CIBER EN TACONES

Normas aplicables y responsabilidades

Mapa de obligaciones, estructura GRC y propuesta inicial de continuidad para un entorno sanitario.

CASO DE ESTUDIO SIMULADO

PYME SANITARIA MEDITERRÁNEA

Índice

1. Caracterización de la empresa.....3

2. Matriz de aplicabilidad normativa.....3

3. Relación entre las normativas aplicables.....5

4. Organigrama GRC propuesto.....6

5. Mentalidad PDCA aplicada.....7

6. Recomendación inicial al cliente.....7

Fuentes consultadas.....8

1. Caracterización de la empresa

PYME Sanitaria Mediterránea es un hospital privado con 220 empleados que presta servicios sanitarios, entre ellos salud mental, y opera en la Comunidad Valenciana y Andalucía, con presencia en Sevilla. Atiende a más de 15.000 pacientes al año y gestiona historiales clínicos digitales con datos de salud, incluidos datos de salud mental, además de datos de menores. Por tanto, maneja información cuya exposición, pérdida o acceso indebido tendría un impacto especialmente alto para los pacientes y para la propia organización.

Su actividad depende además de sistemas digitales conectados a equipamiento médico y utiliza una herramienta de inteligencia artificial para transcribir notas clínicas. Esto amplía el riesgo más allá de sus propios sistemas, porque obliga a conocer qué información procesa esa herramienta, dónde se almacena, quién puede acceder a ella y qué proveedores intervienen.

La empresa nunca ha realizado una auditoría formal de seguridad. Esto significa que todavía no dispone de una evaluación completa que permita saber si las medidas actuales son suficientes o si existen debilidades que deban corregirse con prioridad. Desde GRC, el primer objetivo debe ser conocer ese punto de partida y ordenar las obligaciones que afectan al hospital.

2. Matriz de aplicabilidad normativa

Normativa	¿Aplica?	Obligatoria o voluntaria	Por qué aplica / por qué NO	Prioridad
RGPD	Sí	Obligatoria	El hospital trata datos personales y, además, datos de salud y salud mental, que son especialmente sensibles. Una pérdida, acceso indebido o uso incorrecto puede afectar gravemente a los pacientes y generar responsabilidad para la empresa, por lo que su protección debe abordarse de forma prioritaria.	Alta
LOPDGDD	Sí	Obligatoria	Complementa el RGPD en España y añade obligaciones específicas para centros sanitarios. Este hospital debe contar con un Delegado de Protección de Datos (DPO), una figura independiente que asesora y supervisa el cumplimiento en	Alta

			privacidad. En un centro que mantiene historias clínicas no es una función opcional. [1]	
NIS2	Sí	Obligatoria (Directiva UE; transposición española pendiente)	El hospital pertenece al sector sanitario, considerado de alta criticidad, y con 220 empleados entra en el ámbito previsto por NIS2. Aunque España aún no ha completado su transposición, la empresa no debería esperar: debe prepararse ya para gestionar riesgos de ciberseguridad, continuidad del servicio, incidentes y proveedores críticos. [2][3]	Alta
AI Act	Sí	Obligatoria, según las obligaciones aplicables al sistema y al papel del hospital	El hospital ya utiliza inteligencia artificial para transcribir notas clínicas. Debe identificar qué tipo de sistema utiliza, qué datos procesa, qué papel tiene el proveedor y qué obligaciones le corresponden. Es prioritario porque la herramienta ya está en funcionamiento con información clínica sensible, aunque todavía sea necesario determinar su clasificación regulatoria concreta. [4]	Alta
ISO/IEC 27001:2022	Sí, como marco de gestión	Voluntaria	No es una obligación legal, pero permite organizar riesgos, controles, responsables y evidencias dentro de un único sistema. Es especialmente útil para una empresa que nunca ha realizado una auditoría formal y necesita estructurar y demostrar su cumplimiento ante terceros. [5]	Media
DORA	No	No aplica	Está dirigida al sector financiero y a	Baja

			determinados proveedores tecnológicos vinculados a entidades financieras. El hospital no es una entidad financiera ni consta que preste ese tipo de servicios, por lo que queda fuera de su ámbito.	
ENS	No, con los datos actuales	No aplica	El hospital es una entidad privada y no consta que preste servicios sujetos al Esquema Nacional de Seguridad para una Administración Pública. Si en el futuro contrata con una AAPP en condiciones que activen el ENS, esta conclusión deberá revisarse.	Baja

3. Relación entre las normativas aplicables

En esta empresa, las normas no deberían gestionarse como proyectos separados. RGPD y LOPDGDD forman la base de protección de los datos personales y son especialmente relevantes porque el hospital gestiona historiales clínicos, información de salud mental y datos de menores. NIS2 amplía el foco: además de proteger la información, obliga a pensar en la continuidad del servicio, la gestión de incidentes y los riesgos que pueden introducir los proveedores tecnológicos.

El AI Act añade una capa específica sobre el uso de inteligencia artificial. La herramienta que transcribe notas clínicas debe analizarse junto con la protección de datos y la gestión de terceros, porque el mismo sistema puede afectar a privacidad, seguridad y dependencia del proveedor. No tendría sentido revisar la IA como un asunto aislado.

ISO/IEC 27001 puede servir como estructura común para ordenar todo lo anterior. Aunque no es obligatoria por ley, permite integrar riesgos, controles, responsables y evidencias en un único sistema de gestión, reduciendo duplicidades y facilitando las auditorías y revisiones de cumplimiento. La certificación no sustituye las obligaciones específicas del RGPD, NIS2 o AI Act, pero ayuda a mantenerlas organizadas, documentadas y revisadas de forma continua. [5]

Por tanto, el orden recomendado sería atender primero las obligaciones de protección de datos, NIS2 y el uso actual de inteligencia artificial. Después, ISO/IEC 27001 puede utilizarse para consolidar esas medidas dentro de un sistema estable. La finalidad no es “cumplir varias normas por separado”, sino conseguir que la empresa sepa qué debe proteger, quién es responsable y qué evidencia puede mostrar para demostrar que sus controles funcionan.

4. Organigrama GRC propuesto

Para un hospital privado de 220 empleados no sería proporcionado crear desde el inicio un gran departamento GRC. Tampoco sería adecuado repartir todas las funciones entre pocas personas hasta sobrecargarlas. La estructura inicial debe cubrir las responsabilidades esenciales y poder crecer cuando aumente la complejidad.

DIRECCIÓN	
Responsable de Seguridad / función CISO	**Delegado de Protección de Datos (DPO)** **Línea directa e independiente**
GRC Analyst	Coordinación con Dirección y áreas afectadas
Sistemas + áreas asistenciales + responsables de proveedores	

Rol	**Modelo recomendado**	**Coste orientativo**	**Motivo**
Delegado de Protección de Datos (DPO)	Externo inicialmente	Referencia de perfil interno: 50.000-55.000 €/año; hasta aprox. 85.000 € en perfiles senior	Permite contar con especialización en privacidad sanitaria sin asumir de inicio el coste completo de un perfil senior interno. Debe mantener independencia y acceso directo a Dirección.
Responsable de Seguridad / CISO	Externo o fraccional	Comunidad Valenciana: aprox. 58.000-79.000 €/año en tramo júnior; aumenta con experiencia y responsabilidad [6]	Para 220 empleados puede resultar desproporcionado contratar un CISO senior a tiempo completo. Un servicio fraccional permite ajustar dedicación y coste al riesgo real.
GRC Analyst	Interno	Comunidad Valenciana: aprox. 38.000-51.000 €/año en tramo júnior [6]	El cumplimiento genera trabajo continuo: evidencias, riesgos, proveedores, auditorías y seguimiento. Mantener esta función dentro aporta continuidad y conocimiento de la operativa.

Si el DPO se externaliza, debería contratarse a una consultora o profesional con experiencia demostrable en sanidad y protección de datos, independencia, ausencia de conflictos de interés y capacidad de respuesta ante incidentes o requerimientos regulatorios. El CISO externo o fraccional debería acreditar experiencia en sector sanitario, NIS2, gestión de proveedores y entornos donde conviven sistemas informáticos y equipamiento médico. La dedicación puede contratarse por horas o jornadas periódicas y reforzarse ante una auditoría, incidente o cambio importante.

No incluir inicialmente un Risk Manager o un AI Compliance Officer como puestos independientes no significa que esas funciones desaparezcan. De momento pueden repartirse de forma controlada entre GRC, seguridad y privacidad. Habría que revisar esta estructura si el hospital crece, abre nuevos centros, aumenta su dependencia de proveedores

críticos o empieza a utilizar IA para diagnóstico, priorización de pacientes o decisiones clínicas. En ese momento, mantener esas funciones como tareas secundarias podría dejar de ser suficiente.

5. Mentalidad PDCA aplicada

Riesgo prioritario: interrupción de la atención por caída de los historiales clínicos digitales o de sistemas tecnológicos necesarios para prestar el servicio.

Plan. Identificar los sistemas imprescindibles para la atención y establecer un objetivo claro: poder continuar la actividad aunque uno de ellos quede temporalmente fuera de servicio. El Responsable de Seguridad coordinará este análisis con Dirección, personal asistencial y proveedores críticos. Se definirá qué sistemas deben recuperarse primero, quién toma decisiones y qué información mínima debe estar disponible durante una caída.

Do. Implantar copias de seguridad verificadas, contactos de emergencia con proveedores y un procedimiento temporal para trabajar durante la incidencia. Como alternativa, el hospital puede utilizar formularios clínicos en papel previamente definidos para registrar actuaciones básicas mientras el sistema no esté disponible, incorporando después esa información al historial digital cuando se recupere el servicio.

Check. Realizar un simulacro cada seis meses en el que se pruebe la recuperación de una copia de seguridad y el procedimiento de atención sin acceso al sistema. Deben conservarse como evidencia el acta del ejercicio, participantes, hora de inicio y recuperación, resultado de la restauración, incidencias detectadas y acciones pendientes. Además, tras cualquier cambio importante de proveedor o sistema, deberá repetirse la prueba.

Act. Si la restauración falla, el tiempo de recuperación impide mantener la actividad o el personal no sabe cómo actuar, se actualizarán el procedimiento, las responsabilidades y los controles afectados. La prueba se repetirá después de aplicar las mejoras para comprobar que el problema ha quedado corregido.

6. Recomendación inicial al cliente

La prioridad inmediata es conocer el punto de partida real del hospital: revisar protección de datos, ciberseguridad, proveedores tecnológicos y el uso de inteligencia artificial. La empresa ya opera en un sector de alta criticidad y maneja información clínica especialmente sensible, pero nunca ha realizado una auditoría formal de seguridad. Por eso, el primer paso debe ser identificar las principales brechas y responsables antes de ampliar controles o iniciar una certificación.
La certificación ISO/IEC 27001 puede abordarse después, como herramienta para ordenar y demostrar de forma continua el cumplimiento, pero no debe retrasar las obligaciones actuales de RGPD, LOPDGDD, la preparación para NIS2 y las obligaciones del AI Act que correspondan al sistema utilizado.

El mayor riesgo de no actuar es sufrir un incidente que afecte simultáneamente a pacientes, continuidad asistencial y cumplimiento regulatorio. Como horizonte inicial, propondría 3-6

meses para disponer de un diagnóstico completo, responsables definidos, medidas prioritarias implantadas y un plan documentado de seguimiento. La preparación para una futura certificación ISO/IEC 27001 requeriría un proyecto adicional y más largo, acorde con el tamaño y complejidad del hospital.

Fuentes consultadas

[1] BOE. Ley Orgánica 3/2018 (LOPDGDD), art. 34: DPO en centros sanitarios. Enlace
[2] EUR-Lex. Directiva (UE) 2022/2555 (NIS2), art. 2 y Anexo I: ámbito y sector salud. Enlace
[3] Comisión Europea, 8/07/2026. España remitida al TJUE por no notificar la transposición completa de NIS2. Enlace
[4] EUR-Lex. Reglamento (UE) 2024/1689 (AI Act), versión consolidada 27/07/2026. Enlace
[5] ISO. ISO/IEC 27001:2022: SGSI y carácter voluntario de la certificación. Enlace
[6] ISPROX. Guía Salarial España 2026, Comunidad Valenciana: CISO y GRC / Risk & Compliance Cyber. Enlace