

MARSH | JG | plain concepts | from thought to value

Resiliencia y riesgos digitales en los activos sanitarios de España

Índice

Alcance del estudio 03

Aviso legal y condiciones de uso 04

1. Resumen ejecutivo 05

2. Introducción 06

3. Marco conceptual y normativo 10

4. Activos hospitalarios críticos 13

5. Amenazas 17

6. Escenarios de riesgo 21

7. Buenas prácticas y recomendaciones 27

8. Gestión de Crisis 31

9. Resultado del Análisis 34

10. Conclusiones 35

Anexos | Normativa 36

Equipo y contacto 73

Alcance del estudio

El presente documento ha sido elaborado por JG Ingenieros, Marsh y Plain Concepts, organizaciones de referencia en sus respectivos ámbitos —ingeniería de edificación de alta complejidad, consultoría de riesgos y seguros, soluciones tecnológicas y analítica de datos, respectivamente—, con el objetivo de desarrollar un estudio independiente sobre la resiliencia digital y la continuidad asistencial en el sector sanitario español.

El estudio tiene por finalidad evaluar el grado de preparación de los centros sanitarios frente a incidentes de origen digital, tecnológico u operativo (tales como fallos en las comunicaciones, ciberataques, interrupciones del suministro eléctrico o eventos climáticos adversos) y analizar cómo afrontan los nuevos retos como son la hiperconectividad, Internet de las Cosas Médicas (IoMT) y la inteligencia artificial (IA). El objetivo final es identificar buenas prácticas y formular recomendaciones para el sector. Estas serán aplicables tanto en el diseño de nuevas infraestructuras como en la adaptación y mejora de las existentes.

Este artículo se basa en un análisis del estado de la infraestructura actual del sector sanitario, teniendo en cuenta los últimos eventos que le han afectado y su respuesta, así como la participación de una muestra representativa del sector hospitalario español, que incluye tanto centros públicos como privados, para ello, se han utilizado encuestas estructuradas y entrevistas realizadas con los diferentes agentes del sector.

Aviso legal y condiciones de uso

La presente publicación tiene carácter exclusivamente informativo. Los datos utilizados en el estudio han sido tratados de forma anónima y confidencial en todo momento, y en ningún caso serán utilizados con fines comerciales.

El documento incluye referencias a fuentes de terceros cuando resulta pertinente. JG Ingenieros, Marsh y Plain Concepts no se responsabilizan del contenido de dichas fuentes externas, incluidos los sitios web a los que se pueda hacer referencia.



1. Resumen ejecutivo

El presente documento tiene como objetivo analizar la resiliencia de los activos hospitalarios en España, poniendo el foco en la necesidad de integrar de forma efectiva las dimensiones digital y física para garantizar la continuidad asistencial ante amenazas disruptivas de cualquier índole.

Con este fin, el estudio aborda los principales marcos conceptuales y normativos, además de tener en cuenta la transformación tecnológica que vive el sector sanitario. La creciente digitalización de procesos, la adopción de tecnologías como (IoT), SD-WAN y los servicios en la nube (cloud), y la consolidación de estrategias como la "Salud Digital" del Sistema Nacional de Salud (SNS), están impulsando un cambio estructural en el modelo operativo de los hospitales. Esta evolución mejora la eficiencia y la calidad asistencial, pero también incrementa la dependencia tecnológica y amplía la exposición a riesgos.

En paralelo, los acontecimientos recientes, como la pandemia de la COVID-19, el apagón energético de 2025, el aumento de eventos climáticos extremos, el crecimiento de ciberataques y la creciente presión regulatoria, han evidenciado que la capacidad de respuesta del sistema sanitario depende en gran medida del nivel de modernización, inversión y madurez de sus infraestructuras y sistemas. Las diferencias existentes entre centros, determinadas por la antigüedad y complejidad de su edificación, condicionan tanto la capacidad de mitigación como la recuperación operativa, y pueden influir en la prestación del servicio.

En este contexto, este documento se plantea como una guía para el sector sanitario, abordando de forma integrada los riesgos de carácter digital, como por ejemplo, ataques de ransomware, denegación de servicio o phishing, junto otros riesgos físicos, tales como apagones, fallos de infraestructuras o eventos climáticos, que pueden afectar a la operatividad hospitalaria.

Todo ello se analiza teniendo en cuenta los retos derivados de la incorporación de nuevas tecnologías sobre infraestructuras que, en muchos casos, no fueron diseñadas para soportarlas y la necesidad de garantizar la disponibilidad, integridad, confidencialidad y resiliencia de los sistemas y los datos.

Como resultado este estudio: pretende ser una referencia para la implementación de recomendaciones y buenas prácticas, orientadas a reducir los posibles eventos o problemas detectados, promover inversiones y definir estrategias integradas de resiliencia digital y física. Asimismo, se destaca la importancia de reforzar la cultura organizativa en materia de prevención y respuesta ante incidentes, alineado con las normativas y estándares internacionales aplicables al sector sanitario.

La resiliencia de los hospitales españoles depende de la integración efectiva de infraestructuras y sistemas digitales, siendo esencial reforzar de forma coordinada la seguridad física y digital para garantizar la continuidad asistencial ante amenazas cada vez más complejas.

2. Introducción

El sector sanitario, entendido como el conjunto de hospitales y centros asistenciales, constituye un pilar esencial de las sociedades actuales y es un elemento crucial en la capacidad de respuesta de un Estado ante crisis de diversa naturaleza, como crisis sanitarias, energéticas, climáticas o tecnológicas. Garantizar la operatividad de estas infraestructuras y la continuidad de los servicios asistenciales requiere disponer de altos niveles de resiliencia institucional, organizativa y técnica.

En este contexto actual, el concepto de resiliencia ha adquirido un protagonismo creciente en el ámbito sanitario. El Departamento de Seguridad Nacional define la resiliencia como la capacidad para resistir y recuperarse frente a eventos adversos, garantizando la continuidad de los servicios esenciales. Asimismo, el Plan de Recuperación, Transformación y Resiliencia (PRTR) incorpora la modernización del Sistema Nacional de Salud (SNS) como uno de sus ejes fundamentales, con el objetivo de reforzar su capacidad de respuesta ante crisis y mejorar su resiliencia estructural.[1]

A nivel internacional, organismos como la Organización Mundial de la Salud (OMS) han destacado la necesidad de reforzar la resiliencia de los sistemas de salud como elemento clave para garantizar la cobertura y la seguridad sanitarias ante crisis futuras.[2]

2.1. Crisis recientes y respuesta del sector

Durante la última década, el sistema sanitario español se ha enfrentado a diversas crisis que han puesto a prueba su capacidad de respuesta. Aunque el sistema ha mostrado una elevada capacidad de adaptación, el impacto no ha sido homogéneo, evidenciando diferencias relevantes en infraestructura, inversión y madurez operativa. Las principales tipologías de crisis pueden agruparse en:

- **Crisis sanitaria (COVID-19):** La pandemia generó una presión sin precedentes sobre el sistema sanitario, especialmente en unidades de cuidados intensivos, y obligó a reorganizar recursos en muy poco tiempo. La evaluación oficial del desempeño del SNS identificó un impacto estructural sobre la capacidad asistencial, la mortalidad, la organización sanitaria y la actividad económica, ampliamente documentado por los sistemas nacionales de vigilancia epidemiológica.[3]

- **Crisis energética (apagón eléctrico de 2025):** El apagón del 28 de abril de 2025 evidenció la dependencia crítica del sistema sanitario respecto a la infraestructura energética. Los análisis técnicos del evento describen una secuencia multifactorial de fallos y desconexiones en cascada que derivó en el colapso del sistema eléctrico peninsular, poniendo de relieve la importancia de los sistemas de respaldo en infraestructuras hospitalarias. [4]

1 — Link
2 — Link
3 — Link
4 — Link

- **Crisis climática y medioambiental:** El aumento de fenómenos extremos —olas de calor, sequías, incendios e inundaciones— está incrementando la exposición de los activos sanitarios a riesgos físicos y operativos. Agencia Estatal de Meteorología (AEMET) constata un aumento de temperaturas, una mayor frecuencia de situaciones térmicas extremas y una expansión de condiciones más áridas en España, mientras que el Ministerio para la Transición Ecológica y el Reto Demográfico (MITECO) identifica más de 140 riesgos climáticos con efectos sobre sectores estratégicos, incluido el sanitario.[5]

En conjunto, estas crisis evidencian que, aunque el sistema sanitario presenta un nivel relevante de resiliencia, las diferencias en modernización, inversión y preparación condicionan significativamente la capacidad de respuesta. A medida que aumenta la digitalización, estos eventos adversos pueden ampliarse si no se adopta un enfoque integrado para disponer de una mayor resiliencia.

2.2. Por qué la dimensión digital es crítica

El entorno sanitario ha evolucionado hacia modelos altamente digitalizados en los que los sistemas de información clínica, la telemedicina, la monitorización remota, los dispositivos conectados, las plataformas en la nube y la inteligencia artificial se han convertido en elementos estructurales de la prestación asistencial. Esta transformación, alineada con la Estrategia de Salud Digital del Sistema Nacional de Salud, está orientada a mejorar la calidad, la eficiencia y la continuidad del servicio.[6] En este contexto, la criticidad de la dimensión digital se fundamenta en los siguientes aspectos:

- **Integración en la prestación asistencial.** La tecnología ha dejado de ser un soporte auxiliar para convertirse en el sustrato sobre el que se presta la asistencia sanitaria, condicionando directamente la operativa clínica.

- **Dependencia tecnológica creciente.** La digitalización incrementa la dependencia de sistemas, redes de comunicaciones, suministro energético y plataformas externas, ampliando la exposición a riesgos tecnológicos, como fallos de disponibilidad o vulnerabilidades en dispositivos conectados.

- **Alta exposición a ciberincidentes.** El sector sanitario se sitúa entre los más afectados por incidentes de ciberseguridad en Europa. Según European Union Agency For Cybersecurity (ENISA), estos incidentes impactan de forma significativa en la operativa asistencial.[7]

- **Impacto sistémico de los fallos.** En entornos altamente tecnificados, una incidencia tecnológica puede afectar simultáneamente a múltiples dispositivos y procesos clínicos, generando efectos en cadena.

La resiliencia digital se configura, por tanto, como un elemento central para garantizar la continuidad asistencial y la sostenibilidad del sistema sanitario.



5 — Link

6 — Link

7 — Link

2.3. La ciberseguridad en el entorno hospitalario: evolución y contexto tecnológico

La creciente digitalización ha situado la dependencia tecnológica en el núcleo de la prestación asistencial.

En este contexto, el enfoque de ciberseguridad en el entorno hospitalario se caracteriza por:

- **Entorno altamente interdependiente:** Los sistemas clínicos, dispositivos médicos, infraestructuras técnicas y plataformas digitales configuran un ecosistema integrado en el que múltiples activos dependen entre sí.

- **Impacto directo sobre la asistencia:** Los incidentes digitales pueden afectar directamente a la seguridad del paciente y a la continuidad del servicio, más allá de su dimensión tecnológica.

- **Naturaleza operativa del riesgo.** Los riesgos digitales deben analizarse como eventos con impacto asistencial, operativo y reputacional, especialmente en entornos de alta complejidad como los hospitales.

La ciberseguridad deja de ser un ámbito exclusivamente tecnológico para convertirse en un componente estructural de la operativa diaria.

2.4. Alcance de los activos sanitarios y su exposición al riesgo

Los análisis de riesgos digitales en el sector sanitario deben considerar que los hospitales forman parte de un sistema asistencial interconectado, en el que coexisten centros públicos y privados con distintos niveles de madurez tecnológica y modelos operativos.

Su exposición al riesgo se explica a través de los siguientes elementos:

- **Diferentes niveles de criticidad en función del centro.** Los hospitales de alta complejidad (con Unidad de Cuidados Intensivos (UCI), bloque quirúrgico o diagnóstico por imagen) presentan mayor dependencia tecnológica y mayor impacto potencial ante incidentes que los dispositivos asistenciales de menor complejidad, como los centros de atención primaria.

- **Diversidad de activos hospitalarios.** Los activos pueden agruparse en cuatro grandes categorías: activos asistenciales, sistemas de información clínica, infraestructuras tecnológicas e infraestructuras físicas digitalizadas, presentando cada uno distintos niveles de criticidad y exposición al riesgo.

- **Activos especialmente atractivos de ser atacados.** Determinados activos —especialmente los vinculados a datos clínicos y la prestación asistencial directa (como historia clínica, monitorización o diagnóstico)— presentan mayor atractivo por el valor de la información y por su impacto inmediato en la continuidad del servicio.

- **Exposición transversal al riesgo.** El riesgo no se concentra en un único activo, sino que se distribuye a lo largo del ecosistema hospitalario, condicionado por las interdependencias entre sistemas y la integración creciente entre infraestructuras físicas y digitales.

La gestión del riesgo requiere un enfoque global que considere tanto la naturaleza de los activos como su grado de interdependencia dentro del sistema hospitalario.

2.5. Relevancia estratégica del riesgo digital en el entorno hospitalario

Los riesgos digitales en el entorno hospitalario tienen una dimensión estratégica que trasciende el ámbito tecnológico, al afectar directamente a la capacidad del sistema sanitario para garantizar una prestación asistencial continua, segura y eficiente.

En este contexto, su relevancia se articula en las siguientes dimensiones:

- **Continuidad asistencial:** La digitalización integra los sistemas tecnológicos en el propio proceso asistencial. Como resultado, cualquier interrupción digital puede traducirse en una degradación operativa con un impacto directo en la atención al paciente y en la continuidad del servicio.

- **Protección de la información clínica:** Los datos clínicos son altamente sensibles y críticos para la prestación asistencial. Su protección resulta esencial tanto para garantizar la seguridad del paciente como para cumplir con los requisitos regulatorios y preservar la confianza en el sistema sanitario.

- **Dependencia tecnológica:** La integración de sistemas, plataformas externas y servicios conectados, incrementa la complejidad del entorno hospitalario y genera nuevas dependencias que condicionan su operativa y resiliencia.

- **Interdependencia ciberfísica:** El hospital combina infraestructuras físicas (energía, climatización, agua, gases) y sistemas digitales interconectados. Esta relación puede generar efectos en cascada ante incidentes, amplificando su impacto sobre la operativa.

- **Seguridad desde el diseño:** La incorporación de tecnologías como IoT, cloud o inteligencia artificial refuerza la necesidad de integrar la gestión del riesgo digital desde el diseño de los activos y de los modelos operativos, y no como una capa posterior.

El entorno hospitalario evoluciona hacia un sistema ciberfísico complejo, en el que la resiliencia depende de la capacidad de integrar de forma coherente la seguridad digital, la continuidad operativa y la gestión de dependencias.



3. Marco conceptual y normativo

El marco conceptual y de referencia permite estructurar, clasificar y gestionar el riesgo digital de forma objetiva, proporcionando un lenguaje común, para el análisis y la toma de decisiones, así como criterios de cumplimiento y validación. En este contexto, la normativa define las obligaciones aplicables, mientras que los estándares y marcos de referencia permiten llevar a la práctica la gestión del riesgo.

3.1. Conceptos clave de riesgo

Concepto	Definición	Aplicación en entorno hospitalario
Confidencialidad	Protección frente a accesos no autorizados de la información	Datos clínicos, historiales y resultados
Integridad	Garantía de que la información no se altera	Prescripción médica, diagnóstico
Disponibilidad	Acceso continuo a sistemas y datos	Historia Clínica Electrónica (HCE), UCI, laboratorio
Activo	Elemento que aporta valor y debe protegerse	Sistemas clínicos, dispositivos, infraestructuras
Amenaza	Evento potencial que puede causar daño	Ciberataque, fallo técnico (detalle en sección 5)
Vulnerabilidad	Debilidad explotable por una amenaza	Sistemas obsoletos, IoT sin parchear
Riesgo	Probabilidad e impacto de un evento	Interrupción de servicio asistencial
Impacto	Consecuencia de la materialización del riesgo	Clínico, operativo, reputacional
Dependencia	Relación entre activos o sistemas	Red → HCE → dispositivos
Interdependencia	Dependencias cruzadas entre sistemas	IT ↔ OT ↔ clínico (entorno ciberfísico)

El riesgo hospitalario debe analizarse considerando simultáneamente activos, dependencias y consecuencias, y no únicamente amenazas aisladas.

3.2. Normativa y estándares

Norma	Ámbito	Relevancia en hospitales
RGPD (UE 2016/679)	Protección de datos	Tratamiento de datos clínicos y brechas
NIS2 (UE 2022/2555)	Ciberseguridad	Gestión de riesgos y notificación de incidentes
ENS (RD 311/2022)	Sector público España	Requisitos mínimos de seguridad en sistemas
LPIC (Ley 8/2011)	Infraestructuras críticas	Protección de servicios esenciales
AEPD	Protección de datos	Criterios específicos sector sanitario

Estándar	Ámbito	Relevancia en hospitales
ISO/IEC 27001	Seguridad de la información	Estructura la gestión del riesgo en sistemas clínicos y administrativos
ISO 22301	Continuidad de negocio	Permite garantizar continuidad asistencial ante incidentes
IEC 62443	OT / sistemas industriales	Protege infraestructuras técnicas (energía, climatización, BMS) en entornos hospitalarios digitalizados
NIST CSF	Ciberseguridad	Proporciona un marco práctico para identificar, proteger, detectar y responder a incidentes



3.3. Certificación de producto y cadena de suministro

Certificación	Ámbito	Relevancia en hospitales
MDR (UE 2017/745)	Dispositivos médicos	Garantiza la seguridad, calidad y conformidad de los equipos utilizados en la atención al paciente
Cyber Resilience Act CRA Regulation (EU) 2024/2847	Dispositivos y Software	Establece requisitos obligatorios de ciberseguridad para los "productos con elementos digitales" (hardware y software) que se comercializan en la UE, aplicando el principio de security by design/ by default y obligaciones de documentación y gestión de vulnerabilidades.
IEC 62443 (4-1 / 4-2)	Componentes y sistemas OT	Establece requisitos de seguridad por diseño en sistemas técnicos e infraestructuras hospitalarias digitalizadas

La seguridad del entorno hospitalario depende en gran medida de la seguridad de los productos y proveedores que forman parte de su ecosistema. En este contexto, los procesos de certificación permiten garantizar aspectos esenciales como la seguridad por diseño, la gestión de vulnerabilidades, la validación mediante pruebas de seguridad y la correcta integración de los sistemas. Asimismo, la gestión de proveedores y del ciclo de vida tecnológico resulta clave para asegurar la robustez del entorno operativo. En consecuencia, la seguridad hospitalaria no depende únicamente de sus sistemas internos, sino del conjunto de tecnologías y servicios externos que conforman su entorno digital.



4. Activos hospitalarios críticos

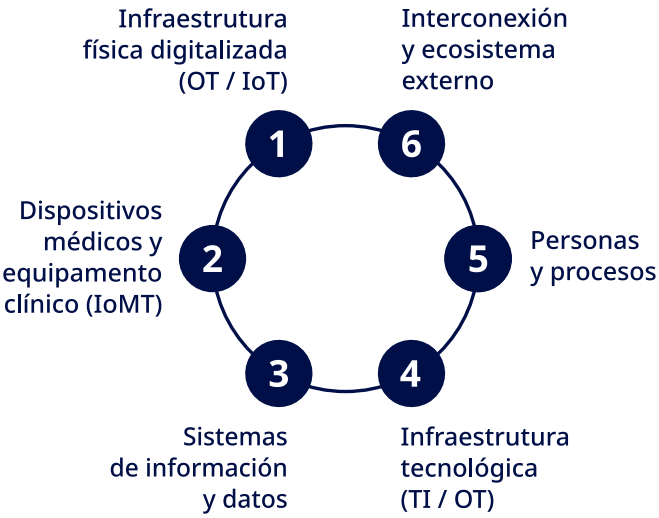
Los hospitales constituyen entornos altamente complejos formados por un conjunto de activos interconectados que integran dimensiones físicas, tecnológicas, clínicas y organizativas.

La operación hospitalaria exige continuidad 24/7, alta disponibilidad y una coordinación constante entre sistemas, lo que configura un entorno ciberfísico en el que la dependencia entre activos es estructural.

Desde el punto de vista cuantitativo, esta complejidad se refleja en la elevada densidad de activos digitales conectados. Diversos estudios del sector sitúan el número de dispositivos conectados en hospitales en un orden de magnitud de:

- 10–15 dispositivos médicos conectados por cama[8]
- 15–20 dispositivos conectados por habitación hospitalaria[9]
- Miles de dispositivos por hospital, con estimaciones superiores a 3.800 dispositivos conectados en hospitales digitalizados[10]

A estos activos clínicos se suman los sistemas de infraestructura técnica, comunicaciones, seguridad y gestión, lo que lleva a que hospitales de tamaño medio y grandes que operen con decenas de miles de activos interconectados. Más allá del volumen, el elemento clave es la interdependencia, consiste en que el funcionamiento de cada activo, depende de múltiples capas (infraestructura física, tecnologías digitales, información y personas), lo que exige abordar su análisis de forma integrada, tal como se ha definido en el marco conceptual del capítulo 3. En este contexto, los activos hospitalarios se estructuran en seis macrodominios, que permiten organizar el análisis y sirven como base para los capítulos posteriores de amenazas, escenarios de riesgo y recomendaciones.



Interdependencias entre dominios

La infraestructura física soporta todos los sistemas

La infraestructura tecnológica conecta el ecosistema

Los sistemas de información integran los datos

Las personas operan y supervisan los activos

El ecosistema externo amplía dependencias e interconexión

8 — Link | 9 — Link | 10 — Link

4.1. Infraestructura física digitalizada (OT / IoT)

Comprende los sistemas del edificio que incorporan automatización, control y sensorización, necesarios para garantizar condiciones operativas adecuadas. Incluyen lo siguiente:

- Sistemas eléctricos y de energía
- Climatización y control ambiental
- Sistemas de agua y fluidos
- Gases medicinales
- Seguridad física (CCTV, accesos, incendios)
- Comunicaciones internas técnicas

Aspectos clave:

- Constituyen la base operativa del hospital
- Garantizan condiciones físicas necesarias para la actividad clínica
- Están crecientemente digitalizados (BMS, PLC, SCADA)
- Presentan dependencia fuerte de redes OT y energía

4.2. Dispositivos médicos y equipamiento clínico (IoMT)

Agrupa los activos directamente vinculados a la atención al paciente, caracterizados por su elevado número y diversidad. Incluyen lo siguiente:

- Monitorización y soporte vital
- Bombas de infusión
- Equipos de imagen
- Equipamiento de laboratorio
- Sistemas quirúrgicos avanzados
- Dispositivos IoT de soporte clínico

Aspectos clave:

- Capa más directamente asociada a la seguridad del paciente
- Altísima densidad de dispositivos conectados
- Larga vida útil y presencia de tecnología legacy
- Creciente conectividad e integración con otros sistemas



4.3. Sistemas de información y datos

Constituyen el núcleo digital que articula la actividad clínica y operativa. Incluye lo siguiente:

- Historia clínica electrónica (HCE)
- LIS (sistema de Información de Laboratorio), RIS (Radiology Information System)/PACS (Picture Archiving and Communication System), farmacia, prescripción electrónica
- Sistemas administrativos y de gestión

Aspectos clave:

- Integran la información clínica del paciente
- Soportan la toma de decisiones asistenciales
- Requieren alta disponibilidad y calidad del dato
- Dependen completamente de la infraestructura TI

4.4. Infraestructura tecnológica (IT/OT)

Actúa como columna vertebral digital que conecta y soporta el conjunto del hospital. Incluyen lo siguiente:

- Redes (LAN, WAN, WiFi)
- Centros de datos y almacenamiento
- Servidores y virtualización
- Sistemas de ciberseguridad
- Dispositivos de usuario

Aspectos clave:

- Habilita la comunicación entre todos los activos
- Determina la disponibilidad global del sistema
- Concentra dependencias críticas (red, CPD, identidad)
- Es un elemento clave en resiliencia operativa

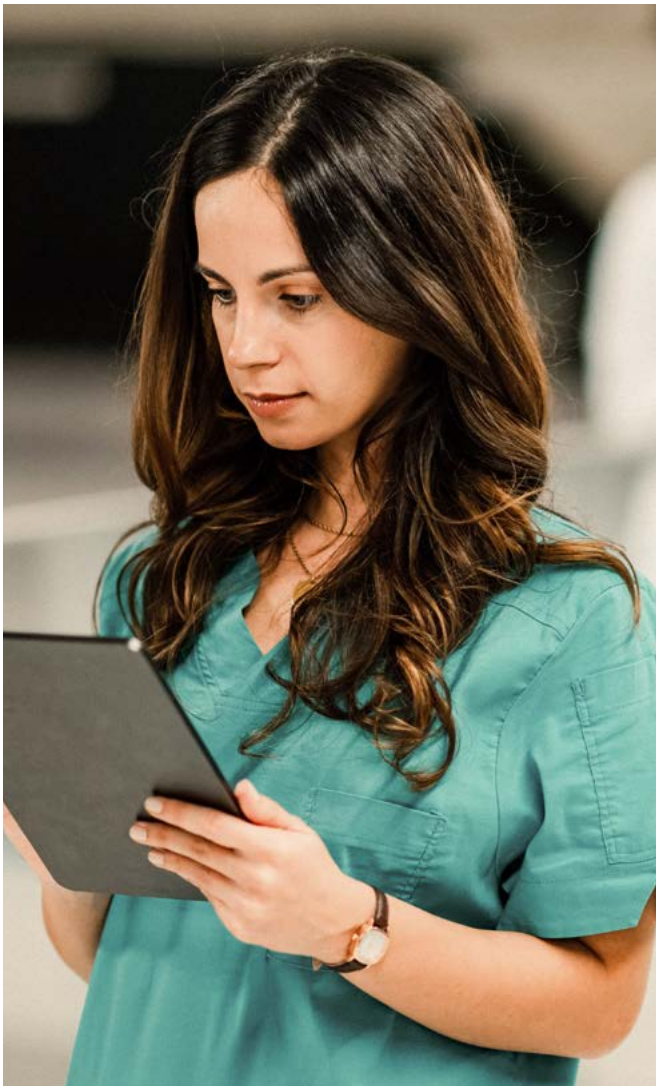
4.5. Personas y procesos

Representa la dimensión organizativa del sistema hospitalario. Incluyen lo siguiente:

- Personal sanitario, técnico y administrativo
- Procesos clínicos, operativos y de soporte
- Modelos de gestión y operación

Aspectos clave:

- Los usuarios son parte activa del sistema ciberfísico
- Los procesos determinan el uso de los activos
- El error humano es un factor estructural
- La cultura organizativa condiciona la resiliencia



4.6. Interconexión y ecosistema externo

Extiende el perímetro del hospital más allá de sus límites físicos. Incluye lo siguiente:

- integración con redes sanitarias externas
- proveedores tecnológicos
- servicios cloud
- telemedicina
- intercambio de datos clínicos

Aspectos clave:

- amplía el perímetro de exposición
- introduce dependencias externas críticas
- exige interoperabilidad (HL7, DICOM, APIs)
- convierte al hospital en nodo de un sistema distribuido

4.7. Interdependencias entre dominios

Los seis dominios descritos no operan de forma independiente, sino como un sistema único con múltiples dependencias cruzadas:

- La infraestructura física soporta todos los sistemas
- La infraestructura tecnológica conecta el ecosistema
- los sistemas de información integran los datos
- Las personas operan y supervisan los activos
- El ecosistema externo amplía dependencias

Esta interdependencia implica que el análisis de activos no puede realizarse de forma aislada, sino considerando su papel dentro del sistema global.

El detalle específico de cada tipología de activo, incluyendo su caracterización técnica, dependencias, criticidad, amenazas, vulnerabilidades, escenarios de riesgo y recomendaciones, se recoge de forma más exhaustiva en la **Tabla 1** del **anexo**.



5. Amenazas

En este contexto, se entiende por amenaza cualquier evento, agente o situación con capacidad de materializar un daño sobre un activo, comprometiendo su disponibilidad, integridad o confidencialidad, y afectando en última instancia a la continuidad asistencial.

A diferencia de los activos, que representan aquello que debe protegerse, las amenazas representan el origen potencial del daño, y se caracterizan por:

- Su capacidad de propagación a través de sistemas interconectados
- Su interacción con vulnerabilidades existentes
- Su impacto potencial sobre múltiples dominios simultáneamente

En el entorno hospitalario, las amenazas presentan además tres particularidades clave:

- **Carácter híbrido (digital y físico).** Una misma amenaza puede afectar tanto a sistemas tecnológicos como a las infraestructuras físicas, generando efectos combinados (por ejemplo, un ataque que deriva en pérdida de condiciones ambientales o suministro).
- **Efecto en cascada.** Debido a la elevada interdependencia entre activos, una misma amenaza puede propagarse rápidamente y afectar a múltiples sistemas clínicos, técnicos y organizativos.
- **Impacto asistencial directo.** A diferencia de otros sectores, la materialización de una amenaza puede tener consecuencias inmediatas sobre la seguridad del paciente, además del impacto operativo o reputacional.

A efectos de este análisis, las amenazas se clasifican en cuatro grandes categorías:

- Amenazas internas, originadas dentro del propio hospital
- Amenazas externas, procedentes de agentes o sistemas fuera de su control
- Fallos técnicos o de funcionamiento, de carácter no intencionado
- Amenazas asociadas a sistemas de inteligencia artificial, derivadas de nuevas tecnologías emergentes

Esta clasificación permite organizar el análisis de forma coherente y facilita la trazabilidad posterior entre amenazas, vulnerabilidades y escenarios de riesgo, evitando duplicidades y asegurando un enfoque estructurado.

5.1. Amenazas por tipología

Amenazas internas

Se originan dentro del propio hospital y están asociadas a personas, procesos o accesos no autorizados.

Principales factores:
- Entorno de confianza operativa
- Acceso con privilegios a sistemas
- Interacción directa con activos críticos

Principales amenazas:
- Abuso de privilegios
- Accesos indebidos a información clínica
- Sabotaje de sistemas o dispositivos
- Errores humanos y malas prácticas
- Pérdida o sustracción de dispositivos
- Inadecuadas prácticas de proveedores que operan en el centro

Amenazas externas

Proceden de actores externos o de eventos que ocurren fuera del control del hospital.

Principales factores:
- Aumento de la conectividad (cloud, APIs, telemedicina)
- Ampliación del perímetro digital
- Dependencia de terceros

Principales amenazas:
- Ransomware, malware y phishing
- Explotación de vulnerabilidades
- Ataques a redes (DDoS, intrusión)
- Manipulación de dispositivos IoMT/IoT
- Sabotaje físico o corte de infraestructuras o servicios.

Fallos técnicos o de funcionamiento

No son intencionados, pero pueden generar impactos críticos.

Principales factores:
- Complejidad tecnológica
- Dependencia de sistemas críticos
- Integración IT–OT

Principales amenazas:
- Fallos de hardware o energía
- Errores de software
- Fallos en actualizaciones o despliegues
- Caída de comunicaciones
- Indisponibilidad de sistemas de autenticación

Amenazas específicas de inteligencia artificial

Asociadas a la incorporación de IA en procesos clínicos y operativos.

Principales factores:
- Comportamiento no determinista
- Dependencia de los datos
- Falta de trazabilidad completa

Principales amenazas:
- Manipulación del modelo o de la inferencia
- Envenenamiento de datos
- Ataques a asistentes (prompt injection)
- Dependencia de servicios externos
- Automatización con permisos excesivos

5.2. Vulnerabilidades

Las vulnerabilidades son las debilidades que permiten que una amenaza se materialice sobre un activo. En el entorno hospitalario, estas vulnerabilidades derivan principalmente de:

- Complejidad tecnológica
- Falta de segmentación
- Debilidades organizativas
- Dependencia de terceros
- Coexistencia de sistemas legacy y modernos

Su identificación es esencial para comprender cómo las amenazas pueden convertirse en incidentes reales.



Vulnerabilidades asociadas a amenazas internas

Debilidades vinculadas al uso, gestión y acceso interno a los sistemas hospitalarios, principalmente por parte de personal propio o terceros con acceso.

Factores clave
- Entorno de confianza operativa
- Acceso directo a sistemas críticos
- Dependencia del comportamiento humano
- Coexistencia de múltiples perfiles de usuario

Principales vulnerabilidades
- Accesos privilegiados sin control ni revisión periódica
- Falta de registros y trazabilidad de acciones
- Ausencia de segregación entre entornos IT/OT
- Gestión inadecuada de dispositivos móviles o personales
- Falta de formación y concienciación de seguridad
- Controles insuficientes en el acceso físico

Vulnerabilidades asociadas a amenazas externas

Debilidades que permiten la explotación remota de sistemas y servicios expuestos, así como el acceso indebido desde el exterior.

Factores clave
- Ampliación del perímetro digital
- Exposición a internet y servicios externos
- Integración con terceros y plataformas cloud
- Alta conectividad de dispositivos
- Falta de medidas de seguridad desde el diseño

Principales vulnerabilidades
- Sistemas sin parchear o actualizaciones pendientes
- Ausencia de autenticación fuerte (MFA)
- Exposición de APIs y servicios sin protección adecuada
- Configuraciones inseguras en entornos cloud
- Segmentación de red insuficiente
- Dispositivos IoMT con configuraciones débiles o por defecto

Vulnerabilidades asociadas a fallos técnicos

Debilidades estructurales relacionadas con la arquitectura tecnológica, la operación de sistemas y la gestión del ciclo de vida de los activos.

Factores clave
- Complejidad tecnológica
- Dependencia de infraestructuras críticas
- Coexistencia de sistemas legacy
- Gestión del cambio

Principales vulnerabilidades
- Ausencia de redundancia en sistemas críticos
- Mantenimiento insuficiente o no planificado
- Dependencia de sistemas únicos (single point of failure)
- Validación insuficiente de actualizaciones o despliegues
- Fallos en sistemas de autenticación (Active Directory (AD), certificados)
- Infraestructuras obsoletas o sin soporte

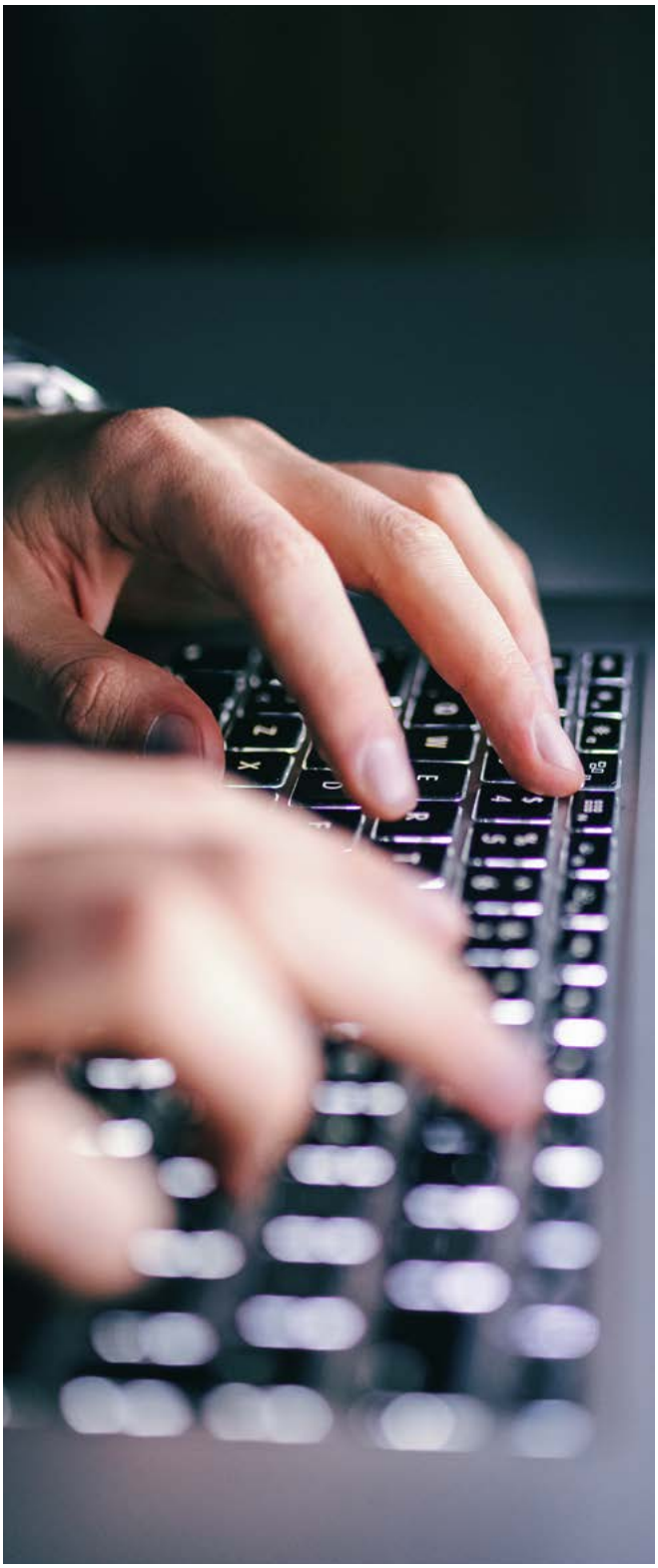
Vulnerabilidades asociadas a inteligencia artificial

Debilidades específicas derivadas del uso de sistemas de IA, relacionadas con datos, modelos, operación y gobernanza.

Factores clave
- Dependencia crítica del dato
- Complejidad de los modelos
- Dificultad de trazabilidad
- Integración con sistemas clínicos

Principales vulnerabilidades
- Falta de validación y robustez de modelos
- Pipelines de datos sin control de integridad
- Ausencia de control sobre inputs y outputs (prompts/respuestas)
- Dependencia de servicios externos de IA
- Falta de control de permisos en agentes
- Monitorización insuficiente del comportamiento del sistema

El detalle exhaustivo de amenazas y vulnerabilidades, así como su relación específica con los activos hospitalarios definidos en el capítulo 4, se desarrolla de forma ampliada en el **anexo del documento**.



6. Escenarios de riesgo

6.1. Escenarios de ataque comunes y emergentes

El sector sanitario y específicamente los hospitales en España, como infraestructura crítica, enfrentan una amplia variedad de amenazas ciber que pueden comprometer la seguridad, privacidad y continuidad de los servicios asistenciales.

A continuación, se describen los escenarios de ataque más comunes y emergentes en el entorno hospitalario:

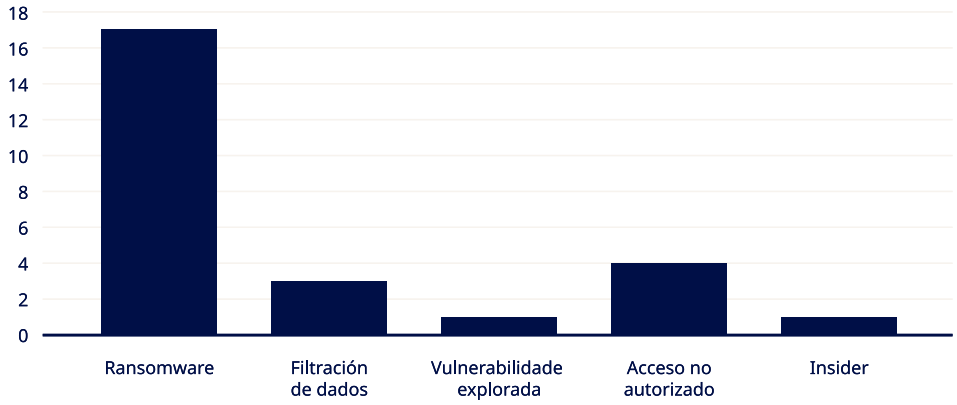


Figura 1: Ataques en hospitales en España 2025 — 2023. Fuente: Marsh.

Como se puede ver en la gráfica, los ataques de ransomware son uno de los principales problemas de seguridad a los que se han enfrentado los hospitales en los últimos años. Este tipo de ataque ha provocado que, en mayor o menor medida, los servicios asistenciales se vieran comprometidos y por lo tanto se viera comprometida la actividad normal del hospital.

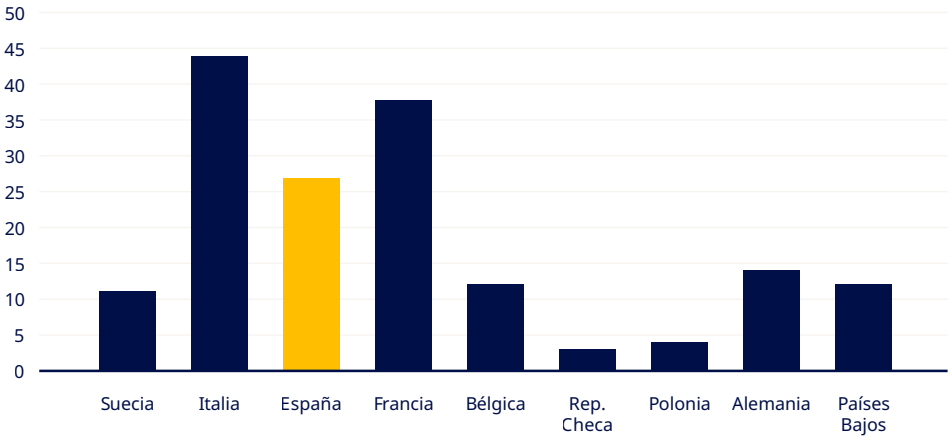


Figura 2: Ataques en hospitales en Europa 2025 — 2023. Fuente: Marsh.

Conforme al panorama internacional la situación que se vislumbra en el sector hospitalario pone de manifiesto que los eventos ciber que se han detectado contra sectores críticos son una realidad.

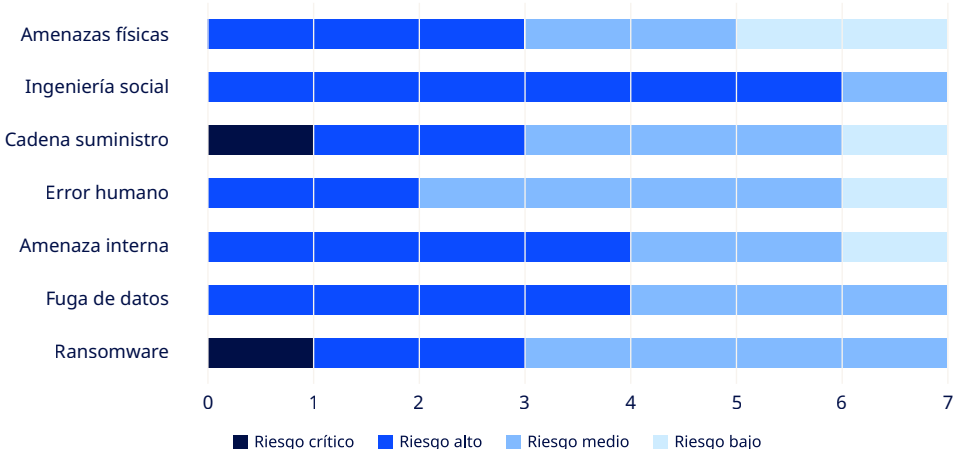


Figura 3: Niveles de riesgo por ataques.

Conforme a la información recopilada, la conclusión a la que llegamos es que las principales amenazas que se perciben son la ingeniería social / phishing, la fuga de datos y las amenazas internas. Asimismo, las amenazas físicas se consideran menos preocupantes que las amenazas digitales, aunque tienen una importancia considerable.

6.2. Casos de estudio y ejemplos prácticos de gestión de riesgos

A continuación, se describen los escenarios que pueden darse en un hospital y que pueden afectar a los pacientes y personal del hospital, tanto médico como no médico y en algún caso a los fabricantes (dispositivos médicos) se pueden ver afectados.

6.2.1. Ransomware

Escenario de amenaza 1	
Tipo de amenaza	El ransomware es un tipo de malware que cifra los datos y sistemas de una organización, bloqueando el acceso hasta que se pague un rescate. En hospitales, este ataque puede paralizar sistemas críticos, afectar a la atención médica y poner en riesgo la vida de los pacientes. Los atacantes suelen utilizar técnicas como correos electrónicos con archivos adjuntos maliciosos o explotar vulnerabilidades en sistemas sin actualizar para infiltrarse en la red hospitalaria y lanzar el ransomware en los sistemas del hospital.
Activos afectados	Información clínica; Procesos administrativos; Dispositivos médicos conectados a la red; Infraestructura de red y servidores; Personal y pacientes.
Criticidad	Muy alta. La indisponibilidad de sistemas críticos afecta directamente a la seguridad del paciente y la continuidad asistencial. Además, la pérdida o alteración de datos clínicos puede tener consecuencias legales, financieras y reputacionales graves.
Probabilidad	Alta. Los hospitales son objetivos frecuentes de ransomware debido a la sensibilidad de sus datos y la urgencia de sus servicios. La existencia de sistemas sin parchear, la falta de formación del personal y la complejidad de las infraestructuras aumentan la probabilidad de éxito del ataque.
Efectos en cascada	Un ataque exitoso puede provocar la interrupción de múltiples servicios hospitalarios, desde urgencias hasta laboratorios y quirófanos. La pérdida de acceso a datos clínicos puede derivar en errores médicos, retrasos en diagnósticos y tratamientos, y aumento de la mortalidad. Además, puede afectar la confianza pública y la reputación institucional.
Tiempo y esfuerzo de recuperación	La recuperación puede extenderse desde días hasta semanas, dependiendo de la rapidez en la detección, la existencia de copias de seguridad y la capacidad de respuesta del equipo de TI.

Ataque de Ransomware

Acceso inicial
(phishing, acceso remoto vulnerable)

Reconocimiento de Red
(detección de servicios IoT/IoMT)

Propagación
(servidores clínicos,
dispositivos médicos IoT)

Escalado de privilegios
(obtener permisos elevados
en sistemas críticos)

Cifrado de sistemas
(datos clínicos, gestión
hospitalaria, IoT)

Extorsión e impacto
(rescate, interrupción de servicio,
impacto asistencial)



6.2.2. Denegación de Servicio Distribuido (DDoS)

Escenario de amenaza 2	
Tipo de amenaza	Un ataque DDoS (Distributed Denial of Service o Denegación de Servicio Distribuido) consiste en un intento malicioso de alterar el tráfico normal de un servidor, servicio o red, abrumando al objetivo con una inundación de peticiones de tráfico desde Internet.
Activos afectados	Dispositivos médicos conectados a la red; Infraestructura de red y servidores; Personal y pacientes.
Criticidad	Alta. La indisponibilidad de sistemas críticos afecta directamente a la seguridad del paciente y la continuidad asistencial.
Probabilidad	Media. Los hospitales son objetivos frecuentes de grupos “hacktivistas” por su visibilidad mediática y cibercriminales que usan el ataque DDoS como táctica de distracción para ocultar una intrusión más grave.
Efectos en cascada	Un ataque exitoso puede provocar la interrupción de múltiples servicios hospitalarios, desde urgencias hasta laboratorios y quirófanos. La pérdida de acceso a datos clínicos puede derivar en errores médicos, retrasos en diagnósticos y tratamientos, y aumento de la mortalidad. Además, puede afectar la confianza pública y la reputación institucional.
Tiempo y esfuerzo de recuperación	Generalmente de minutos a horas. A diferencia del ransomware, un DDoS suele durar lo que dura el ataque activo. Supone un esfuerzo alto durante el ataque (monitoreo en tiempo real, contacto con proveedores de internet, filtrado de IPs) que se extenderá con la duración del ataque.



Fases de un ataque de Denegación de Servicio Distribuido DDoS

Fase 1
"Acceso a la Red Hospitalaria"

El atacante obtiene acceso inicial a la red interna mediante credenciales robadas, phishing, dispositivos comprometidos o accesos remotos vulnerables.

Fase 2
"Reconocimiento de servicios y activos IoT/IoMT"

Monitores multiparamétricos, ventiladores mecánicos, tablets sanitarias, dispositivos de telemedicina...

Fase 3
"Identificación de Objetivos Vulnerables"

Análisis de la información para localizar equipos con debilidades conocidas, configuraciones inseguras o recursos limitados susceptibles a interrupción.

Fase 4
"Ejecución del Ataque DDoS"

Generación de tráfico excesivo o explotación de vulnerabilidades que provocan agotamiento de recursos, bloqueo del servicio o reinicio de los dispositivos afectados.

Fase 5
"Impacto Operacional"

Interrupción de la disponibilidad de dispositivos médicos conectados y servicios clínicos, afectando la continuidad asistencial y la monitorización de pacientes.

6.2.3. Filtración de datos

Escenario de amenaza 3	
Tipo de amenaza	Una filtración de datos es un incidente de seguridad en el que información confidencial, privada o protegida es accedida y extraída por una persona no autorizada. A diferencia del ransomware (que solo cifra), aquí el objetivo es robar la información para venderla o utilizarla para extorsión.
Activos afectados	Bases de datos de historias clínicas (PHI); Datos de empleados, pacientes y proveedores
Criticidad	Crítico. A diferencia de una caída de servidor (que se arregla), una filtración es irreversible. Una vez el dato es público, no se puede "des-publicar". Viola el RGPD (Reglamento General de Protección de Datos) de forma grave.
Probabilidad	Alto. La filtración de datos afecta directamente a la privacidad del paciente o de los empleados del hospital.
Efectos en cascada	Multas Regulatorias: Sanciones millonarias de la AEPD (Agencia Española de Protección de Datos). Ingeniería Social Secundaria: Los pacientes empiezan a recibir correos estafa muy creíbles porque los estafadores conocen sus datos. Demandas Colectivas: Pacientes demandando al hospital por violación de privacidad. Daño Reputacional: Pérdida de confianza en la institución.
Tiempo y esfuerzo de recuperación	Tiempo Indefinido (años). Aunque el sistema técnico se recupere en semanas, el esfuerzo legal, forense y de notificación a las víctimas dura un tiempo prolongado.

Fases de la Filtración de Datos

1. Compromiso inicial

- Ransomware
- Credenciales comprometidas
- Vulnerabilidades perimetrales
- Phishing
- Accesos remotos inseguros

2. Reconocimiento y descubrimiento

- Sistemas clínicos
- Repositorios
- Bases de datos médicas
- IoMT

3. Acceso a Información sensible

- Historiales
- Diagnósticos
- Imágenes
- Datos personales

4. Exfiltración de Datos

- Canales cifrados
- Nube
- Herramientas remotas

5. Impacto y Consecuencias

- Pérdida confidencialidad
- Incumplimiento normativo
- Daño reputacional
- Sanciones
- Riesgo pacientes



7. Buenas prácticas y recomendaciones

A continuación, se detallan una serie de buenas prácticas basadas en estándares y normas internacionales, cuyo objetivo es proteger los activos de los hospitales. Estas medidas de seguridad, también conocidas como controles, permiten gestionar los riesgos de seguridad. Se pueden clasificar según su naturaleza:

- **Medidas organizativas**[11]**:** Incluyen políticas, procedimientos, herramientas y métodos administrativos, así como acciones para crear y mantener la concienciación en seguridad. Las políticas y procedimientos definen los comportamientos aceptables e inaceptables de los empleados en el entorno laboral y funcionan como normas internas de la organización. Ejemplos son la clasificación de activos, el análisis de riesgos y las auditorías.

- **Medidas técnicas**[12]**:** Se basan en tecnología y software para automatizar procesos de seguridad. Ejemplos de estas medidas son el uso de cortafuegos (firewalls), redes privadas virtuales (VPN), sistemas de detección y prevención de intrusiones (IDS/IPS), escáneres de vulnerabilidades y criptografía, etc.

- **Medidas procedimentales**[13]**:** Constituyen el conjunto de procesos, protocolos y guías operacionales que estructuran cómo el hospital implementa, ejecuta y supervisa los controles de ciberseguridad de forma consistente y repetible. A diferencia de las medidas organizativas (que establecen la gobernanza estratégica) y las medidas técnicas (que proporcionan la tecnología automatizada), las procedimentales son la ejecución cotidiana de las políticas en el entorno operativo del hospital.

Debilidades más señaladas
Cada hospital marcó las 3 debilidades que más le exponen.



11 — ISO/IEC 27001:2022

12 — ISO/IEC 27001:2022

13 — ENS

7.1. Buenas prácticas organizativas

La mayoría de las buenas prácticas pueden aplicarse en el entorno hospitalario, sin embargo, como se detalla a continuación, existen consideraciones específicas que deben tenerse en cuenta al implementarlas[14].

Las medidas organizativas incluyen, entre otras, el modelo de gobernanza de seguridad, las políticas y procedimientos de seguridad, el cumplimiento de estándares y certificaciones, la formación y sensibilización del personal, la gestión de riesgos, las auditorías y evaluaciones, así como las cláusulas contractuales que regulan la seguridad.



14 — IEC 62443-3-3

Categoría	Buena Práctica
Modelo de gobernanza de seguridad[15]	**1. Designación de un Responsable de Seguridad de la Información:** Asignar un líder claro y responsable de la seguridad de la información CISO (Chief Information Security Officer) que coordine las políticas, estrategias y respuestas ante incidentes, garantizando la integración de la seguridad en todas las áreas del hospital. **2. Creación de comités de seguridad multidisciplinares:** Formar grupos con representantes de áreas clínicas, técnicas y administrativas para abordar la seguridad de forma integral, facilitando la comunicación, coordinación y toma de decisiones conjuntas sobre riesgos y controles. **3. Integración de la seguridad en la estrategia global del hospital:** Incorporar la seguridad de la información como un componente esencial en la planificación estratégica institucional, asegurando recursos, apoyo de la alta dirección y alineación con los objetivos organizacionales a largo plazo.
Políticas y procedimientos de seguridad[16]	**4. Desarrollo y actualización de políticas claras y comprensibles:** Elaborar documentos normativos que definan comportamientos, procedimientos y responsabilidades, revisarlos periódicamente para adaptarse a nuevas amenazas, tecnologías y cambios regulatorios. **5. Comunicación y difusión efectiva de políticas a todo el personal:** Implementar campañas de comunicación y formación para asegurar que todo el personal conozca, comprenda y aplique las políticas de seguridad, facilitando el acceso a la documentación y promoviendo una cultura de seguridad.
Estándares y certificaciones[17]	**6. Implementación de estándares internacionales y normativas nacionales:** Adoptar marcos reconocidos como ISO 27001, ISO 22301, ENS y NIS 2 para estructurar la gestión de seguridad, cumplir con requisitos legales y mejorar la confianza de pacientes y terceros.
Formación y sensibilización[18]	**7. Programas continuos de formación** Implementar formación constante para todo el personal en seguridad de la información y protección de datos. **8. Cultura de seguridad** Promover la concienciación sobre amenazas como phishing, ingeniería social y manejo seguro de dispositivos conectados.
Gestión de riesgos[19]	**9. Evaluaciones periódicas** Realizar análisis de riesgos que consideren amenazas tecnológicas, personal y terceros. **10. Enfoque integral** Identificar, analizar, mitigar y monitorizar riesgos relacionados con activos críticos, especialmente dispositivos IoT y sistemas conectados.

15 — ISO/IEC 27001:2022
16 — ENS
17 — ISO/IEC 27001:2022
18 — NIS2
19 — ISO/IEC 27001:2022

Categoría	Buena Práctica
Auditorías y evaluaciones[20]	**11. Auditorías regulares** Evaluar la efectividad de políticas, controles y medidas técnicas de seguridad. **12. Pruebas específicas** Realizar pruebas de penetración y evaluaciones de vulnerabilidades en sistemas y dispositivos inteligentes. **13. Mejora continua** Utilizar resultados de auditorías para corregir deficiencias y adaptarse a nuevas amenazas.
Cláusulas contractuales que regulan la seguridad[21]	**14. Requisitos contractuales** Incluir cláusulas que establezcan mínimos de seguridad y protección de datos en contratos con proveedores y terceros. **15. Responsabilidades claras** Definir obligaciones en caso de incidentes, incluyendo notificación y cooperación. **16. Seguridad en IoT** Incorporar cláusulas que regulen la gestión de riesgos en dispositivos, protocolos de comunicación y servicios IoT durante todo su ciclo de vida.



20 — ENS

21 — RGPD

7.2. Buenas prácticas técnicas

En el contexto de los hospitales, la implementación de medidas técnicas robustas es fundamental para proteger los sistemas, dispositivos y datos críticos frente a las crecientes amenazas ciber. Estas medidas buscan mitigar riesgos específicos asociados a la interconexión de dispositivos médicos, sistemas de información y redes hospitalarias, garantizando la confidencialidad, integridad y disponibilidad de la información, así como la seguridad operativa. A continuación, se presentan las principales buenas prácticas técnicas recomendadas, junto con las amenazas más significativas que cada una ayuda a mitigar.

Categoría	Buena Práctica Técnica	Amenazas Mitigada
Seguridad de Redes	**1. Segmentación de red**[22] Separar redes clínicas, administrativas y de equipos conectados (IoT, etc) para limitar el alcance de un ataque.	• Propagación de ataques; • Accesos no autorizados; • Malware; • Ransomware.
	2. Monitorización y detección de intrusiones[23] Implementar sistemas IDS/IPS para detectar actividades sospechosas.	• Accesos no autorizados; • Ataques de denegación de servicio (DDoS).
Gestión de Dispositivos	**3. Gestión de configuración y parches** Mantener actualizados los dispositivos y sistemas con parches de seguridad.	• Malware; • Explotación; • Vulnerabilidades.
	4. Control de accesos Uso de autenticación multifactor y control de accesos.	• Accesos no autorizados; • Robo de identidad.
Protección de Datos	**5. Cifrado de datos en tránsito y reposo** Proteger la confidencialidad e integridad de la información.	• Interceptación de datos; • Manipulación de información; • Fugas de datos.
	6. Copias de seguridad y recuperación Implementar backups regulares y planes de recuperación ante desastres.	• Pérdida de datos; • Ransomware; • Fallos de sistema.
Seguridad en IoT	**7. Seguridad integrada en dispositivos IoT** Adoptar prácticas de desarrollo seguro y testeo de dispositivos exhaustivas.	• Vulnerabilidades en dispositivos; • Ataques a dispositivos médicos; • Manipulación de datos.

22 — IEC 62443-3-2

23 — ENS

7.3. Buenas prácticas procedimentales

Las medidas procedimentales permiten llevar a la práctica las políticas organizativas y respaldan la implementación de controles técnicos.

Estos procedimientos son críticos para garantizar que las políticas no se queden en documentos y que la tecnología se use de forma coherente.

Buena Práctica	Buenas Prácticas Procedimentales	Amenaza mitigada
Gestión de Accesos y Control de Identidades[24]	**1.** Implementación del principio de menor privilegio y autenticación multifactor. Requiere auditorías periódicas de permisos para personal sanitario, administrativo y proveedores externos que acceden a los historiales clínicos y dispositivos médicos conectados.	• Acceso no autorizado; • Robo de identidad y credenciales; • Acceso privilegiado sin supervisión.
Gestión de Cambios y Actualizaciones[25]	**2.** Cambios menores (parches) requieren documentación (qué, por qué, cuándo, quién), pruebas en ambiente idéntico a producción y disponer de un inventario de activos conectados a la red.	• Malware; • Manipulación de información.
Respuesta a Incidentes y Continuidad Asistencial	**3.** Diseño, prueba y ejecución de protocolos de actuación ante crisis ciber, incluye simulacros de procedimientos operativos automáticos y manuales, el triaje de sistemas afectados, la contención de dispositivos IoMT y la recuperación progresiva basada en la criticidad clínica para garantizar que la atención al paciente no se interrumpa.	• Phishing; • Incumplimiento normativo.
Auditoría, Capacitación y Verificación Continua	**4.** Formación para todo personal con contenido adaptado por rol (RGPD, phishing, protección datos clínicos). Simulacros de phishing y entrenamiento personalizado	• Vulnerabilidades en dispositivos; • Ataques a dispositivos médicos; • Manipulación de datos.
Copias de Seguridad, Gestión de Proveedores y Ciclo de Vida de Datos	**5.** Verificación periódica de la integridad de los backups. Evaluación y auditoría continua de terceros. Procedimientos de creación, clasificación, almacenamiento seguro, retención legal y la destrucción certificada de la información.	• Pérdida total de datos; • Corrupción de backups; • Vulnerabilidades en dispositivos software de proveedores; • Proveedores que sufren incidentes sin notificar al hospital.

24 — ISO 27001

25 — ISO 27001

8. Gestión de Crisis

Estamos asistiendo a un panorama en el que el número y la tipología de ataques e incidentes que sufren los hospitales aumentan año a año, al igual que el impacto de crisis no necesariamente digitales, como la COVID-19 o el apagón. En consecuencia, desde el punto de vista asistencial, los servicios prestados se ven afectados, con el consiguiente impacto tanto a nivel reputacional como operativo.

Ante este panorama, la cuestión ya no es si un evento me afectará, sino cuándo se dará el siguiente evento y qué medidas previas se han tomado para estar preparados ante eventos digitales o físicos que pueden afectar a nuestro sistema asistencial. Por ello, cuando un hospital se vea afectado en sus sistemas de información o en la operación clínica, debe contar con una gestión de crisis que permita minimizar el impacto asistencial, proteger a los pacientes y recuperar la operatividad en el menor tiempo posible. Cada centro debe adaptar esta gestión a su realidad, pero como referencia general, una gestión de crisis básica debería contemplar las siguientes fases:

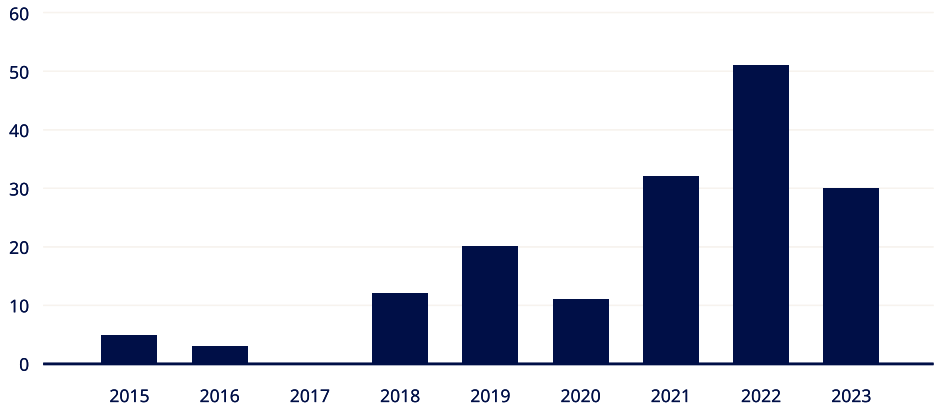


Figura 4: Ataques ciber en Europa a lo largo de los anõs 2015 — 2023.

Preparación

La gestión efectiva de una crisis, comienza mucho antes de que ocurra el incidente o el evento. Durante la fase de preparación, el hospital debe constituir un equipo de crisis multidisciplinar con representación clara de TI/ciberseguridad, ingeniería hospitalaria, dirección facultativa, dirección general y comunicación. Este equipo debe estar entrenado y disponible para una activación inmediata, con roles definidos que aseguren una coordinación sin ambigüedades: un responsable único de coordinación durante la crisis; un director clínico que garantice la continuidad asistencial, priorizando servicios críticos como urgencias, UCI y quirófanos; un director de sistemas encargado de dirigir la respuesta ante caídas del sistema, ciberataques o fallos de telecomunicaciones; un director de comunicación que gestione tanto la información interna como externa; y un director de operaciones encargado de gestionar la infraestructura del edificio, incluyendo mantenimiento, seguridad física, suministros de agua, luz, gases medicinales y logística.

Detección

La detección eficaz comienza con el seguimiento continuo del entorno digital, mediante herramientas como un SIEM, que correlacionan eventos de seguridad, detectan comportamientos anómalos y generan alertas ante patrones sospechosos, como tráfico inusual, múltiples intentos de inicio de sesión fallidos o comunicaciones hacia direcciones externas no autorizadas. Sin embargo, la detección no es puramente tecnológica: el personal clínico, administrativo y de TI puede reportar indicadores tempranos de un incidente, como accesos inusuales a historias clínicas, sistemas que responden lentamente, mensajes de rescate o equipos médicos sin conectividad.

El hospital debe mantener canales claros para el reporte de anomalías de cualquier tipo, ya sean lógicas o físicas, que, llegado el momento, pueden afectar a los servicios prestados, y fomentar una cultura en la que cualquier empleado se sienta autorizado para alertar al equipo de seguridad sin miedo a represalias.

Contención

Una vez confirmado el incidente, el objetivo inmediato es impedir su propagación y proteger la continuidad de la operación clínica. En caso de un ataque informático, la contención comienza con el aislamiento técnico de los sistemas afectados, desconexión de red si es necesario, cierre de accesos remotos, bloqueo de cuentas comprometidas y, en casos graves, apagado del equipamiento infectado para evitar que el malware se replique hacia otras áreas del hospital.

La comunicación interna debe ser rápida y clara: antes de una hora, todo el personal debe saber que hay un incidente, cuáles son los servicios afectados, qué instrucciones seguir y a quién dirigirse con dudas, evitando así pánico, rumores o decisiones descoordinadas.

El responsable único de crisis coordina con las autoridades competentes según la gravedad: si el incidente afecta a datos clínicos o se considera grave, el CCN-CERT (Centro Criptológico Nacional) debe ser notificado dentro de 24 horas, y la AEPD (Agencia Española de Protección de Datos) dentro de 72 horas si hay una brecha de datos personales.

La comunicación externa también es crítica: un mensaje coordinado desde las áreas Legal, Comunicación, Ingeniería y Ciberseguridad se dirige a pacientes y ciudadanos si es necesario, explicando qué pasó, qué datos pueden estar afectados, qué medidas se están tomando y qué pueden hacer los pacientes, manteniendo la confianza en la institución y evitando la desinformación mediática.

Análisis

Tras superar una crisis, y una vez restablecidos los sistemas y los servicios, se realiza el análisis posterior al incidente/evento: una reunión en la que participan el comité definido anteriormente y otros grupos de interés clave. En esta sesión se analiza la cronología completa del incidente, qué salió bien (detección rápida, equipo coordinado) y qué falló (vulnerabilidad no parcheada, procedimiento manual incompleto, tardanza en la notificación a autoridades, sistemas auxiliares sin capacidad suficiente para proporcionar energía, falta de dimensionamiento de la infraestructura, etc.).

El resultado es un documento formal de lecciones aprendidas, identificación de gaps en procesos técnicos, organizativos o de coordinación, y plan de mejora: actualización de procedimientos de contención, refuerzo de seguridad en áreas vulnerables, revisión de planes de continuidad, capacitación adicional del personal y cambios en la arquitectura si es necesario.

Fases Gestión de Crisis

1. Preparación
Protocolos, defensas y formación

2. Detección
Monitorización y alertas (SOC)

3. Contención
Aislamiento de red y mitigación

4. Análisis
Forense, lecciones y mejora continua

Este enfoque no sustituye a un plan formal de gestión de crisis o continuidad asistencial, pero proporciona un marco básico que permite a los hospitales responder de forma estructurada ante un incidente y avanzar hacia modelos de resiliencia digital más maduros.



9. Resultado del Análisis

Se ha llevado a cabo una serie de entrevistas personales y encuestas que abarcan todos los aspectos tratados en este informe, los resultados obtenidos revelan grandes diferencias entre los centros sanitarios respecto a la madurez de seguridad, centros sanitarios con un nivel de madurez alto, coexisten con centros con bajo nivel que no tienen unas medidas mínimas para afrontar posibles eventos, que no disponen de personal especializado, inventarios manuales e inventarios descontrolados de proveedores.

Existe una percepción de un alto riesgo en la gestión de activos, especialmente en:

- Gestión de dispositivos IoMT/OT.
- Acceso remoto de proveedores.
- Equipamiento médico sin medidas de seguridad “security by design”.
- Formación insuficiente del personal.
- Ausencia de simulacros en ciberataques.

Las tres debilidades más críticas son:

- Obsolescencia tecnológica y falta de presupuesto: equipos médicos y servidores antiguos, sin soporte del fabricante o sin actualizaciones de seguridad.
- Factor humano: baja concienciación del personal clínico y no clínico frente a phishing e ingeniería social.
- Recursos insuficientes: equipos de TI saturados y ausencia de un responsable dedicado (o funciones formalizadas) de ciberseguridad.

Estas debilidades reflejan ausencia de gobernanza integrada: los centros menos maduros carecen simultáneamente de liderazgo ejecutivo comprometido, comités multidisciplinares coordinados y presupuesto dedicado, mientras que centros avanzados han invertido en la definición de roles y responsabilidades, así como identificar, equipos coordinados y formación obligatoria.

El hallazgo más alarmante es la deficiente preparación ante incidentes: menos del 50% ha realizado simulacros recientes de ciberataques; solo una minoría dispone de protocolos clínicos claros, procedimientos manuales documentados, comités de crisis formales o sistemas centralizados de logs. Ante una crisis real, estos hospitales improvisarían la respuesta, causando caos organizativo y no cumplir con la obligación de notificaciones conforme a la legislación. Adicionalmente, el acceso remoto no controlado de proveedores a sistemas críticos mediante VPN genéricas sin auditoría ni control de accesos representa un vector de ataque en la cadena de suministro con un riesgo extremadamente elevado.

10. Conclusiones

Los hospitales españoles operan con sistemas ciberfísicos altamente complejos e interdependientes, con miles de activos digitales conectados distribuidos entre infraestructuras críticas, dispositivos médicos, sistemas de información clínica y personal.

Esta arquitectura, necesaria para garantizar la prestación asistencial 24/7, genera dependencias que ante un incidente pueden producir efectos en cascada comprometiendo múltiples servicios simultáneamente. Sin embargo, existen disparidades significativas en los niveles de modernización, inversión y madurez operativa entre centros, lo que condiciona directamente la capacidad de detección, contención y recuperación ante ataques ciberataques, fallos técnicos o eventos externos. La resiliencia del sistema sanitario depende de mitigar las brechas mediante una inversión coordinada en infraestructura, tecnología y procedimientos documentados.

La digitalización del sector, impulsada por estrategias como la Salud Digital del SNS, ha convertido la tecnología en elemento estructural de la prestación asistencial, incrementando exponencialmente la exposición a amenazas ciber (ransomware, phishing, filtraciones de datos) y la dependencia de sistemas, redes, energía y servicios externos. El sector sanitario es objetivo prioritario de ciberdelincuentes y actores estatales, siendo la combinación de infraestructuras críticas, datos clínicos sensibles regulados por RGPD, urgencia operativa para restaurar servicios y sistemas legacy sin parchear lo que lo hace particularmente vulnerable. El impacto no es únicamente económico o reputacional: puede traducirse directamente en daño a pacientes, retrasos en diagnósticos y aumento de mortalidad.

En este contexto, los marcos normativos aplicables (RGPD, NIS2—obligatoria 2026, ENS, LPIC, ISO 27001, IEC 62443) se han vuelto más exigentes y multidimensionales, con sanciones significativas por incumplimiento. Sin embargo, la resiliencia no depende únicamente de cumplimiento normativo o inversión tecnológica, sino de una transformación integrada que combine seguridad física y digital, liderazgo ejecutivo comprometido, cultura organizativa madura, equipos multidisciplinares entrenados y procedimientos operativos documentados. Los hospitales con mayor resiliencia no son los de mayor presupuesto, sino aquellos que han desarrollado una visión integrada del riesgo, coordinación entre dominios (clínica, TI, infraestructura) y capacidad comprobada de operar en modo de contingencia.

Anexos | Normativa

A continuación, se identifica la normativa utilizada o referenciada durante el análisis realizado.

Normativa	Explicación normativa	Control	Descripción control
ISO/IEC 27001:2022	Framework internacional de gestión de seguridad de información. Proporciona requisitos y directrices para establecer, implementar, mantener y mejorar un SGSI. Certificable externamente.	A.5 Gobernanza	Política SGSI, roles, responsabilidades, comités de seguridad, supervisión dirección.
		A.6 Gestión de Recursos	Las personas son activos críticos que requieren competencia, concienciación y supervisión formal.
		A.8 Clasificación Información	Datos clínicos = CRÍTICOS; requieren cifrado, control acceso rol-based, auditoría completa.
		A.9 Control Acceso	Control de acceso de usuarios; facturas, nóminas, datos financieros requieren MFA, auditoría.
		A.9.2 Control de Acceso de Usuario	Solicitud documentada, verificación necesidad, aprobación supervisor, asignación PAM, MFA obligatorio.
		A.12.1 Gestión Riesgos	Identificación, análisis, evaluación, tratamiento, seguimiento; anual mínimo.
		A.14 Procesos Soporte Técnico	Mantenimiento, patching, gestión cambios deben estar documentados, controlados, auditados.
		A.16. Equipo Crisis Multidisciplinar	Roles definidos: CISO, CTO, Director Clínico, Comunicación; reuniones coordinadas.
		A.16.1 Comunicación Interna	Personal informado: estado incidente, instrucciones, prohibiciones de desconexión equipos.
		A.16.12 Post-Mortem Formal	Reunión 1-2 semanas post-crisis; documentación; distribución learnings a todo hospital.
		A.18. Conformidad Estándares	Hospital evalúa cumplimiento ISO 27001, IEC 62443, ENS, RGPD, NIS2 anualmente.

Normativa	Explicación normativa	Control	Descripción control
RGPD (UE 2016/679)	Reglamento General de Protección de Datos. Obligatorio UE. Protege derechos individuos respecto tratamiento datos personales.	Art. 4(1). Interesados	Pacientes = sujetos de derechos; sus datos requieren máxima protección conforme a Art. 5 y Art. 32.
		Art. 28. Cláusulas Contractuales	Contratos procesadores incluyen: confidencialidad, seguridad, notificación brechas, auditoría.
ENS (Real Decreto 311/2022)	Esquema Nacional de Seguridad. Obligatorio España para administraciones públicas.	C.1.1.1. Políticas Formales	Documentos aprobados dirección; comunicados; entendidos; cumplidos; revisados anualmente.
		C.1.3. Auditorías	Evaluación cumplimiento seguridad anual; seguimiento hallazgos; mejora continua.
		C.4.1.1. SIEM 24/7	IDS/IPS monitoreo continuo; alertas anomalías; correlación eventos; retención logs 6+ meses.
		C.4.2. Coordinación Única	Un responsable crisis; autoridad sobre todos los equipos; escaladas claras.
		C.4.2, NIS2 Art. 23. Notificación Autoridades	CCNS <24h incidente grave; AEPD <72h si datos afectados; CNPIC si operador esencial.
		C.5.1. Modo Degradado	Procedimientos manuales documentados; personal entrenado; testing anual simulacros.
AEPD	Agencia Española Protección Datos. Autoridad española supervisión RGPD. Impone multas (ejemplos: €500K-€20M). Publica guías sector sanitario.	Guía Sector Sanitario	Personal debe conocer obligaciones RGPD, especialmente respecto a acceso controlado a historias clínicas

Normativa	Explicación normativa	Control	Descripción control
Ley 41/2002 (España)	Ley Autonomía del Paciente. Derecho español sobre derechos información, consentimiento, privacidad.	Derechos Pacientes	Información, consentimiento informado, privacidad y acceso a historia clínica como derechos fundamentales
IEC 62443-3-3	Estándar internacional ciberseguridad sistemas de control industriales (OT). Define niveles madurez SL 1-4. Aplicable SCADA/PLC hospitales.	Consideraciones Específicas	Hospitales smart tienen SCADA/PLC; requieren aislamiento red, failover automático
		Segmentación OT (IEC 62443-3-2)	Zone-DMZ (externos), Zone-IT (servidores), Zone-OT (SCADA/PLC); firewalls entre zonas
ISO/IEC 27035:2016	Estándar gestión incidentes seguridad información. Define 7 fases: preparación, detección, análisis, contención, investigación, remediación, post-incident.	Medidas Procedimentales	Procesos documentados, protocolos operacionales, ejecución disciplinada
NIS2 (Directiva UE 2022/2555)	Directiva Redes e Información (segunda versión). Obligatoria 2026. Sanidad = operador esencial. Multas €10M o 2% facturación.	Art. 19 Capacitación Obligatoria	Programa anual para todos empleados; contenido adaptado rol (clínico, TI, admin)
		Art. 23 Notificación Autoridades	CCNS <24h incidente grave AEPD <72h si datos afectados CNPIC si operador esencial

Macrodominio

Infraestructura física digitalizada

Nombre activo	**Sistemas eléctricos y de energía digitalizada**
Descripción	Infraestructura eléctrica crítica monitorizada y gestionada digitalmente que suministra energía a sistemas clínicos, TI y OT.
Elementos que integran este tipo de activos	CT MT/BT; QGBT y subcuadros; SAI/UPS; grupos electrógenos; medidores; relés programables; SCADA/BMS de energía.
Cantidad típica / Fabricantes	1–2 CT; 1 QGBT + subcuadros; 4–10 UPS centrales + UPS locales; 1–3 grupos. Fabricantes orientativos: Schneider, Eaton, Vertiv, Socomec, Riello; Caterpillar, Cummins.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001/27002; IEC 62443; normativa BT y continuidad.
Criticidad	Muy alta.
Dependencias clave	Combustible; red OT; BMS/SCADA; climatización CPD; mantenimiento.
Principales amenazas	Acceso no autorizado al SCADA/BMS; manipulación de parámetros; malware/ransomware; DoS sobre monitorización.
Principales vulnerabilidades	Red OT poco segmentada; credenciales por defecto; firmware no actualizado; accesos remotos de fabricante.
Escenarios de riesgo	Caída coordinada de UPS y fallo de grupo; disparos injustificados; pérdida de visibilidad del estado eléctrico.
Recomendaciones	Segmentación OT; hardening; control de accesos privilegiados; actualización planificada; monitorización continua; pruebas periódicas de contingencia.

Macrodominio

Infraestructura física digitalizada

Nombre activo	**Sistemas de climatización (HVAC) y control ambiental**
Descripción	Tratamiento de aire y control ambiental digitalizado crítico para quirófanos, UCI, aislamiento, laboratorios y esterilización.
Elementos que integran este tipo de activos	UTAs con PLC/DDC; enfriadoras; calderas; sensores de temperatura, humedad, presión y CO_2; filtración HEPA; BMS.
Cantidad típica / Fabricantes	20–40 UTAs; 2–4 enfriadoras; 2–3 calderas; cientos de sensores. Fabricantes orientativos: Siemens, Schneider, Honeywell, JCI, Carrier, Trane, Daikin.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; IEC 62443; normas de calidad de aire / salas limpias.
Criticidad	Muy alta.
Dependencias clave	Energía; BMS; red OT; sensores; zonas críticas.
Principales amenazas	Acceso remoto indebido; cambio de consignas; apagado en zonas críticas; manipulación de alarmas.
Principales vulnerabilidades	Protocolos sin cifrado; cuentas genéricas; exposición del BMS; cambios no trazados.
Escenarios de riesgo	Pérdida de sobrepresión en quirófanos; fallo en climatización de UCI; condiciones fuera de rango que afectan a pacientes o equipos.
Recomendaciones	Segregar BMS; restringir accesos remotos; gestión de cambios; validación periódica de condiciones críticas.

Macrodominio

Infraestructura física digitalizada

Nombre activo	**Sistemas de agua y fluidos con control digital**
Descripción	Sistemas de tratamiento y distribución de agua general y purificada controlados digitalmente para diálisis, esterilización y otros usos clínicos.
Elementos que integran este tipo de activos	Planta principal; sistema de agua purificada; PLC; HMI; sensores de nivel, caudal, presión y temperatura; integración con BMS/SCADA.
Cantidad típica / Fabricantes	1 planta principal; 1 sistema de agua purificada; cientos de señales. Fabricantes orientativos: Veolia, Culligan, BWT, Fresenius, Baxter, Nipro.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; IEC 62443; normativa sectorial de agua sanitaria y diálisis.
Criticidad	Muy alta.
Dependencias clave	Energía; red OT; proveedor; BMS; diálisis/esterilización.
Principales amenazas	Manipulación remota de parámetros; desactivación de alarmas; DoS sobre PLC/HMI.
Principales vulnerabilidades	Accesos remotos de proveedor; falta de segregación; autenticación débil; registro limitado.
Escenarios de riesgo	Agua no conforme en diálisis; indisponibilidad de esterilización; pérdida de visibilidad de alarmas críticas.
Recomendaciones	Control estricto de accesos remotos; segmentación de red de planta; validación periódica; plan de continuidad.

Macrodominio

Infraestructura física digitalizada

Nombre activo	**Sistemas de gases medicinales con gestión digital**
Descripción	Redes de oxígeno, aire medicinal, vacío y otros gases críticos con supervisión y alarmas digitalizadas.
Elementos que integran este tipo de activos	Centrales de gases; compresores; bombas de vacío; vaporizadores; PLC; paneles de alarma; transductores; integración con BMS.
Cantidad típica / Fabricantes	Miles de puntos terminales; 1 central; múltiples paneles. Fabricantes orientativos: Linde, Air Liquide, Gasmedi, MGS, Amico, Dräger.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; IEC 62443; normativa sectorial de gases medicinales.
Criticidad	Muy alta.
Dependencias clave	Energía; red OT; BMS; mantenimiento; presión/caudal.
Principales amenazas	Interferencia en señales; desactivación de alarmas; fallos en PLC.
Principales vulnerabilidades	Dependencia de un único PLC; falta de respaldo manual; documentación limitada.
Escenarios de riesgo	Lecturas incorrectas de presión; alarmas no activadas; pérdida de gas en quirófanos/UCI.
Recomendaciones	Redundancia en supervisión; auditorías de PLC; pruebas de alarmas; procedimientos manuales.

Macrodominio

Infraestructura física digitalizada

Nombre activo	**Sistemas de seguridad física digital**
Descripción	Control de accesos, videovigilancia, intrusión e incendios basado en IP y software centralizado.
Elementos que integran este tipo de activos	Lectores y controladoras; CCTV IP; NVR/VMS; centrales de intrusión e incendios; detectores; módulos.
Cantidad típica / Fabricantes	500–1.500 cámaras; miles de credenciales y puntos de acceso. Fabricantes orienta-tivos: LenelS2, Bosch, HID, Honeywell, Axis, Genetec, Milestone.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; RGPD; IEC 62443 si se integra en OT.
Criticidad	Alta.
Dependencias clave	Red TI; identidad; CPD; seguridad perimetral.
Principales amenazas	Toma de control de VMS/CCTV; apertura remota de puertas; borrado de logs; desactivación de alarmas.
Principales vulnerabilidades	Firmware obsoleto; credenciales débiles; mala gestión de usuarios; redes no segmentadas.
Escenarios de riesgo	Intrusión física en CPD/farmacia; pérdida de evidencias; filtración de imágenes sensibles.
Recomendaciones	Segregar redes de seguridad; IAM estricto; actualización de firmware; correlación con SIEM; pruebas periódicas.

Macrodominio

Infraestructura física digitalizada

Nombre activo	**Comunicaciones internas digitalizadas**
Descripción	Sistemas internos de comunicación (VoIP, megafonía, llamada paciente-enfermera) que soportan coordinación clínica y operativa.
Elementos que integran este tipo de activos	PBX local/cloud; terminales IP; megafonía zonificada; servidores de audio; llamada paciente-enfermera; integración DECT/smartphones.
Cantidad típica / Fabricantes	200–400 teléfonos IP; megafonía por zonas; llamada enfermera por cama. Fabricantes orientativos: Cisco, Avaya, Mitel, Bosch, Ascom, Rauland.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; RGPD si hay grabación.
Criticidad	Alta.
Dependencias clave	Red IP; energía; PBX; QoS; dispositivos móviles.
Principales amenazas	DoS/DDoS sobre PBX; manipulación de anuncios; caída de llamada enfermera; interceptación.
Principales vulnerabilidades	PBX expuesta; falta de redundancia; configuración por defecto; dependencia de una sola red.
Escenarios de riesgo	Descoordinación ante emergencias; pacientes sin poder avisar; emisión de órdenes falsas.
Recomendaciones	Diseño redundante; separación de tráfico crítico; pruebas periódicas; QoS y seguridad PBX.

Macrodominio

Infraestructura física digitalizada

Nombre activo	**BMS / SCADA centralizado**
Descripción	Plataforma de control central de instalaciones técnicas y sistemas OT del edificio.
Elementos que integran este tipo de activos	Servidores BMS/SCADA; HMIs; gateways; bases de datos; integraciones con HVAC, energía, agua, gases y seguridad.
Cantidad típica / Fabricantes	1 plataforma central + estaciones de operación. Fabricantes orientativos: Siemens Desigo, Schneider EcoStruxure, Honeywell EBI, Metasys.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; IEC 62443.
Criticidad	Muy alta.
Dependencias clave	Red OT; energía; operadores; sistemas técnicos.
Principales amenazas	Acceso indebido; manipulación centralizada; ransomware; pérdida de supervisión.
Principales vulnerabilidades	Exposición de consolas; credenciales compartidas; accesos remotos; falta de segmentación.
Escenarios de riesgo	Alteración simultánea de varios sistemas técnicos desde la plataforma central.
Recomendaciones	Aislamiento OT; hardening; bastionado de accesos; revisión de integraciones; monitorización.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Monitorización y soporte vital (IoMT)**
Descripción	Dispositivos que monitorizan constantes y proporcionan soporte vital en UCI, quirófanos y áreas críticas.
Elementos que integran este tipo de activos	Monitores multiparamétricos; telemetría; ventiladores; anestesia; incubadoras; centrales de monitorización; módulos de red.
Cantidad típica / Fabricantes	Orden de magnitud: 10–15 dispositivos conectados por cama; cientos en hospitales medianos/grandes. Fabricantes orientativos: Philips, GE, Dräger, Mindray, Nihon Kohden, Hamilton.
Normativa digital aplicable	MDR; RGPD; ENS (RD 311/2022); NIS2; normativa sectorial de producto sanitario.
Criticidad	Muy alta.
Dependencias clave	Red clínica; HCE; energía; central de monitorización; mantenimiento; fabricante.
Principales amenazas	Ransomware/malware; manipulación de alarmas/parámetros; pérdida de conectividad; explotación de OS embebidos.
Principales vulnerabilidades	OS obsoletos; sin parcheo; contraseñas por defecto; protocolos propietarios sin cifrado; mala segmentación.
Escenarios de riesgo	Monitores desconectados en UCI; modificación de umbrales; indisponibilidad en quirófanos.
Recomendaciones	Segmentación clínica; inventario; ciclo de vida; pruebas de interoperabilidad; requisitos de seguridad en compras.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Bombas y sistemas de infusión**
Descripción	Equipos que administran medicación y fluidos intravenosos de forma controlada y programable.
Elementos que integran este tipo de activos	Bombas volumétricas; de jeringa; PCA; estaciones de acoplamiento; conectividad Ethernet/WiFi; software central.
Cantidad típica / Fabricantes	800–1.500 bombas en hospital de 400 camas (orientativo). Fabricantes orientativos: Baxter, B. Braun, Fresenius Kabi, BD, ICU Medical, Medtronic.
Normativa digital aplicable	MDR; RGPD; ENS (RD 311/2022); NIS2; normativa sectorial de producto sanitario.
Criticidad	Muy alta.
Dependencias clave	Red IoMT; librerías de medicación; software central; personal clínico.
Principales amenazas	Manipulación de librerías; cambio de parámetros; DoS al sistema central; accesos no autorizados.
Principales vulnerabilidades	Firmware antiguo; librerías no firmadas; autenticación débil; WiFi no segmentado.
Escenarios de riesgo	Dosis incorrectas; caída del sistema central; reprogramación masiva en crisis.
Recomendaciones	Hardening; segmentación IoMT; control de librerías; pruebas tras actualizaciones.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Equipos de imagen médica conectados**
Descripción	Sistemas de diagnóstico por imagen de alta complejidad integrados con RIS/PACS y HCE.
Elementos que integran este tipo de activos	TAC, RMN, RX, mamógrafo, PET/PET-TAC; consolas de adquisición; software propietario; conectividad PACS/HCE.
Cantidad típica / Fabricantes	5–10 macroequipos por hospital de referencia (orientativo). Fabricantes orientativos: Siemens Healthineers, GE Healthcare, Philips.
Normativa digital aplicable	MDR; RGPD; ENS (RD 311/2022); NIS2; normativa sectorial de producto sanitario.
Criticidad	Muy alta.
Dependencias clave	PACS/RIS; almacenamiento; red; energía; consolas; mantenimiento.
Principales amenazas	Ransomware en consolas/PACS; explotación de OS legacy; alteración de imágenes; indisponibilidad.
Principales vulnerabilidades	OS sin soporte; cuentas locales; falta de cifrado; backups no probados.
Escenarios de riesgo	Paralización radiológica; retrasos diagnósticos; desvío de pacientes; pérdida temporal de históricos.
Recomendaciones	Continuidad de imagen; segmentación; actualización planificada; restauración de backups; DICOM seguro.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Equipos de laboratorio clínico conectados**
Descripción	Analizadores automáticos integrados con LIS/HCE para bioquímica, hematología, coagulación, inmunología y microbiología.
Elementos que integran este tipo de activos	Analizadores; tracks de automatización; interfaces LIS; software de control; mantenimiento remoto.
Cantidad típica / Fabricantes	10–20 equipos principales + módulos y 1 track (orientativo). Fabricantes orientativos: Roche, Abbott, Siemens, Beckman Coulter, Sysmex.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; normativa sectorial de laboratorio/IVD.
Criticidad	Muy alta.
Dependencias clave	LIS; red laboratorio; HCE; muestras; soporte remoto.
Principales amenazas	Ransomware en LIS; fallo de interfaces; manipulación de resultados; accesos remotos indebidos.
Principales vulnerabilidades	Legacy; conexiones propietarias; segmentación insuficiente; accesos de tercero sin control.
Escenarios de riesgo	Paralización del laboratorio; retraso diagnóstico; resultados erróneos o no validados.
Recomendaciones	Segregar red laboratorio; controlar accesos remotos; alta disponibilidad LIS; validación post-incidente.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Sistemas quirúrgicos avanzados y robótica**
Descripción	Sistemas de cirugía asistida altamente integrados con imagen y HCE.
Elementos que integran este tipo de activos	Robot quirúrgico; navegación; microscopios robotizados; arcos en C/TAC intraoperatorio; consolas; módulos robóticos.
Cantidad típica / Fabricantes	1 robot + varios sistemas asociados en hospitales de alta complejidad. Fabricantes orientativos: Intuitive, Siemens, GE, Philips, Medtronic, Brainlab, Stryker.
Normativa digital aplicable	MDR; RGPD; ENS (RD 311/2022); NIS2; normativa sectorial de producto sanitario.
Criticidad	Muy alta.
Dependencias clave	Imagen intraoperatoria; energía; red; PACS; personal experto; fabricante.
Principales amenazas	Fallos de software; pérdida de comunicación; manipulación de planificación; indisponibilidad de imagen.
Principales vulnerabilidades	Dependencia de una consola/proveedor; testing limitado; dificultad de actualizar.
Escenarios de riesgo	Suspensión de cirugía robótica; conversión urgente a técnica abierta; cancelación de agenda.
Recomendaciones	Contingencia quirúrgica; pruebas de fallo controlado; coordinación con fabricantes; ciberseguridad en compra/mantenimiento.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Farmacia automatizada y dispensación**
Descripción	Sistemas robotizados y automatizados para almacenamiento, preparación y dispensación de medicamentos.
Elementos que integran este tipo de activos	Robots de dispensación; armarios automatizados; software de farmacoterapia; integración con HCE/prescripción/farmacia.
Cantidad típica / Fabricantes	Variable según tamaño. Fabricantes orientativos: Omnicell, BD Pyxis, Swisslog, Baxter.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; normativa farmacéutica y trazabilidad.
Criticidad	Alta.
Dependencias clave	Prescripción electrónica; red; stock; personal de farmacia.
Principales amenazas	Ransomware; alteración de catálogos/pautas; indisponibilidad de robot; accesos indebidos.
Principales vulnerabilidades	Integración débil con HCE; cuentas compartidas; baja trazabilidad de cambios.
Escenarios de riesgo	Error o retraso en dispensación; imposibilidad de preparación segura; impacto en medicación crítica.
Recomendaciones	Trazabilidad de cambios; IAM; redundancia operativa/manual; pruebas de continuidad; segregación de red.

Macrodominio

Dispositivos médicos y equipamiento clínico

Nombre activo	**Dispositivos IoT no médicos de soporte clínico**
Descripción	Capa IoT de entorno (camas inteligentes, sensores, domótica, cámaras clínicas) que complementa la atención y operación.
Elementos que integran este tipo de activos	Camas inteligentes; sensores ambientales; cámaras IP de uso clínico; actuadores de iluminación/persianas
Cantidad típica / Fabricantes	Cientos o miles de dispositivos. Fabricantes variados integrados con BMS/seguridad.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; ISO 27001; IEC 62443 si se integra en OT.
Criticidad	Media-alta.
Dependencias clave	Red IoT; BMS; apps de enfermería; WiFi.
Principales amenazas	Puerta de entrada; secuestro de cámaras; manipulación de escenas/iluminación; fallos masivos.
Principales vulnerabilidades	Dispositivos low-cost; credenciales por defecto; inventario incompleto; mezcla de redes.
Escenarios de riesgo	Intrusión vía cámara/sensor; fallo de iluminación/control ambiental; exposición de imágenes.
Recomendaciones	Segregar IoT; homologación; inventario; gateways seguros; limitación de datos personales.

Macrodominio

Sistemas de información y datos

Nombre activo	**Historia clínica electrónica (HCE) y sistemas clínicos core**
Descripción	Núcleo de gestión clínica y asistencial del hospital.
Elementos que integran este tipo de activos	HCE; prescripción electrónica; farmacia; admisión; documentación clínica; motores de reglas/alertas.
Cantidad típica / Fabricantes	Variable según tamaño. Proveedores representativos: Oracle Cerner, Epic, sistemas locales/regionales.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Muy alta.
Dependencias clave	IAM; red; CPD; integración; personal clínico.
Principales amenazas	Ransomware; acceso no autorizado; alteración de datos; indisponibilidad de BD o aplicación.
Principales vulnerabilidades	Credenciales débiles; mala segregación; privilegios excesivos; parches incompletos.
Escenarios de riesgo	HCE no accesible; errores de medicación; pérdida de trazabilidad asistencial.
Recomendaciones	IAM fuerte; MFA; segregación; backups probados; alta disponibilidad; control de cambios.

Macrodominio

Sistemas de información y datos

Nombre activo	**Sistemas especializados (PACS/RIS/LIS) y repositorios clínicos**
Descripción	Sistemas que almacenan y gestionan imagen, laboratorio y otros datos diagnósticos y documentales.
Elementos que integran este tipo de activos	PACS; RIS; LIS; repositorios documentales; archivado clínico.
Cantidad típica / Fabricantes	Variable según tamaño y arquitectura.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Muy alta.
Dependencias clave	Almacenamiento; red; HCE; integración; backup.
Principales amenazas	Ransomware; corrupción de datos; indisponibilidad; errores de sincronización.
Principales vulnerabilidades	Backups insuficientes; interfaces frágiles; dependencia de almacenamiento central.
Escenarios de riesgo	No disponibilidad de imagen/lab/documentación; retrasos clínicos y diagnósticos.
Recomendaciones	Continuidad por servicio; recuperación probada; monitorización de integraciones; segmentación.

Macrodominio

Sistemas de información y datos

Nombre activo	**Motores de integración / interoperabilidad**
Descripción	Plataformas que orquestan el intercambio entre sistemas clínicos y externos.
Elementos que integran este tipo de activos	ESB; motores HL7/FHIR; APIs; brokers de mensajería; gateways DICOM; middleware.
Cantidad típica / Fabricantes	1–n motores según arquitectura.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; marcos de interoperabilidad sanitaria.
Criticidad	Muy alta.
Dependencias clave	HCE; PACS; LIS; red; sistemas externos.
Principales amenazas	Manipulación de mensajes; DoS; fallo de colas; credenciales comprometidas.
Principales vulnerabilidades	Falta de validación; APIs expuestas; colas sin resiliencia; cifrado insuficiente.
Escenarios de riesgo	Ruptura de flujos HCE–LIS–PACS; pérdida de órdenes/resultados; errores silenciosos.
Recomendaciones	Alta disponibilidad; monitorización de colas; control de APIs; cifrado; trazabilidad extremo a extremo.

Macrodominio

Sistemas de información y datos

Nombre activo	**Sistemas administrativos y ERP**
Descripción	Aplicaciones de gestión económico-financiera, compras, RR. HH., citación y otros procesos no clínicos.
Elementos que integran este tipo de activos	ERP; facturación; compras; RR. HH.; cita; gestión documental.
Cantidad típica / Fabricantes	Variable según organización.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Alta.
Dependencias clave	Red; identidad; CPD; usuarios administrativos.
Principales amenazas	Ransomware; fraude; acceso no autorizado; manipulación documental.
Principales vulnerabilidades	Contraseñas débiles; macros/phishing; segregación insuficiente de funciones.
Escenarios de riesgo	Parálisis administrativa; errores de facturación/compra; exposición de datos personales.
Recomendaciones	Segregación de funciones; MFA; control documental; formación; auditoría.

Macrodominio

Infraestructura tecnológica

Nombre activo	**Redes de comunicaciones y conectividad**
Descripción	Capa de conectividad del hospital (LAN/WAN/WiFi) sobre la que operan el resto de activos.
Elementos que integran este tipo de activos	Switching; routing; firewalls; WiFi; NAC; enlaces WAN/Internet; segmentación VLAN/VRF.
Cantidad típica / Fabricantes	Cientos de switches/APs según tamaño del hospital.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Muy alta.
Dependencias clave	Energía; CPD; seguridad perimetral; IAM.
Principales amenazas	DoS/DDoS; propagación lateral; accesos indebidos; fallo de controladoras.
Principales vulnerabilidades	Segmentación insuficiente; configuraciones inseguras; single points of failure.
Escenarios de riesgo	Caída del hospital digital por fallo de red; afectación simultánea de HCE, IoMT y BMS.
Recomendaciones	Red por dominios; redundancia; NAC; microsegmentación; monitorización continua.

Macrodominio

Infraestructura tecnológica

Nombre activo	**Centros de datos, virtualización, almacenamiento y backup**
Descripción	Soporte de computación, almacenamiento y recuperación del hospital.
Elementos que integran este tipo de activos	CPD principal y contingencia; virtualización; almacenamiento NAS/SAN; backup; replicación; salas técnicas.
Cantidad típica / Fabricantes	1 CPD principal + contingencia (según tamaño).
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001; ISO 22301.
Criticidad	Muy alta.
Dependencias clave	Energía; climatización; red; backup; personal TI.
Principales amenazas	Ransomware; corrupción de datos; fallo de replicación; sabotaje; indisponibilidad física.
Principales vulnerabilidades	Backups no inmutables; contingencia no probada; segmentación insuficiente.
Escenarios de riesgo	Pérdida total o parcial de servicios hospitalarios; recuperación lenta o incompleta.
Recomendaciones	Backups inmutables; DRP probado; replicación; segregación; protección física y lógica.

Macrodominio

Infraestructura tecnológica

Nombre activo	**Identidad, acceso y servicios de directorio**
Descripción	Gestión de identidades, autenticación y privilegios en sistemas hospitalarios.
Elementos que integran este tipo de activos	AD/LDAP; SSO; MFA; PAM; PKI; gestión de cuentas y perfiles.
Cantidad típica / Fabricantes	Variable según tamaño y arquitectura.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Muy alta.
Dependencias clave	HCE; red; aplicaciones clínicas; personal; proveedores.
Principales amenazas	Robo de credenciales; abuso de privilegios; movimiento lateral.
Principales vulnerabilidades	Cuentas compartidas; MFA incompleto; privilegios excesivos; altas/bajas mal gobernadas.
Escenarios de riesgo	Compromiso masivo de accesos; escalado de privilegios en sistemas críticos.
Recomendaciones	IAM/PAM robusto; MFA; segregación de funciones; recertificación de permisos.

Macrodominio

Infraestructura tecnológica

Nombre activo	**Sistemas de ciberseguridad y monitorización**
Descripción	Capas de protección, detección y respuesta del entorno hospitalario.
Elementos que integran este tipo de activos	Firewalls; IDS/IPS; SIEM; EDR/XDR; NAC; herramientas de vulnerabilidades; consolas SOC.
Cantidad típica / Fabricantes	Variable según arquitectura y madurez.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Alta.
Dependencias clave	Red; logs; identidad; personal técnico.
Principales amenazas	Desactivación de controles; evasión de detección; saturación de logs; compromiso de consola.
Principales vulnerabilidades	Cobertura incompleta; reglas desactualizadas; falta de casos de uso OT/IoMT.
Escenarios de riesgo	Incidente no detectado o detectado demasiado tarde; pérdida de capacidad de respuesta.
Recomendaciones	Cobertura integral; casos de uso clínicos/OT; hardening de consolas; ejercicios de respuesta.

Macrodominio

Personas y procesos

Nombre activo	**Procesos clínicos**
Descripción	Actividades de atención directa al paciente: diagnóstico, tratamiento, medicación y seguimiento.
Elementos que integran este tipo de activos	Protocolos clínicos; HCE; prescripción; dispositivos médicos conectados; registros clínicos.
Cantidad típica / Fabricantes	Variable según hospital y especialidad.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; marcos de seguridad clínica.
Criticidad	Muy alta.
Dependencias clave	HCE; dispositivos; personal sanitario; red; farmacia.
Principales amenazas	Manipulación de datos; errores humanos; indisponibilidad de sistemas; accesos indebidos.
Principales vulnerabilidades	Obsolescencia; mala segmentación; credenciales débiles; formación insuficiente.
Escenarios de riesgo	Diagnósticos erróneos; errores de medicación; indisponibilidad en momentos críticos.
Recomendaciones	Controles de acceso; formación continua; segmentación; auditoría; planes de contingencia.

Macrodominio

Personas y procesos

Nombre activo	**Procesos de soporte técnico**
Descripción	Mantenimiento de infraestructuras, sistemas, seguridad física e incidencias.
Elementos que integran este tipo de activos	Equipos IT/OT; herramientas de monitorización; backup; tickets; mantenimiento; control de accesos físicos.
Cantidad típica / Fabricantes	Variable según hospital.
Normativa digital aplicable	ENS (RD 311/2022); NIS2; ISO 27001.
Criticidad	Alta.
Dependencias clave	CPD; red; OT; proveedores; contratos.
Principales amenazas	Fallos técnicos; accesos indebidos; sabotaje; errores humanos.
Principales vulnerabilidades	Parcheo insuficiente; configuraciones por defecto; monitorización limitada.
Escenarios de riesgo	Caída de sistemas; brechas; interrupción de servicios.
Recomendaciones	Gestión de cambios; parcheo; monitorización; DRP; formación técnica.

Macrodominio

Personas y procesos

Nombre activo	**Personal sanitario**
Descripción	Profesionales que proporcionan atención directa y operan sistemas críticos.
Elementos que integran este tipo de activos	Médicos; enfermería; técnicos; farmacéuticos; accesos clínicos; dispositivos portátiles.
Cantidad típica / Fabricantes	Miles de usuarios según tamaño del hospital.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); normativa sanitaria y protocolos internos.
Criticidad	Muy alta.
Dependencias clave	HCE; IAM; dispositivos; procesos clínicos.
Principales amenazas	Error humano; phishing; uso inadecuado; agotamiento.
Principales vulnerabilidades	Baja concienciación; ausencia de controles; accesos excesivos.
Escenarios de riesgo	Filtración de datos; errores en tratamientos; degradación operativa.
Recomendaciones	Formación y concienciación; IAM; políticas claras; soporte organizativo.

Macrodominio

Personas y procesos

Nombre activo	**Personal técnico y administrativo**
Descripción	Personal de soporte IT/OT, mantenimiento, seguridad y administración.
Elementos que integran este tipo de activos	TI/OT; mantenimiento; seguridad; administración; herramientas de gestión.
Cantidad típica / Fabricantes	Variable según hospital.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); normativa laboral y de seguridad.
Criticidad	Alta.
Dependencias clave	Red; CPD; contratos; sistemas administrativos.
Principales amenazas	Phishing; accesos indebidos; errores operativos; sabotaje.
Principales vulnerabilidades	Formación insuficiente; procedimientos débiles; controles de acceso incompletos.
Escenarios de riesgo	Caídas de sistemas; errores administrativos; exposición de datos.
Recomendaciones	Formación; procedimientos estandarizados; control de accesos; auditoría.

Macrodominio

Interconexión y ecosistema externo

Nombre activo	**Servicios cloud y proveedores críticos**
Descripción	Servicios externos que soportan aplicaciones, respaldo, colaboración, telemedicina, mantenimiento y soporte.
Elementos que integran este tipo de activos	SaaS; IaaS; soporte remoto; MSP/MSSP; almacenamiento cloud; plataformas externas.
Cantidad típica / Fabricantes	Variable según ecosistema del hospital.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; ISO 27001; cláusulas contractuales de seguridad.
Criticidad	Muy alta.
Dependencias clave	Internet/WAN; contratos; IAM; integración; proveedor.
Principales amenazas	Compromiso de tercero; abuso de acceso remoto; indisponibilidad del servicio; fuga de datos.
Principales vulnerabilidades	Dependencia contractual; baja visibilidad; configuraciones inseguras; gobernanza insuficiente de terceros.
Escenarios de riesgo	Caída de servicio cloud crítico; acceso indebido por proveedor; interrupción de soporte remoto seguro.
Recomendaciones	Evaluación de terceros; requisitos contractuales; mínimo privilegio; supervisión de accesos; contingencia multisitio.

Macrodominio

Interconexión y ecosistema externo

Nombre activo	**Sistemas regionales / HCE compartida / receta electrónica**
Descripción	Integraciones con redes autonómicas, nacionales y servicios compartidos del sistema sanitario.
Elementos que integran este tipo de activos	Plataformas HCE compartida; receta electrónica; repositorios regionales; intercambio de imagen y documentos.
Cantidad típica / Fabricantes	Variable según comunidad autónoma y arquitectura regional.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; marcos de interope-rabilidad sanitaria.
Criticidad	Muy alta.
Dependencias clave	Motores de integración; red; sistemas externos; normativa.
Principales amenazas	Caída de servicios externos; manipulación de flujos; indisponibilidad de APIs; acceso indebido.
Principales vulnerabilidades	Dependencia externa; cambios no coordinados; trazabilidad limitada entre organizaciones.
Escenarios de riesgo	No acceso a información clínica compartida; errores de continuidad asistencial intercentros.
Recomendaciones	Acuerdos operativos; pruebas de interoperabilidad; monitorización extremo a extremo; mecanismos de contingencia manual.

Macrodominio

Interconexión y ecosistema externo

Nombre activo	**Telemedicina y atención remota**
Descripción	Plataformas y dispositivos que permiten consulta, monitorización y asistencia remota.
Elementos que integran este tipo de activos	Portales de teleconsulta; videoconferencia; RPM; apps; dispositivos de paciente; integraciones HCE.
Cantidad típica / Fabricantes	Variable según cartera digital del centro.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; requisitos de identidad y consentimiento.
Criticidad	Alta.
Dependencias clave	Internet; dispositivos del paciente; cloud; HCE; identidad.
Principales amenazas	Intercepción; acceso indebido; suplantación; indisponibilidad de plataforma.
Principales vulnerabilidades	Dispositivos del paciente no gestionados; autenticación débil; dependencia de cloud pública.
Escenarios de riesgo	Consulta no segura; pérdida de seguimiento remoto; interrupción de atención domiciliaria/telemonitorización.
Recomendaciones	Cifrado; autenticación fuerte; evaluación de app/plataforma; continuidad del servicio; consentimiento informado.

Macrodominio

Interconexión y ecosistema externo

Nombre activo	**APIs y sistemas externos de interoperabilidad**
Descripción	Interfaces expuestas para intercambio de datos con terceros, plataformas y servicios externos.
Elementos que integran este tipo de activos	APIs REST/FHIR; gateways; portales; servicios web; colas externas.
Cantidad típica / Fabricantes	Variable según número de integraciones.
Normativa digital aplicable	RGPD; ENS (RD 311/2022); NIS2; marcos de interoperabilidad; ISO 27001.
Criticidad	Muy alta.
Dependencias clave	Motores de integración; IAM; red; terceros.
Principales amenazas	Explotación de API; fuga de datos; DoS; credenciales comprometidas.
Principales vulnerabilidades	APIs expuestas; falta de rate limiting; claves embebidas; validación insuficiente.
Escenarios de riesgo	Caída o manipulación de flujos externos; exposición masiva de datos por API.
Recomendaciones	API gateway; autenticación fuerte; cifrado; rate limiting; pruebas de seguridad y trazabilidad.

Equipo y contacto

Para cualquier consulta relacionada con el estudio, puede contactar con los autores a través de las siguientes vías de contacto:



Gil Vinyeta Medina
JG Ingenieros
gvinyeta@jgingenieros.es



Xavi Pes Bosch
Plain Concepts
xavi.pes@plainconcepts.com



Aníbal Díaz Ginés
Marsh Risk
anibal.diaz@marsh.com

Han participado en la elaboración del estudio:

- **JG Ingenieros:**
  Jaume Cera, David Tudela
- **Plain Concepts:**
  Javier Fernández, Javier Cantón
- **Marsh Risk Consulting:**
  Joel Rodríguez, Albert Bolumar

Acerca de Marsh

Marsh (NYSE: MRSH) es líder mundial en gestión de riesgos, reaseguro y capital, personas e inversiones y consultoría estratégica que asesora a clientes en 130 países. Con unos ingresos anuales superiores a 27.000 millones de dólares y más de 95.000 empleados, Marsh contribuye a generar la confianza necesaria para prosperar gracias a su perspectiva global. Para más información, visita corporate.marsh.com, o síguenos en LinkedIn y X.

Sobre JG

JG Ingenieros es un equipo independiente de profesionales que ofrece servicios de consultoría técnica, diseño, supervisión de la construcción y asistencia en la operación de edificios de alta complejidad. Nuestra actividad se estructura en cuatro áreas de negocio: Instalaciones, Edificación, Consultoría y Test & Soluciones Digitales. Contamos con un equipo diverso y altamente cualificado, con presencia en distintas ciudades a nivel internacional. Prestamos servicios de ingeniería, arquitectura y consultoría con el objetivo de mejorar el bienestar de las personas, la productividad y la sostenibilidad de los activos que desarrollamos. Participamos en todas las fases del ciclo de vida de la edificación, diseñando soluciones que optimizan la inversión y la eficiencia operativa, desde los estudios de viabilidad hasta la gestión en fase de operación.

About Plain Concepts

Plain Concepts is a global technology consultancy that helps organizations create business value through Artificial Intelligence, Data & Analytics, Cloud, and Software Engineering. With more than 800 professionals across Europe, North America, and the Middle East, we partner with leading enterprises to modernize platforms, accelerate innovation, improve operational efficiency, and scale digital transformation initiatives. Our combination of deep technical expertise, industry knowledge, and execution capabilities enables clients to move from strategy to measurable outcomes—faster, with lower risk, and at scale.

Marsh, S.A. Mediadores de Seguros, Correduría de Seguros y Reaseguros (“Marsh Risk”), con domicilio en Paseo de la Castellana 216, 28046 Madrid, y NIF A-81332322. Inscrita en el Registro Mercantil de Madrid (Tomo 10.248, Libro 0, Folio 160, Sección 8, Hoja M-163304, Inscripción 1) y en el registro de la Dirección General de Seguros y Fondos de Pensiones (DGSFP) con las claves J-0096 (Correduría de Seguros) y RJ-0010 (Correduría de Reaseguros). Marsh Risk tiene concertados los seguros de responsabilidad civil y de caución exigidos por la normativa sobre distribución de seguros aplicable. Todos los derechos de propiedad intelectual, estén o no registrados, sobre las informaciones, contenidos, datos, gráficos y demás materiales incluidos en este documento (el “Contenido”), así como sobre su forma de presentación, pertenecen a Marsh Risk. El destinatario/cliente no adquiere, ni deberá intentar adquirir, derecho alguno sobre dicha titularidad. Queda prohibida la reproducción, distribución, publicación, transformación y/o difusión, total o parcial, del Contenido a terceros (incluidos consultores y asesores del cliente), con o sin fines comerciales y a título gratuito u oneroso, sin el previo consentimiento escrito de Marsh Risk. Este documento se ha elaborado para el propósito indicado y no es válido para ningún otro fin distinto del expresamente especificado. Este documento constituye una comunicación de carácter informativo y/o de marketing. La información se facilita únicamente con fines informativos, puede modificarse sin previo aviso y no sustituye el asesoramiento específico que pudiera requerirse. Cualesquiera manifestaciones de naturaleza fiscal, contable o jurídica deben entenderse como observaciones generales basadas exclusivamente en nuestra experiencia como mediadores de seguros y consultores de riesgos, y no pueden considerarse asesoramiento fiscal, contable o jurídico, que no estamos autorizados a prestar; estas materias deben revisarse con asesores adecuadamente cualificados. Marsh Risk no asume responsabilidad por decisiones o actuaciones adoptadas sobre la base de la información aquí contenida, ni por la falta de análisis de implicaciones legales, comerciales o técnicas derivada de la información/documentación facilitada. Marsh Risk ha utilizado la información y los datos que le han sido facilitados sin verificar su exactitud o integridad, salvo en lo requerido por normas o prácticas generalmente aceptadas en el sector; en caso de que la documentación o información proporcionada sea incompleta, inexacta o no esté actualizada, Marsh Risk no será responsable de las consecuencias derivadas de dichas circunstancias.



© 2026 Marsh. Todos los derechos reservados.

26218403-EU