor para sobrecargarlo y evitar que responda a solicitudes legítimas	El atacante busca agotar los recursos del servidor para hacerlo inoperable. Ejemplo: Ataque DDoS	- Fallos de cifrado y autentificación. - Dispositivos inseguros - Falta de actualización del sistema - Puertos mal configurados o abiertos	Física, Sintáctica y Semántica
Software malicioso	Infección de un sistema a través de correos electrónicos, sitios web resistentes, dispositivos USB o descargas de software malicioso	El atacante busca dañar el sistema o recopilar información confidencial de usuario. Ejemplo: Ransomware	- Falta de actualización del sistema - Dispositivos inseguros - Situación cibernética técnica imprecisa - Sistema de copias de seguridad deficiente - Protección de datos inadecuada - Práctica de contraseñas débiles	Física, Sintáctica, Semántica y de Servicio
Ingeniería social	El atacante manipula a los usuarios para obtener información confidencial como contraseñas o información de inicio de sesión	El atacante utiliza la confianza del usuario para obtener acceso a sistemas o información. Ejemplo: Phising	- Falta de conocimiento y concienciación - Ciberpolíticas	Cognitiva
Gusanos	El programa aprovecha las vulnerabilidades de seguridad en los sistemas. Se duplica a sí mismo y se propaga automáticamente sin la intervención del usuario	El atacante busca dañar los sistemas y recopilar información confidencial. Ejemplo: WannaCry	- Falta de actualización del sistema - Dispositivos inseguros - Puertos mal configurados o abiertos - Fallos de cifrado y autentificación.	Física, Sintáctica y Semántica
Hombre en el Medio (MITM)	El atacante intercepta la comunicación entre dos dispositivos para modificarla o monitorearla. Puede ser llevado a cabo mediante el uso de redes Wi-Fi públicas no seguras o el uso de malware	El atacante puede obtener información confidencial o modificar los datos transmitiditos. Ejemplo: modificación de dosis de un medicamento interceptando la comunicación entre médico y paciente	- Fallos de cifrado o autentificación - Falta de actualización del sistema - Puertos mal configurados o abiertos - Práctica de contraseñas débiles - Falta de conocimiento y concienciación	Física, Sintáctica, Semántica, de Servicio y Cognitiva
Ataque criptográfico	El atacante explota las debilidades en los algoritmos de cifrado o en la gestión de claves para acceder a datos cifrados. Puede ser llevado a cabo mediante el uso de fuerza bruta o la explotación de debilidades en el algoritmo de activación.	El atacante puede descifrar datos grabados y obtener información confidencial. Ejemplo: acceso a registros médicos de un paciente bloqueado	- Fallos de cifrado y autentificación - Dispositivos inseguros - Falta de actualización del sistema - Práctica de contraseñas débiles	Física, Sintáctica, Semántica y de Servicio

Tabla 2. Clasificación de los vectores de ataque más comunes en el sector sanitario en función de las vulnerabilidades que extorsionan y la capa del ciberentorno que afectan.

4.4. Prevención de riesgos

La prevención y mitigación de los riesgos de los vectores de ataque en el sector hospitalario es un tema crítico que requiere una atención exhaustiva. Por ello, es necesario adoptar un enfoque proactivo en materia de ciberseguridad, que se anticipe a las posibles vulnerabilidades y amenazas para evitar o mitigar los incidentes cibernéticos.

Las actividades de ciberseguridad de muchas organizaciones siguen caracterizándose por un enfoque reactivo, y los hospitales no son una excepción. Un enfoque reactivo significa que, en caso de ciberataque, las conclusiones y las medidas son rápidas y urgentes.

Las medidas preventivas son más eficaces y rentables que las medidas reactivas ya que contribuyen a mejorar la calidad y la eficiencia de la atención sanitaria, así como a garantizar el cumplimiento de la normativa vigente en materia de protección de datos personales.

Cada una de las capas del ciberentorno hospitalario presenta sus propios riesgos y vulnerabilidades. Al mejorar la seguridad de cada una de estas capas, se contribuye a reducir significativamente las posibilidades de sufrir ciberataques y a minimizar sus impactos potenciales. Para lograrlo, se ha de tratar cada una de las capas de forma específica según sus características y necesidades.

En la Ilustración 15 se evidencia la necesidad de implementar una estrategia holística que garantice la confidencialidad, integridad y disponibilidad de los datos. Una estrategia holística en ciberseguridad implica tener en cuenta todos los factores que pueden afectar a la seguridad de los datos y las infraestructuras sanitarias, desde el diseño y la implementación de las soluciones tecnológicas hasta la formación y la concienciación de los usuarios y el personal sanitario. Esta clase de estrategia también supone adoptar un enfoque preventivo y proactivo, que permita anticiparse y responder a las amenazas emergentes, así como evaluar y mejorar continuamente las medidas de seguridad existentes.

A continuación se presentan una serie de tablas donde se exponen recomendaciones de acciones preventivas para cada una de las capas que conforman el ciberentorno hospitalario, así como ejemplos prácticos que evidencian la factibilidad de su implementación.

CAPA FÍSICA	
MEDIDAS PREVENTIVAS	**PUESTA EN PRÁCTICA**
Controlar el acceso a los dispositivos médicos, las redes de comunicación y los sistemas informáticos.	– Autentificación mediante tokens de seguridad o biometría. – Control de acceso basado en roles (RBAC). – Registros de auditoría.
Asegurar el cifrado y la autentificación de los datos transmitidos.	– Certificados SSL/TLS. – Autentificación de dos factores (2FA). – Parches de seguridad.
Disponer de sistemas de respaldo y recuperación ante posibles incidentes.	– Copias de seguridad regulares en servidores remotos o en la nube. – Plan de recuperación ante desastres. – Servidores redundantes. – Almacenamiento en espejo.

Tabla 3. Medidas de prevención y ejemplos prácticos para la capa física del ciberentorno hospitalario.

CAPA SINTÁCTICA	
MEDIDAS PREVENTIVAS	**PUESTA EN PRÁCTICA**
Utilizar software y protocolos seguros para la interacción entre los dispositivos conectados a la red.	– Protocolo HTTPS. – Protocolo WPA2. – Protocolo VPN.
Evitar el uso de contraseñas por defecto o codificadas.	– Cambio de contraseña cada 30 días. – Política de gestión de contraseñas. – Herramienta LastPass.
Monitorizar y auditar las actividades y eventos en la red.	– Sistemas de administración de información y eventos de seguridad (SIEM).
Detectar y bloquear posibles intrusiones o ataques.	– Herramienta Snort. – Herramienta Suricata. – Herramienta OSSEC.

Tabla 4. Medidas de prevención y ejemplos prácticos para la capa sintáctica del ciberentorno hospitalario

CAPA SEMÁNTICA	
MEDIDAS PREVENTIVAS	**PUESTA EN PRÁCTICA**
Gestionar adecuadamente los datos e información clínica almacenados en los sistemas informáticos.	– Estándar HL7. – Herramienta ETL.
Garantizar el cumplimiento de las normas de protección de datos personales y sanitarios.	– Auditorías internas. – Escáneres de huellas dactilares para el control de acceso.
Limitar el acceso y la divulgación no autorizados a la información sensible.	– Software VeraCript. – Unidades flash USB encriptadas.

Tabla 5. Medidas de prevención y ejemplos prácticos para la capa semántica del ciberentorno hospitalario

CAPA DE SERVICIOS	
MEDIDAS PREVENTIVAS	**PUESTA EN PRÁCTICA**
Seleccionar y contratar servicios públicos o comerciales en línea que ofrezcan garantías de seguridad.	– Centro Criptológico Nacional (CCN). – Instituto Nacional de Ciberguridad (INCIBE). – CyberMDX.
Establecer acuerdos y protocolos claros con los proveedores de servicios, así como evaluar y supervisar el rendimiento y la calidad de los servicios contratados.	– Cláusula sobre la realización de auditorías regulares. – Cláusula sobre la notificación de violaciones de seguridad.

Tabla 6. Medidas de prevención y ejemplos prácticos para la capa de servicios del ciberentorno hospitalario.

CAPA COGNITIVA	
MEDIDAS PREVENTIVAS	**PUESTA EN PRÁCTICA**
Fomentar una cultura de seguridad entre el personal sanitario, que implique una actitud proactiva, responsable y colaborativa frente a los riesgos cibernéticos.	– Talleres de formación continua y actualizada sobre ciberseguridad.
Reconocer y premiar las buenas prácticas y los logros en materia de ciberseguridad para incentivar la implicación del personal.	– CISSP (Certified Information Systems Security Professional).

Tabla 7. Medidas de prevención y ejemplos prácticos para la capa cognitiva del ciberentorno hospitalario.

El sector sanitario se enfrenta a retos específicos en materia de ciberseguridad, derivados de la gestión de datos sensibles de los pacientes, la interoperabilidad de los sistemas de información, la digitalización de los procesos asistenciales o la incorporación de dispositivos médicos conectados. Estos factores aumentan la exposición a ciberamenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información y los servicios sanitarios, así como la seguridad de los pacientes.

Por ello, es necesario establecer una estrategia holística en materia de ciberseguridad que ponga en marcha las medidas proactivas y preventivas en el conjunto de capas del ciberentorno hospitalario. Esta estrategia debe implicar a todos los actores del sector, desde los fabricantes de dispositivos y sistemas hasta los proveedores y usuarios de servicios sanitarios, así como a las autoridades reguladoras y supervisores. Solo así se podrá garantizar una sanidad digital segura y resiliente ante los desafíos del ciberespacio.

Presentación de los casos

En el presente apartado se expone la información recopilada cronológicamente sobre dos casos recientes de ciberataques en el sector sanitario: el caso del Hospital Clínic de Barcelona y el caso del Hospital universitario Saint-Pierre de Bruselas. Para el estudio del primer caso, se ha seleccionado información tanto de la página oficial del hospital como del periódico El País, mientras que para el segundo caso, se ha utilizado como fuente el periódico Le Soir.

La exposición cronológica de los casos permitirá comprender con mayor claridad los eventos que desencadenaron los ciberataques, así como las diferentes medidas adoptadas por los hospitales para hacer frente a los incidentes y el resultado final que se obtuvo con el plan de respuesta de cada hospital.

5.1. Caso del Hospital Clínic

El domingo día 5 de marzo de 2023, a las 08.30 horas, el responsable de guardia del Hospital Clínic de Barcelona alarmó sobre una caída del sistema al no poder acceder al SAP. El sistema SAP se trata de uno de los principales softwares de Planificación de Recursos Empresariales (ERP) y permite digitalizar los procesos administrativos y de operaciones, con lo que se optimizan los costes y se facilita el escalado de la infraestructura tecnológica.*[28]*

Ante la imposibilidad de acceder al sistema, uno de los técnicos del hospital intentó introducir cinco contraseñas sin éxito. Por lo que, a las 11.17 horas, se notificó a la Agencia de Ciberseguridad de Cataluña (ACC) de que el Clínic había sufrido un ciberataque tipo Ransomware y a las 11.30 se inició el plan de actuación para dar respuesta al incidente.

Este tipo de ataque implica el bloqueo de las puertas de acceso a cada nivel de archivo de la información, así como la encriptación de los archivos, impidiendo su acceso. De esta manera, los ciberdelincuentes se aprovechan de la situación y exigen un rescate a cambio de liberarlos.

Para llevar a cabo el plan de contingencia, se desprogramaron cirugías, visitas y sesiones de radioterapia, aunque se mantuvo la hospitalización en las plantas y las urgencias, además del servicio de radiología, las pruebas endoscópicas y diálisis.*[29]* Sin embargo, el hospital se encontraba completamente incomunicado: no tenía acceso a la intranet, ni a la historia de los pacientes, ni a su teléfono ni a

su correo electrónico para poder informar sobre el estado de la atención médica.*[30]*

Fue entonces cuando el director del hospital se coordinó con los directores de los principales hospitales de Barcelona y el Sistema de Emergencias Médicas (SEM) para administrar el traslado de los pacientes más críticos que podían llegar al Clínic, como los de códigos ictus e infarto.*[30]* Mientras tanto, el personal médico y de enfermería tuvo que recurrir a procesos analógicos, como las órdenes y recetas en papel, para mantener la actividad asistencial.*[29]*

El lunes día 6 de marzo, la Generalitat en colaboración con la ACC y la dirección del centro iniciaron un trabajo conjunto con los Mossos y la Interpol para conocer el alcance del secuestro. Posteriormente, se verificó que el ciberataque provenía de fuera de España y que había afectado tanto a las tres sedes del hospital en Villarroel, Plató y Maternitat, como a tres centros de atención primaria en Barcelona: Casanova, Borrel y Les Corts.*[31]*

Como resultado, ese lunes se desprogramaron 150 intervenciones y se anularon entre 2.000 y 3.000 visitas y entre 300 y 400 analíticas. Sin embargo, a las 19.41 horas, los técnicos del centro sanitario lograron reactivar el acceso a una parte de los sistemas de información perjudicados. Gracias a ello, para el martes día 7 ya se realizaron el 10% de las consultas externas y el 40% de las cirugías programadas. *[32]*

Entre el día 9 y 10 de marzo el grupo de ciberdelincuentes conocido como RansomHouse se puso en contacto con el hospital para pedir el rescate por 4,5 millones de dólares (4,2 millones de euros) a cambio de los datos secuestrados. Se confirmó que eran los autores del crimen porque aportaron una copia de vida, que es una imagen del árbol principal del servidor donde aparecen todas las carpetas.*[33]* Sin embargo, las autoridades recomendaron no pagar el rescate por tres razones:

- No hay garantía de que los ciberdelincuentes devuelvan los datos o los borren después del pago y además pueden seguir exigiendo más dinero o publicarlos en la Dark web.
- Pagar el rescate fomenta el negocio de los ciberdelincuentes y los anima a seguir atacando a otras organizaciones sanitarias.

- Pagar el rescate puede suponer una infracción de la ley de protección de datos, ya que implica la transferencia de datos personales a terceros no autorizados.

Asimismo se consideraba que había una alta probabilidad de que los delincuentes publicaran los datos ante la negativa a pagar el rescate, ya que los Ransomware son ataques que presentan una doble extorsión. Primero se introduce un código malicioso que bloquea al acceso a los datos. Luego se pide un rescate para liberarlos y, si no se consigue, se realiza una segunda extorsión: se roban los datos y se amenaza con publicarlos o venderlos a terceros. *[33]*

A día 10 ya se había recuperado el 90% de la actividad quirúrgica compleja, el 40% de la actividad quirúrgica menos compleja, el 70% de las consultas externas y el código ictus e infarto. Además, el 15% de los servicios digitales ya estaban operativos.*[33]*

Tres semanas después, la situación seguía siendo crítica y el hospital todavía operaba sin acceso a internet y sin poder consultar los archivos de los servidores afectados. También se emitió un comunicado donde se informó que los datos de los pacientes y los trabajadores podían estar comprometidos.*[34]*

El 30 de marzo, se difundieron enlaces en Telegram que permitían la descarga de archivos con información identificativa y de salud de pacientes, de trabajadores y de proveedores. Esta información suponía entre tres y cuatro gigas de información de los cuatro terabytes y medio que habían sido sustraídos. Como consecuencia, el Clínic modificó la contraseña de 8.000 usuarios e implantó el sistema de la doble autentificación para reforzar la seguridad.*[35]* Como contraataque, el 5 de abril los Mossos lograron bloquear la web de los ciberdelincuentes en la red de TOR mediante un ataque de denegación de servicio distribuido (DDOS). *[36], [37]* Posteriormente, se enfocaron en localizar dónde se encontraban las bases de datos que habían sido publicadas en la Dark web.*[35]*

El 6 de abril, los ciberatacantes amenazaron con filtrar información personal de pacientes con enfermedades infecciosas y además incitaron a los usuarios del centro hospitalario a denunciar la pérdida de sus datos personales.*[38]*

Las últimas notificaciones que se tienen sobre el caso son los comunicados por parte del Hospital Clínic de la detección de nuevas filtraciones en la Dark web los días 17 y 27 de abril de varios datos de pacientes y profesionales y se ha emitido la tipología de los mismos el 21 de junio. *[37]*

5.2. Caso del Hospital Saint Pierre

La presentación del segundo caso de estudio se basa en la información expuesta en el artículo del periódico Le Soir,*[39]* ya que es el más completo de los que abordan el tema.

En la madrugada del viernes 10 de marzo, los informáticos del hospital universitario Saint-Pierre de Bruselas detectaron una actividad anormal en su red informática. Los servidores comenzaron a ralentizarse gravemente, lo que llevó a los técnicos a alertar sobre la probabilidad de un ciberataque a las 4 de la mañana.

Inmediatamente se puso en marcha el plan de emergencia específico para responder contra ciberataques, que se había estado elaborando durante los últimos 18 meses en previsión de posibles amenazas. Los servicios especializados de la Policía Federal y el Ministerio Fiscal se unieron al hospital para llevar a cabo el plan, que consistía básicamente en la desconexión de los servidores, el desvío de ambulancias a otros hospitales y la vuelta a la comunicación en papel dentro del hospital.

El funcionamiento de muchas aplicaciones se vio afectado, incluidos los historiales de los pacientes y las líneas telefónicas. Aunque los equipos de los quirófanos no se vieron perjudicados y en ningún momento hubo problema con la atención de los pacientes gracias a las soluciones provisionales del plan de contingencia.

A última hora de la tarde del sábado 11 de marzo, los informáticos lograron reiniciar los servidores, lo que permitió que el 100% de las aplicaciones informáticas volvieran a estar operativas.

Aunque se desconoce el origen y la finalidad del ciberataque, mientras los servidores informáticos permanecían aislados del mundo exterior y el acceso a Internet estaba desconectado, se comprobó que no había más virus y se verificó que no había ningún robo ni filtración de datos médicos.

El lunes 13 de marzo, todas las consultas y hospitalizaciones programadas se llevaron a cabo con normalidad, y el hospital reabrió su servicio de urgencias volviendo a estar operativo al 100%.

Tras exponer toda la información relevante sobre los casos de estudio, se procede a la presentación de un diagrama cronológico para adquirir una visión general de los hechos de manera más ordenada y precisa.

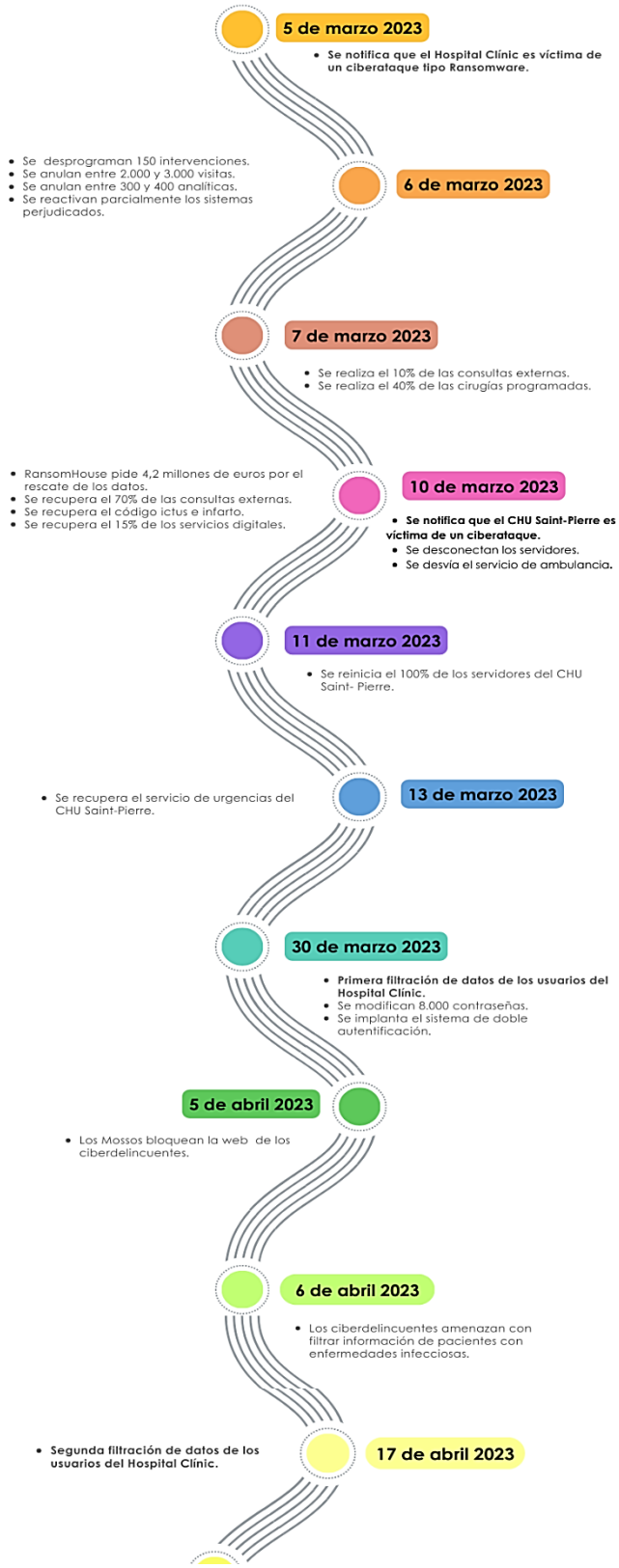

Ilustración 16. Línea del tiempo de los sucesos relacionados con los casos de los ciberataques al Hospital Clínic de Barcelona y al CHU Saint-Pierre de Bruselas.

Análisis de los casos de estudio

En este apartado se presentan los análisis de los casos de estudio seleccionados con el objetivo de identificar las buenas prácticas y las lecciones aprendidas en la gestión de incidentes de ciberseguridad en el ámbito sanitario. Para ello, se seguirá el siguiente esquema:

- En primer lugar, se explicará brevemente el procedimiento general de gestión de incidentes de ciberseguridad, basado en la Guía nacional de notificación y gestión de incidentes.*[40]* Para cada etapa del proceso, se plantearán una serie de preguntas que servirán como guía para realizar posteriormente un análisis más detallado de los casos de estudio.

- En segundo lugar, se llevará a cabo el análisis del ciberataque al Hospital Clínic de Barcelona mediante las cuestiones propuestas y además se apoyará en una entrevista realizada al jefe del departamento de informática médica del propio hospital.

- Por último, se hará una comparativa entre ambos casos de estudio, resaltando las similitudes y las diferencias en la gestión de los incidentes. Con ello, se pretenden extraer las recomendaciones y lecciones aprendidas para mejorar la seguridad informática en el sector sanitario.

6.1. Procedimiento de gestión de incidentes

La gestión de incidentes en ciberseguridad es el conjunto de actividades que se realizan para prevenir, detectar, contener, erradicar y recuperarse de los ataques informáticos que pueden afectar a la seguridad de la información de los pacientes y de los servicios sanitarios. El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea, como se aprecia en la Ilustración 17.

Ilustración 17. Fases de la gestión de un ciberincidente.[40]

1) **Preparación.** Consiste en establecer políticas, procedimientos, roles y recursos necesarios para gestionar los incidentes de forma eficaz y coordinada. Incluye la realización de análisis de riesgos, la actualización de las políticas y procedimientos relativos a la gestión y la actualización de contacto. También implica la formación y concienciación del personal sanitario sobre las buenas prácticas de ciberseguridad y el uso seguro de los dispositivos y sistemas informáticos. Las cuestiones que se proponen dentro de la primera fase son las siguientes:

    1. ¿Qué medidas preventivas se aplican para proteger los sistemas y datos clínicos?

    2. ¿Cuál es su política y plan de gestión de ciberincidentes y con qué frecuencia se revisa y se actualiza?

    3. ¿Cómo se forma y se evalúa al personal en materia de conocimientos y procedimientos de gestión de ciberincidentes?

2) **Identificación**. Consiste en detectar y analizar los posibles incidentes que se produzcan en el entorno sanitario, mediante el uso de herramientas de monitorización, alerta y auditoría. También implica la transmisión de información a otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección. Las preguntas propuestas para la segunda fase son las siguientes:

    4. ¿Qué herramientas o mecanismos se utilizan para la detección de posibles ciberincidentes en los sistemas?

    5. ¿Qué tipo de incidente se ha producido?

    6. ¿Qué nivel de peligrosidad e impacto tiene?

3) **Contención.** Consiste en aislar y limitar el alcance del incidente para evitar que se propague o cause más daños. Incluye la desconexión o bloqueo de los dispositivos o sistemas afectados, la preservación de las evidencias y la recolección de información situacional que permita detectar anomalías. Las preguntas propuestas para la tercera fase son las siguientes:

    7. ¿Qué medidas se han tomado para aislar y limitar el incidente?

    8. ¿Qué herramientas o procedimientos se han utilizado para recoger y almacenar las evidencias del incidente?

4) **Mitigación.** Consiste en eliminar o reducir las causas y los efectos del incidente. Incluye la identificación y aplicación de las soluciones técnicas disponibles para eliminar el malware, restaurar los sistemas o recuperar los datos. Las preguntas propuestas para la cuarta fase son las siguientes:

   9. ¿Qué soluciones técnicas se han aplicado para eliminar o reducir el incidente?

   10. ¿Qué herramientas o métodos se han utilizado para restablecer los sistemas y los datos afectado por el ciber incidente?

5) **Recuperación.** Consiste en restablecer el funcionamiento normal de los servicios sanitarios afectados por el incidente. Incluye la verificación y validación de los sistemas restaurados, la eliminación o sustitución de los dispositivos o componentes dañados y la reanudación gradual de las actividades.

   11. ¿Cómo se ha verificado y validado el funcionamiento de los servicios restaurados?

   12. ¿Se han sustituido o eliminado dispositivos o componentes del sistema?

   13. ¿Cómo se ha reanudado la actividad normal de los servicios sanitarios tras el ciberincidente?

6) **Actuaciones posts-incidentes.** Consiste en realizar un análisis detallado del incidente para extraer lecciones aprendidas y mejorar el proceso de gestión de incidentes. Incluye la elaboración y difusión de un informe final del incidente, con las acciones realizadas, los resultados obtenidos, las recomendaciones propuestas y las medidas adoptadas.

   14. ¿Qué vulnerabilidades o debilidades se han detectado en los sistemas o procesos del hospital que permitieron el incidente?

   15. ¿Qué lecciones aprendidas se han extraído?

   16. ¿Qué medidas correctivas adicionales se ha implementado o se tiene previsto implementar para prevenir o reducir el riesgo de que se repita un incidente similar?

6.2. Análisis del caso de estudio I

El ciberataque al Hospital Clínic se produjo en medio de un proceso de integración del hospital a la ACC, que había diseñado un plan específico para proteger el sistema sanitario catalán desde septiembre de 2021.*[38]* El ciberincidente alarmó y potenció la aceleración del proceso de integración.

Con lo que la ACC realizó una prueba de estrés al Hospital Clínic para evaluar su nivel de seguridad y detectar las posibles vulnerabilidades que facilitaron el ataque. El resultado fue que el hospital tenía escasos recursos para intervenir ante una amenaza cibernética y que una credencial débil permitió el acceso de los ciberdelincuentes al sistema informático.[38] Estos aprovecharon el fallo de seguridad para acusar al hospital de una mala gestión de los datos y animar a los usuarios a reclamar por ello.*[36]*

Para confirmar las fuentes de información y realizar un análisis más riguroso, se ha entrevistado al director del departamento de informática médica del hospital Xavier Pastor. La información recopilada se presenta a continuación en una serie de tablas que contienen las preguntas propuestas para cada una de las fases del procedimiento de gestión de incidentes en materia de ciberseguridad y sus respuestas correspondientes.

PREPARACIÓN	
PREGUNTAS	**RESPUESTAS**
¿Qué medidas preventivas se aplican para proteger los sistemas y datos clínicos?	• **Protección física:** – Modelo de sistemas centralizado y restringido con 2 centros de proceso de datos (CPD), uno de almacenamiento y otro que soporta las transacciones. – Sistemas de vigilancia. • **Protección informática:** – Antivirus corporativos. – Política de contraseñas autogestionada por el usuario. – Supresión de la entrada de datos periféricos.
¿Cuál es su política y plan de gestión de ciberincidentes y con qué frecuencia se revisa y se actualiza?	– Plan de contingencia para trabajar con regularidad el tiempo necesario para remontar el sistema. – Time out de usuario olvidado. – Cambios de contraseñas temporales. – Imposición de contraseñas robustas.
¿Cómo se forma y se evalúa al personal en materia de conocimientos y procedimientos de gestión de ciberincidentes?	– Manual sobre la normativa de buenas prácticas de seguridad a los nuevos usuarios. – Firma del contrato de confidencialidad.

Tabla 8. Preguntas y respuestas a la primera etapa del proceso de gestión del ciberincidente al Hospital Clínic.

IDENTIFICACIÓN	
PREGUNTAS	**RESPUESTAS**
¿Qué herramientas o mecanismos se utiliza para la detección de posibles ciberincidentes en los sistemas?	– Parametrización de las peticiones de usuario para el uso de aplicaciones. – Herramientas orientadas a contener ataques masivos.
¿Qué tipo de incidente se ha producido?	– Ciberataque tipo Ransomware, forzando la identificación de usuarios a través del sistema de escritorio de acceso virtual.
¿Qué nivel de peligrosidad e impacto tiene?	– Servicios y servidores orientados a la protección del paciente inoperativos. – Pausa de proyectos. – Filtración de documentación fragmentada de pacientes, personal y proveedores.

Tabla 9. Preguntas y respuestas a la segunda etapa del proceso de gestión del ciberincidente al Hospital Clínic.

CONTENCIÓN	
PREGUNTAS	**RESPUESTAS**
¿Qué medidas se han tomado para aislar y limitar el incidente?	– Cambio de 8000 contraseñas. – Sistema de doble autentificación.
¿Qué herramientas o procedimientos se han utilizado para recoger y almacenar las evidencias del incidente?	– Identificación y revisión de los sistemas afectados. – Seguimiento y priorización de los sistemas que había que remontar según grado de afectación o de impacto.

Tabla 10. Preguntas y respuestas a la tercera etapa del proceso de gestión del ciber incidente al Hospital Clínic.

MITIGACIÓN	
Preguntas	**Respuestas**
¿Qué soluciones técnicas se han aplicado para eliminar o reducir el incidente?	– Medidas más estrictas de robustez. – Actualización mensual de contraseñas.
¿Qué herramientas o métodos se han utilizado para restablecer los sistemas y los datos afectado por el ciber incidente?	– Esta cuestión no ha podido ser respondida ya que presenta un grado de complejidad técnica propio de un responsable en sistemas.

Tabla 11. Preguntas y respuestas a la cuarta etapa del proceso de gestión del ciber incidente al Hospital Clínic.

RECUPERACIÓN	
PREGUNTAS	**RESPUESTAS**
¿Cómo se ha verificado y validado el funcionamiento de los servicios restaurados?	• Protocolo de chequeo por parte de la ACC: – Aislamiento del servidor. – Comprobación de infección. – Comprobación del Sistema Operativo y de sus aplicaciones. – Aplicación de cambios de versiones. – Aplicación de parches de seguridad.
¿Se han sustituido o eliminado dispositivos o componentes del sistema?	– Servidores de hardware. – Software con SO que no cumplía con las condiciones de seguridad exigibles.
¿Cómo se ha reanudado la actividad normal de los servicios sanitarios tras el ciber incidente?	– Cambio de impresoras y ordenadores de red a locales. – Restricción de la Historia Clínica en cuanto a los periféricos. – Restricción de pruebas de laboratorio y de forma manual. – Desprogramación de intervenciones y derivación de pacientes agudos.

Tabla 12. Preguntas y respuestas a la quinta etapa del proceso de gestión del ciber incidente al Hospital Clínic.

ACTUACIONES POST-INCIDENTES	
PREGUNTAS	**RESPUESTAS**
¿Qué vulnerabilidades o debilidades se han detectado en los sistemas o procesos del hospital que permitieron el incidente?	– Revisión del plan de contingencia actualmente en proceso.
¿Qué lecciones aprendidas se han extraído?	– Potenciar la concienciación del personal en materia de ciberseguridad. – Acrecentar la inversión en la actualización de los sistemas, sobre todo en la dimensión de la seguridad.
¿Qué medidas correctivas adicionales se han implementado o se tiene previsto implementar para prevenir o reducir el riesgo de que se repita un incidente similar?	– Migración de la Historia Clínica a la nube. – Imposición a cualquier usuario informático del hospital de un curso obligatorio online sobre seguridad informática (en proceso).

Tabla 13. Preguntas y respuestas a la sexta etapa del proceso de gestión del ciberincidente al Hospital Clínic.

6.3. Comparativa de los casos de estudio

En esta última parte del apartado, se ha llevado a cabo una breve comparativa entre ambos casos de estudio. Lamentablemente y aunque se ha intentado conseguir información más detallada a nivel de gestión del caso del CHU Saint-Pierre, el análisis y la investigación siguen en curso, por lo que no han cedido a comunicar nada al respecto.

	Caso del Hospital Clínic	Caso del CHU Saint-Pierre
Preparación	– Plan de contingencia.	– Plan de emergencia específico frente a ciberataques.
Identificación	– Sin acceso al sistema SAP.	– Identificación de la disminución del rendimiento de los servidores.
Contención	– Desprogramación de visitas. – Traslado de pacientes. – Vuelta a la comunicación en papel. – Sistema de doble autentificación.	– Desconexión de los servidores. – Desvío de ambulancias. – Vuelta a la comunicación en papel.
Mitigación	– Actualización frecuente de contraseñas más robustas.	– No hay información.
Recuperación	– Protocolo de chequeo de los sistemas afectados.	– Verificación de la ausencia de intrusiones o infecciones maliciosas.
Actuaciones post-incidentes	– Migración de la Historia Clínica a la nube.	– Investigación en curso.

Tabla 14. Comparativa de los casos de estudio en función de las fases de gestión de incidentes.

En la comparativa se hace evidente la importancia de disponer de un plan de respuesta y contingencia adecuado para hacer frente a este tipo de incidentes. En ambos centros sanitarios se produjeron incidentes cibernéticos pero el impacto y la respuesta fueron diferentes en cada caso. El Hospital Clínic de Barcelona tuvo que desprogramar visitas y cirugías y derivar a otros hospitales las urgencias más graves, mientras que el CHU Saint-Pierre pudo mantener la actividad asistencial normal aunque con alguna dificultad pero durante poco tiempo.

El plan de respuesta en ambos centros fue similar, basado en la activación de un protocolo de contingencia y la colaboración con las autoridades de ciberseguridad. No obstante, el CHU contaba con un plan de emergencia que había estado elaborando durante 18 meses, que además se aceleró debido a la oleada de ciberataques que afectaron a otros hospitales europeos en los últimos meses. Sin embargo, si el ciberataque en el CHU se hubiese producido antes, quizás no habría podido reaccionar de forma tan inmediata. Por otro lado, el Hospital Clínic se enfrentó a un escenario mucho más grave, un ciberataque tipo Ransomware en el que se cifraron los datos y se pidió un rescate que complicó aún más la situación.

Ambos casos recuerdan la necesidad de estar alerta y de revisar constantemente el plan de contingencia y de gestión de ciberincidentes, teniendo en cuenta el peor

de los escenarios posibles, así como los escenarios intermedios y las vulnerabilidades que pueden surgir en el cibernentorno hospitalario.

Conclusiones

Como se ha hecho evidente durante todo el trabajo, la ciberseguridad es un aspecto clave para garantizar la protección de los datos personales y la continuidad de los servicios sanitarios en un entorno cada vez más digitalizado y conectado. En este sentido, se hace necesario poner en marcha la propuesta sobre el proyecto del Reglamento de la comisión de marzo de 2022 destinado a garantizar un elevado nivel común de ciberseguridad en todas las instituciones, órganos y organismos de la UE, ya que aboga por un marco normativo armonizado para reforzar la resiliencia y la capacidad de respuesta ante este tipo de incidentes.

Asimismo, se requiere una mayor financiación tanto para la adopción de tecnología más avanzada en seguridad, como para el desarrollo de un equipo altamente competente en la materia ya que , como se ha demostrado en el análisis financiero, se tratan de inversiones que incrementan la eficiencia de los servicios sanitarios y con ello, también se ahorra tiempo y dinero. Además, se contribuye a mejorar la confianza y la satisfacción de los usuarios y los profesionales sanitarios.

Otro aspecto fundamental es el de equilibrar los cuatro principios de la ética biomédica para minimizar los efectos sociales producidos por este tipo de incidentes en el sector. Para ello, se hace imprescindible concienciar y educar a todo el personal sanitario, para hacer frente al desarrollo tecnológico que cada vez exige una mayor interconexión, lo que favorece la optimización de los procesos y por tanto, la beneficencia. De esta forma, también se respeta el principio de autonomía de los pacientes, se evita la no maleficencia y se promueve la justicia distributiva.

Por último, se recomienda realizar auditorías periódicas para adaptarse a las exigencias legales y éticas que permitan evaluar el nivel de cumplimiento de la normativa y detectar posibles riesgos o incumplimientos que puedan derivar en sanciones o brechas de seguridad. De igual modo, se debe establecer una estrategia holística en materia de ciberseguridad que ponga en marcha las medidas proactivas y preventivas mencionadas en el conjunto de capas del ciberentorno hospitalario. Dicha estrategia debe estar en actualización constante y también debe estudiarse previamente desde todos los escenarios posibles para garantizar o al menos minimizar el impacto multifacético que los incidentes de ciberseguridad presentan en el ámbito sanitario

Bibliografía

[1] «What is Cibersecurity?», ibm.com. https://www.ibm.com/topics/cybersecurity (accedido 14 de abril de 2023).

[2] A. F. Figueroa Uribe, J. Hernández Ramírez, A. F. Figueroa Uribe, y J. Hernández Ramírez, «Seguridad hospitalaria, una visión de seguridad multidimensional», Rev. Fac. Med. Humana, vol. 21, n.º 1, pp. 169-178, ene. 2021, doi: 10.25176/rfmh.v21i1.3490.

[3] «La novena edición del Informe sobre el panorama de amenazas de ENISA | Dando forma al futuro digital de Europa», 9 de noviembre de 2021. https://digital-strategy.ec.europa.eu/en/news/9th-edition-enisa-threat-landscape-report (accedido 16 de abril de 2023).

[4] «El aumento de los ataques cibernéticos a las instituciones de salud muestra la necesidad de una mayor ciberseguridad». https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=320e9ef15650 (accedido 16 de abril de 2023).

[5] «05-08-2022-CS-Report-CyberSecurity-Spagna-2Q2022-ES.pdf». Accedido: 16 de abril de 2023. [En línea]. Disponible en: https://www.exprivia.it/wp-content/uploads/2022/08/05-08-2022-CS-Report-CyberSecurity-Spagna-2Q2022-ES.pdf

[6] A. Calvo, «Ciberataques a hospitales, un problema grave en auge», CORRECTA - Ciberseguridad | Robotización | Sales Automation | Social Listening, 1 de septiembre de 2021. https://www.correcta.es/problema-ciberataques-hospitales/ (accedido 16 de abril de 2023).

[7] «BOE.es - DOUE-L-2019-80998 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº

526/2013 ("Reglamento sobre la Ciberseguridad").» https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80998 (accedido 10 de junio de 2023).

[8] «Agencia de la Unión Europea para la Ciberseguridad | Unión Europea». https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_es (accedido 16 de abril de 2023).

[9] «El marco de certificación de la ciberseguridad de la UE | Configurar el futuro digital de Europa», 25 de mayo de 2023. https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-certification-framework (accedido 10 de junio de 2023).

[10] «Front Page», Certificación Europrivacy. https://europrivacy.org/en/frontpage (accedido 16 de abril de 2023).

[11] «La ciberseguridad en las instituciones, órganos y organismos de la UE: el Consejo adopta su posición sobre unas normas comunes». https://www.consilium.europa.eu/es/press/press-releases/2022/11/18/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-adopts-its-position-on-common-rules/ (accedido 10 de junio de 2023).

[12] «Equipo de respuesta a emergencias informáticas (CERT-UE) | Unión Europea». https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_es (accedido 16 de abril de 2023).

[13] «BOE.es - DOUE-L-2022-81963 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).» https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963 (accedido 16 de abril de 2023).

[14] «Cost of a data breach 2022», 10 de abril de 2023. https://www.ibm.com/reports/data-breach (accedido 16 de abril de 2023).

[15] M. Loi, M. Christen, N. Kleine, y K. Weber, «Cybersecurity in health – disentangling value tensions», J. Inf. Commun. Ethics Soc., vol. 17, n.º 2, pp. 229-245, ene. 2019, doi: 10.1108/JICES-12-2018-0095.

[16] «BOE.es - Código de Derecho de la Ciberseguridad». https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad (accedido 27 de abril de 2023).

[17] Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, vol. 305. 2019. Accedido: 10 de junio de 2023. [En línea]. Disponible en: http://data.europa.eu/eli/dir/2019/1937/oj/spa

[18] «Art. 33 GDPR – Notification of a personal data breach to the supervisory authority», General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-33-gdpr/ (accedido 27 de abril de 2023).

[19] «Sanciones y medidas correctivas en materia de protección de datos», iberley.es, 28 de enero de 2019. https://www.iberley.es/temas/sanciones-medidas-correctivas-materia-proteccion-datos-62814 (accedido 27 de abril de 2023).

[20] «BOE-A-2002-22188 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.» https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188 (accedido 27 de abril de 2023).

[21] Ministerio de la Presidencia, 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, vol. BOE-A-2010-1330. 2010, pp. 8089-8138. Accedido: 27 de abril de 2023. [En línea]. Disponible en: https://www.boe.es/eli/es/rd/2010/01/08/3

[22] «BOE-A-2015-10389 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.» https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389 (accedido 27 de abril de 2023).

[23] «BOE-A-1995-25444 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.» https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 (accedido 27 de abril de 2023).

[24] «BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.» https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257 (accedido 27 de abril de 2023).

[25] «BOE-A-2015-3442 Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.» https://www.boe.es/buscar/act.php?id=BOE-A-2015-3442 (accedido 27 de abril de 2023).

[26] Jefatura del Estado, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, vol. BOE-A-2018-16673. 2018, pp. 119788-119857. Accedido: 27 de abril de 2023. [En línea]. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3

[27] M. Lehto, P. Neittaanmäki, J. Pöyhönen, y A. Hummelholm, «Cyber Security in Healthcare Systems», Comput. Methods Appl. Sci., 2022, doi: 10.1007/978-3-030-91293-2_8.

[28] J. T. Palacín, «El Clínic de Barcelona, un hospital en la nube», innovaspain, 5 de julio de 2022. https://www.innovaspain.com/hospital-clinic-de-barcelona-aws/ (accedido 20 de mayo de 2023).

[29] C. Blanchar, «El Hospital Clínic de Barcelona sufre un ciberataque y desprograma visitas y cirugías mientras no se resuelva», El País, 5 de marzo de 2023. https://elpais.com/espana/catalunya/2023-03-05/el-hospital-clinic-de-barcelona-victima-de-un-ciberataque-que-afecta-a-las-urgencias-el-laboratorio-y-la-farmacia.html (accedido 20 de mayo de 2023).

[30] J. M. Pascual Manuel G., «El ciberataque al Hospital Clínic de Barcelona, desde dentro: "Ha sido como hacer un viaje en el tiempo"», El País, 12 de marzo de 2023. https://elpais.com/tecnologia/2023-03-12/el-ciberataque-al-hospital-clinic-de-barcelona-desde-dentro-ha-sido-como-hacer-un-viaje-en-el-tiempo.html (accedido 20 de mayo de 2023).

[31] «El ciberataque que sufre el Hospital Clínic de Barcelona procede del extranjero y obliga a anular 3.000 visitas / Cataluña / EL PAÍS». https://elpais.com/espana/catalunya/2023-03-06/el-ciberataque-que-sufre-el-hospital-clinic-de-barcelona-procede-del-extranjero.html (accedido 20 de mayo de 2023).

[32] «El hospital Clínic, 48 horas después del ciberataque: "Hacemos pruebas y lo escribimos en papel" / Cataluña / EL PAÍS». https://elpais.com/espana/catalunya/2023-03-07/el-hospital-clinic-de-barcelona-48-horas-despues-del-ciberataque-hacemos-las-pruebas-y-lo-escribimos-en-papel.html#?rel=mas_sumario (accedido 20 de mayo de 2023).

[33] J. Mouzo, «Los ciberdelincuentes que atacaron el Clínic piden 4,2 millones de euros para liberar los datos», El País, 10 de marzo de 2023. https://elpais.com/espana/catalunya/2023-03-10/los-ciberdelincuentes-que-atacaron-el-clinic-piden-45-millones-de-dolares-para-liberar-los-datos.html (accedido 20 de mayo de 2023).

[34] «El hospital Clínic reconoce que el ciberataque puede "comprometer la confidencialidad" de los pacientes / Cataluña / EL PAÍS». https://elpais.com/espana/catalunya/2023-03-21/el-hospital-clinic-reconoce-ahora-que-el-ciberataque-podria-comprometer-la-confidencialidad-de-los-datos-de-pacientes-y-trabajadores.html?rel=buscador_noticias (accedido 20 de mayo de 2023).

[35] R. Carranco, «Los ciberdelincuentes filtran de madrugada datos robados del Hospital Clínic», El País, 30 de marzo de 2023. https://elpais.com/espana/catalunya/2023-03-30/los-ciberdelincuentes-filtran-de-madrugada-datos-robados-del-hospital-clinic.html (accedido 20 de mayo de 2023).

[36] B. Coll, «Los ciberdelincuentes del Clínic contraatacan y amenazan con filtrar datos de pacientes con enfermedades infecciosas», El País, 6 de abril de 2023. https://elpais.com/espana/catalunya/2023-04-06/los-ciberdelincuentes-del-clinic-contraatacan-y-amenazan-con-filtrar-datos-de-pacientes-con-enfermedades-infecciosas.html (accedido 20 de mayo de 2023).

[37] «Ciberataque al hospital Clínic de Barcelona | Hospital Clínic Barcelona». https://www.clinicbarcelona.org/prensa/ultima-hora/ciberataque-al-hospital-clinic-de-barcelona (accedido 20 de mayo de 2023).

[38] «Ciberataque en el Clínic: ¿Por qué el hospital no estaba integrado en la Agencia de ciberseguridad si existía un plan para ello? | Cataluña | EL PAÍS». https://elpais.com/espana/catalunya/2023-04-08/ciberataque-en-el-clinic-por-que-el-hospital-no-estaba-integrado-en-la-agencia-de-ciberseguridad-si-existia-un-plan-para-ello.html?rel=buscador_noticias (accedido 20 de mayo de 2023).

[39] «Retour à la normale au CHU Saint-Pierre cible d'une cyberattaque», Le Soir, 11 de marzo de 2023. https://www.lesoir.be/500384/article/2023-03-11/retour-la-normale-au-chu-saint-pierre-cible-dune-cyberattaque?referer%3D%2Farchives%2Frecherche%3Fdatefilter%3Dlastyear%26sort%3Ddate%2520desc%26word%3DCHU%2520Saint-Pierre (accedido 11 de junio de 2023).

[40] «Guía nacional de notificación y gestión de ciberincidentes».