CIBER EN TACONES

INFORME 02 / 08

# Plan de seguridad del Centro 1

Propuesta de SGSI, controles prioritarios y preparación para la certificación ISO 27001.

CASO DE ESTUDIO SIMULADO

PYME SANITARIA MEDITERRÁNEA

# ÍNDICE

1. Perímetro inicial de certificación.....3

2. Qué debe estar listo antes de la auditoría.....4

3. Gobierno y responsabilidades de seguridad.....4

4. Controles prioritarios para el Centro 1.....5

5. Priorización de riesgos y selección de controles.....7

6. Plan de implantación y certificación.....8

7. Resumen ejecutivo para Dirección.....8

8. Fuentes consultadas.....9

# 1. Perímetro inicial de certificación

PYME Sanitaria Mediterránea desarrolla su actividad en el sector sanitario privado y cuenta con 220 empleados distribuidos en tres centros de Valencia. Su funcionamiento depende de información clínica especialmente sensible: gestiona historiales clínicos electrónicos, dispone de un portal de citas online y mantiene integración con el sistema público de salud. Esto hace que la seguridad de la información afecte no solo a la tecnología, sino también a la confidencialidad de los pacientes, la continuidad de la atención y la relación con servicios externos. Además de las obligaciones aplicables en materia de protección de datos, la organización está clasificada como entidad importante dentro del marco de la Directiva sobre seguridad de las redes y sistemas de información (NIS2). Este contexto debe tenerse en cuenta al definir qué procesos, sistemas y responsabilidades quedarán cubiertos por el Sistema de Gestión de Seguridad de la Información (SGSI).

La organización quiere obtener la certificación ISO 27001:2022 para poder concurrir a licitaciones públicas. Para lograrlo, se recomienda iniciar la certificación en uno de los tres centros de Valencia, trabajando sobre un perímetro suficientemente concreto para poder implantarlo, comprobarlo y demostrar su funcionamiento ante una auditoría.

Comenzar por un único centro reduce la complejidad inicial, facilita detectar y corregir deficiencias antes de extender el modelo y evita replicar en toda la organización procesos o controles que todavía no hayan demostrado funcionar de forma consistente. Una vez estabilizado el sistema y comprobado que los controles funcionan adecuadamente, la Dirección podrá valorar la ampliación progresiva del alcance a los otros dos centros.

## Alcance propuesto

La primera certificación se limitará al Centro 1 de Valencia. Dentro de este centro, el alcance incluirá los procesos de admisión de pacientes, gestión de citas e historia clínica electrónica, junto con las personas, sistemas de información y servicios tecnológicos necesarios para su funcionamiento seguro.

Esto incluye el portal de citas online, los sistemas utilizados para gestionar las historias clínicas electrónicas y la conexión con el sistema público de salud cuando intervenga directamente en los procesos incluidos. El objetivo no es certificar únicamente una aplicación informática, sino la forma completa en la que el centro gestiona y protege la información durante la prestación de estos servicios.

También deberán contemplarse las dependencias necesarias para que esos procesos funcionen. Si una plataforma, infraestructura o servicio tecnológico es compartido con los otros centros y resulta imprescindible para la actividad del Centro 1, los controles que afecten a esa dependencia deberán quedar incluidos dentro del sistema de gestión. Cuando intervengan proveedores externos, el alcance deberá cubrir cómo se gestionan sus accesos, responsabilidades y requisitos de seguridad, sin que ello implique certificar al propio proveedor.

Los Centros 2 y 3 quedarán fuera de esta primera fase, al igual que los procesos asistenciales o administrativos que no estén vinculados al perímetro seleccionado. No obstante, las funciones corporativas, sistemas compartidos o servicios externos que puedan afectar directamente a la seguridad de los procesos incluidos deberán contemplarse cuando exista una dependencia real.

Esta delimitación permite iniciar la certificación con un alcance controlable, relevante para el negocio y suficientemente representativo como para construir un modelo que posteriormente pueda ampliarse al resto de la organización.

### Declaración de alcance

**El Sistema de Gestión de Seguridad de la Información (SGSI) para esta primera certificación ISO 27001:2022 comprenderá los procesos de admisión de pacientes, gestión de citas e historia clínica electrónica del Centro 1 de PYME Sanitaria Mediterránea en Valencia, incluyendo las personas, sistemas de información, conexiones y servicios tecnológicos necesarios para su funcionamiento. Los Centros 2 y 3 y los procesos no vinculados directamente con este perímetro quedarán fuera de esta primera fase.**

## 2. Qué debe estar listo antes de la auditoría

Para certificar el Centro 1, la empresa deberá cumplir los siete requisitos de gestión de ISO 27001:2022 y generar las evidencias que permitan demostrar que el sistema está implantado y funciona en la práctica.

| ISO 27001:2022 | Qué exige | Qué habrá que hacer en el Centro 1 | Documento o evidencia a generar |
|---|---|---|---|
| 4. Contexto | Definir alcance, partes interesadas y requisitos aplicables. | Delimitar procesos, sistemas y dependencias del Centro 1. | Alcance aprobado y relación de requisitos y partes interesadas. |
| 5. Liderazgo | Compromiso de Dirección, política y responsabilidades. | Aprobar la política y asignar responsables. | Política firmada, matriz de responsabilidades y acta del Comité. |
| 6. Planificación | Analizar riesgos, tratarlos y fijar objetivos. | Identificar riesgos y seleccionar controles. | Análisis de riesgos, plan de tratamiento, objetivos y Declaración de Aplicabilidad (SoA). |
| 7. Apoyo | Asegurar recursos, formación, comunicación y documentación. | Preparar al personal y organizar la documentación. | Registros de formación, comunicaciones y control documental. |
| 8. Operación | Ejecutar los controles y el tratamiento de riesgos. | Aplicar las medidas previstas en los procesos incluidos. | Registros de accesos, copias, incidencias y gestión de proveedores. |
| 9. Evaluación | Medir resultados, auditar y revisar desde Dirección. | Comprobar que el sistema funciona antes de certificarlo. | Indicadores, auditoría interna y acta de revisión por Dirección. |
| 10. Mejora | Corregir fallos y mejorar continuamente. | Resolver desviaciones y comprobar su corrección. | Registro de no conformidades, acciones correctivas y cierre. |

## 3. Gobierno y responsabilidades de seguridad

La certificación requiere respaldo de Dirección y responsabilidades claras. Para el Centro 1 se propone una estructura sencilla, suficiente para tomar decisiones, ejecutar las medidas y mantener evidencia de su seguimiento.

### Política de seguridad

Dirección aprobará una política aplicable al Centro 1 que comprometa a la organización a proteger la confidencialidad de la información de pacientes, mantener su integridad y garantizar la disponibilidad de los sistemas necesarios para admisión, citas e historia clínica electrónica. También deberá asegurar los recursos necesarios, exigir el cumplimiento de las medidas acordadas y revisar la política al menos una vez al año o cuando se produzcan cambios relevantes en los sistemas, el alcance o los requisitos aplicables.

### Comité de Seguridad

El Sistema de Gestión de Seguridad de la Información (SGSI) estará supervisado por un Comité de Seguridad formado por Dirección, el responsable de Seguridad/Gobierno, Riesgo y Cumplimiento (GRC), el responsable de Sistemas, el Delegado de Protección de Datos (DPO) y un responsable de admisión o gestión clínica.

Dirección aprobará políticas, recursos y decisiones relevantes; Seguridad/GRC coordinará riesgos, controles, evidencias y auditorías; Sistemas gestionará los aspectos tecnológicos y los proveedores; el DPO asesorará y supervisará los aspectos de privacidad y protección de datos; y el área clínica aportará la visión operativa del Centro 1.

Durante la implantación, el comité se reunirá mensualmente y, una vez estabilizado el sistema, podrá pasar a reuniones trimestrales. Se convocará una reunión extraordinaria cuando un incidente afecte a la continuidad de los procesos incluidos, comprometa o pueda comprometer datos de salud, implique accesos no autorizados a sistemas críticos, afecte a un proveedor esencial o pueda generar obligaciones de notificación. También se reunirá ante cambios relevantes en los sistemas o hallazgos que puedan comprometer la certificación.

Cada reunión dejará un acta con las decisiones tomadas, responsables y fechas de cumplimiento. De este modo, Dirección podrá hacer seguimiento y el auditor dispondrá de evidencia de que el sistema se gobierna de forma activa.

## 4. Controles prioritarios para el Centro 1

Con el perímetro de certificación ya definido, se han identificado 18 controles que requieren una revisión prioritaria por su relación con la información clínica, los accesos, la continuidad del servicio y los sistemas que soportan la admisión, las citas y la historia clínica electrónica.

Estas decisiones formarán la base de la Declaración de Aplicabilidad (SoA), donde quedará documentado qué controles corresponden al alcance, cuáles pueden excluirse y la justificación de cada decisión. La valoración se completará con el análisis de riesgos y con las evidencias obtenidas durante el diagnóstico inicial.

El estado actual se ha valorado únicamente con la información disponible al inicio del proyecto. Cuando no se dispone de evidencia suficiente para confirmar que una medida está implantada, se indica como “Sin evidencia”. Esto no significa que el control no exista, sino que todavía no se ha demostrado su implantación.

| Ref. | Control | ¿Aplica? | Justificación para el Centro 1 | Estado actual |
|---|---|---|---|---|
| A.5.9 | Inventario de información y otros activos asociados | Sí | Es necesario conocer qué información, sistemas y equipos sostienen los procesos incluidos y quién responde de ellos. | Sin evidencia |

| | | | | |
|---|---|---|---|---|
| A.5.14 | Transferencia de información | Sí | La integración con el sistema público de salud implica intercambio de información que debe realizarse de forma controlada y segura. | Sin evidencia |
| A.5.15 | Control de acceso | Sí | El acceso a historias clínicas, citas y admisión debe limitarse según las funciones de cada usuario. | Sin evidencia |
| A.5.18 | Derechos de acceso | Sí | Los permisos deben concederse, revisarse y retirarse cuando cambien las funciones de una persona o deje de necesitar acceso. | Sin evidencia |
| A.5.24 | Preparación para la gestión de incidentes de seguridad | Sí | Un incidente puede afectar a la información clínica y a la continuidad de los servicios incluidos, por lo que debe existir una respuesta organizada. | Sin evidencia |
| A.5.30* | Preparación de las tecnologías de la información y las comunicaciones (TIC) para la continuidad del negocio | Sí | La caída de los sistemas de admisión, citas o historia clínica puede interrumpir la actividad del Centro 1. | Sin evidencia |
| A.5.31 | Requisitos legales, regulatorios y contractuales | Sí | Los procesos incluidos deben tener identificadas las obligaciones legales y contractuales que afectan a la información y a los servicios. | Sin evidencia |
| A.5.34 | Privacidad y protección de datos personales | Sí | Las historias clínicas contienen datos personales de salud cuya protección forma parte directa de los procesos incluidos. | Sin evidencia |
| A.6.3 | Concienciación, educación y formación en seguridad | Sí | El personal debe saber cómo proteger la información y cómo actuar ante errores, accesos indebidos o incidentes. | Sin evidencia |
| A.6.6 | Acuerdos de confidencialidad | Sí | Las personas con acceso a información clínica deben conocer y asumir sus obligaciones de confidencialidad. | Sin evidencia |
| A.7.2 | Controles de entrada físicos | Sí | Debe impedirse el acceso no autorizado a las zonas desde las que se utilizan o custodian sistemas e información del alcance. | Sin evidencia |
| A.8.5 | Autenticación segura | Sí | El acceso a historias clínicas y otros sistemas sensibles debe identificar correctamente al usuario antes de permitir el acceso. | Sin evidencia |
| A.8.12* | Prevención de fuga de datos | Sí | Una extracción o envío no autorizado de información clínica | Sin evidencia |

| | | | | |
|---|---|---|---|---|
| | | | podría afectar directamente a los pacientes y a la organización. | |
| A.8.13 | Copias de seguridad | Sí | La información debe poder recuperarse ante pérdida de datos, fallo técnico o incidente de seguridad. | Sin evidencia |
| A.8.15 | Registro de eventos | Sí | Se necesita trazabilidad para conocer qué ocurre en los sistemas e investigar accesos o incidentes. | Sin evidencia |
| A.8.16* | Monitorización de actividades | Sí | Permite detectar comportamientos anómalos o accesos que puedan indicar un incidente. | Sin evidencia |
| A.8.24 | Uso de criptografía | Sí | La información clínica debe protegerse tanto cuando está almacenada como cuando se transmite entre sistemas. | Sin evidencia |
| A.8.28* | Codificación segura | Por determinar | Debe comprobarse si el portal de citas, la historia clínica o sus integraciones incluyen desarrollo propio, software a medida, modificaciones de código o desarrollos encargados a terceros antes de decidir si este control puede excluirse. | Pendiente de evaluar |

** Control incorporado en ISO 27001:2022.*

## 5. Priorización de riesgos y selección de controles

El análisis de riesgos se centrará en los activos que sostienen los procesos incluidos en la certificación: historia clínica electrónica, portal de citas, sistemas de admisión, cuentas de usuario, equipos, conexiones con el sistema público de salud y servicios externos necesarios para su funcionamiento.

Sobre estos activos se evaluarán amenazas como accesos no autorizados, ransomware (secuestro de sistemas o datos), pérdida de información, caídas de servicio o errores humanos. También se revisarán vulnerabilidades que puedan facilitar esos incidentes, por ejemplo permisos excesivos, contraseñas débiles, copias de seguridad insuficientes, sistemas desactualizados o falta de formación del personal.

Cada riesgo se valorará según su probabilidad y el impacto que podría tener sobre la atención al paciente, la confidencialidad de los datos y la continuidad del servicio. Los riesgos más altos tendrán prioridad de tratamiento.

El resultado servirá para confirmar los controles del Anexo A que deben aplicarse al Centro 1 y para justificar aquellos que puedan excluirse. Así, cada control incluido tendrá una razón concreta y cualquier exclusión deberá poder explicarse con base en el riesgo real del centro. Tras aplicar las medidas, se revisará el riesgo residual para comprobar si puede aceptarse o necesita controles adicionales.

Para realizar este análisis se propone utilizar la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT v3), ya que permite mantener trazabilidad entre los activos clínicos, las amenazas, su impacto y las decisiones de tratamiento.

## 6. Plan de implantación y certificación

Para el Centro 1 se propone un proyecto de nueve meses, con tiempo suficiente para implantar los controles, generar evidencias de su funcionamiento y corregir desviaciones antes de solicitar la certificación.

| Periodo | Trabajo previsto | Resultado |
|---|---|---|
| Mes 1 | Diagnóstico de brechas (gap analysis) durante 3 semanas, revisando controles existentes, documentación y evidencias disponibles. | Situación de partida y plan de trabajo priorizado. |
| Mes 2 | Análisis de riesgos y definición de su tratamiento. | Riesgos priorizados y medidas necesarias. |
| Mes 3 | Cierre de la Declaración de Aplicabilidad (SoA), aprobación de la política y asignación de responsabilidades. | Controles definidos y gobierno del sistema aprobado. |
| Meses 4-6 — 2.º trimestre del proyecto | Implantación o refuerzo de los controles prioritarios, formación del personal y generación de evidencias. | Controles funcionando y registros que demuestren su aplicación. |
| Mes 7 | Auditoría interna, revisión por Dirección y corrección de las desviaciones detectadas. | Sistema preparado para iniciar la certificación externa. |
| Mes 8 | Auditoría documental (Stage 1), realizada por una entidad certificadora acreditada por la Entidad Nacional de Acreditación (ENAC). | Validación del alcance, la documentación y la preparación para la siguiente fase. |
| Mes 9 | Auditoría de implantación (Stage 2), con revisión de evidencias, entrevistas y comprobación del funcionamiento de los controles. | Obtención del certificado si no existen incumplimientos graves que lo impidan. |

**Punto crítico del proyecto.** El mes 7 concentra el mayor riesgo de retraso. La auditoría interna puede detectar controles que todavía no funcionan correctamente, falta de evidencias o procedimientos que no se están aplicando. Estas desviaciones deberán corregirse antes de iniciar la certificación externa.

**Entidad certificadora recomendada.** Se propone AENOR por su acreditación para certificar ISO/IEC 27001:2022 y por su experiencia en el sector sanitario. Esta combinación resulta especialmente adecuada para una organización que trata información clínica y depende de sistemas digitales para procesos asistenciales y administrativos.

**Coste estimado.** Para la implantación y certificación ISO 27001:2022 del Centro 1 se estima una inversión de 35.000 a 50.000 €, incluyendo consultoría de implantación y auditoría externa. La horquilla responde a la complejidad del entorno sanitario, la sensibilidad de la información y las integraciones con otros sistemas, y se mantiene contenida al limitar el alcance a un único centro.

**Seguimiento posterior.** Primera auditoría de vigilancia en el mes 18 y auditoría de recertificación en el tercer año desde la emisión del certificado.

## 7. Resumen ejecutivo para Dirección

**Situación actual.** El Centro 1 gestiona procesos críticos y datos de salud, pero su nivel real de preparación para ISO 27001:2022 todavía debe verificarse mediante el diagnóstico inicial.

**Lo que necesita.** Para certificarse, el centro debe definir responsabilidades, identificar sus principales riesgos, implantar o reforzar los controles necesarios y demostrar con evidencias que funcionan antes de someterse a la auditoría externa.

**Coste y plazo.** El proyecto se ha planificado en nueve meses, con el objetivo de completar la certificación en el mes 9. La inversión estimada es de 35.000 a 50.000 €, incluyendo consultoría de implantación y auditoría externa.

**Riesgo de no actuar.** No iniciar el proyecto mantiene sin validar la protección de los sistemas que sostienen la admisión, las citas y la historia clínica electrónica. Un incidente podría interrumpir estos servicios, impedir el acceso a información clínica o exponer datos de pacientes, con consecuencias regulatorias y reputacionales para el hospital. Además, la organización está clasificada como entidad importante en el marco de la Directiva sobre seguridad de las redes y sistemas de información (NIS2) y busca esta certificación para concurrir a licitaciones públicas, por lo que retrasarla también puede aplazar o impedir el acceso a oportunidades de negocio que exijan acreditar este nivel de seguridad.

## 8. Fuentes consultadas


• **International Organization for Standardization (ISO).** ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

• **Centro Criptológico Nacional (CCN-CERT).** MAGERIT v3 — Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

• **Entidad Nacional de Acreditación (ENAC).** Buscador de entidades acreditadas.

• **AENOR.** Seguridad y Privacidad de la Información: ISO 27001 e ISO 27701.

• **Unión Europea — EUR-Lex.** Directiva (UE) 2022/2555 (NIS2), relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión.