# Mapa de cumplimiento integrado

Relación de controles, obligaciones y evidencias para una gestión integrada de ISO 27001, NIS2 y RGPD.

# Índice

1. Diagnóstico de frameworks aplicables 3

2. Mapeo cruzado de controles 4

3. Análisis de cobertura y solapamiento 6

4. Orden de implementación 7

5. Mapa de cumplimiento integrado 8

6. Recomendación ejecutiva 10

Bibliografía 10

## 1. Diagnóstico de frameworks aplicables

PYME Sanitaria Mediterránea es un hospital privado de 220 empleados con HIS, LIS y datos de salud. El caso es simulado: los hallazgos E01–E10 provienen de la auditoría interna simulada y el vishing al proveedor LIS de marzo de 2026, con posible exposición de historiales, de la expediente del incidente LIS. El cifrado LIS incompleto refuerza la necesidad de un cumplimiento coordinado.

| Norma | Aplica | Carácter | Justificación |
|---|---|---|---|
| ISO/IEC 27001:2022 | Sí | Voluntario | Se recomienda como base del SGSI para evaluar los riesgos del HIS/LIS y la HCE, asignar responsables y mantener evidencias verificables. Facilita acreditar las garantías de seguridad solicitadas por aseguradoras. |
| ENS — RD 311/2022 | No | No obligatorio | El art. 2.3 también alcanza a empresas privadas que prestan determinados servicios o soluciones al sector público. No consta esa relación en Mediterránea; no procede su certificación, aunque puede servir de referencia técnica. |
| NIS2 — Directiva (UE) 2022/2555 | Sí | Directiva UE; desarrollo nacional pendiente | Los prestadores sanitarios figuran en el Anexo I. Con 220 empleados, la clasificación de referencia es entidad importante (arts. 2–3); deben comprobarse facturación, balance y vínculos societarios que puedan llevar a la categoría esencial. |
| DORA — Reglamento (UE) 2022/2554 | No | No obligatorio | El art. 2 se aplica a entidades financieras y determinados proveedores TIC del ámbito financiero. El hospital desarrolla actividad sanitaria y queda fuera del supuesto descrito. |
| RGPD — Reglamento (UE) 2016/679 | Sí | Obligatorio | Trata datos de salud, menores y empleados (arts. 5 y 9). El art. 32 exige seguridad adecuada. La gestión y notificación a la AEPD del incidente LIS deben revisarse conforme a los arts. 33 y 34. |

**Conclusión para Dirección.** Se recomienda consolidar ISO 27001 como estructura común del SGSI del Centro 1, integrando NIS2 y RGPD para evitar controles y evidencias duplicados. Deben priorizarse el acceso remoto del proveedor LIS, el cifrado de datos clínicos, las copias HCE y la respuesta ante incidentes.

La categoría NIS2 debe contrastarse con la facturación, el balance y los vínculos societarios, y con la transposición española vigente. El análisis de aplicabilidad no retrasa la corrección de los riesgos clínicos acreditados.

## 2. Mapeo cruzado de controles

Se seleccionan diez controles de ISO/IEC 27001:2022 que permiten atender requisitos comunes de NIS2 y RGPD. Su aplicación se centra en la protección del HIS y LIS, los historiales clínicos, el acceso remoto de proveedores y la continuidad asistencial. Se consideran transversales cuando una misma medida y sus evidencias contribuyen a satisfacer varias obligaciones, sin que ello suponga un cumplimiento automático de todas ellas.

| Control ISO 27001:2022 | ENS | NIS2 | DORA | Transversalidad y evidencia compartida |
|---|---|---|---|---|
| **A.5.1** — Políticas de seguridad | | Art. 21.2.a | | ISO–NIS2–RGPD (art. 24). Política que asigne a TI la administración del HIS/LIS, al responsable de seguridad la supervisión de accesos externos y a Dirección su aprobación; política firmada y matriz de responsabilidades. |
| **A.5.19** — Seguridad de proveedores | | Art. 21.2.d | | ISO–NIS2–RGPD (arts. 28 y 32). Evaluación del proveedor LIS tras el incidente de vishing, obligaciones contractuales de seguridad y autorizaciones documentadas de mantenimiento remoto. |
| **A.5.18** — Derechos de acceso | | Art. 21.2.i | | ISO–NIS2–RGPD (art. 32). La auditoría identificó un permiso de consulta HCE que permanecía activo tras un cambio de puesto (NCm-01). Se requiere revocarlo, revisar el procedimiento de cambios de funciones y comprobar, mediante nuevos registros y muestras, que los permisos se retiran dentro del plazo establecido. |
| **A.8.5** — Autenticación segura | | Art. 21.2.i, j | | ISO–NIS2–RGPD (art. 32). MFA para conexiones remotas al LIS, identificación de cuentas autorizadas y registros de autenticación que permitan detectar accesos indebidos. |
| **A.8.24** — Criptografía | | Art. 21.2.h | | ISO–NIS2–RGPD (arts. 5.1.f y 32). Completar el cifrado en reposo del LIS; configuración criptográfica y pruebas que acrediten la protección de las bases de datos clínicas. |

| Control ISO 27001:2022 | ENS | NIS2 | DORA | Transversalidad y evidencia compartida |
|---|---|---|---|---|
| **A.5.24** — Preparación ante incidentes | | Art. 21.2.b; art. 23 | | ISO–NIS2–RGPD (arts. 33 y 34). Expediente del incidente de marzo: cronología, sistemas afectados, evaluación de la posible exposición de historiales, decisiones de notificación y acciones correctivas. |
| **A.8.13** — Copias de seguridad | | Art. 21.2.c | | ISO–NIS2–RGPD (art. 32.1.c). Verificar la inclusión de las bases clínicas del HIS/LIS en las copias y documentar pruebas de restauración íntegra y recuperación de datos. |
| **A.8.15** — Registro de eventos | | Art. 21.2.b | | ISO–NIS2–RGPD (art. 32). Logs de consultas HCE, operaciones privilegiadas y acceso LIS; revisión de alertas e incidentes. Los registros también aportan evidencia para evaluar eficacia (21.2.f), sin sustituir esa evaluación. |
| **A.8.8** — Vulnerabilidades técnicas | | Art. 21.2.e | | ISO–NIS2–RGPD (art. 32). Revisión de vulnerabilidades del HIS/LIS y conexiones de mantenimiento remoto; hallazgos, responsables, plazos de corrección y pruebas de cierre. |
| **A.6.3** — Formación en seguridad | | Art. 21.2.g | | ISO–NIS2–RGPD (arts. 24 y 32). Formación contra vishing al personal que autoriza accesos al LIS, coordinada con el proveedor afectado; simulaciones y resultados documentados. |

Nota de aplicabilidad: las columnas ENS y DORA permanecen vacías porque no se han identificado obligaciones de estos marcos para la actividad y las condiciones actuales del hospital. El RGPD se incorpora en la última columna por su aplicación transversal a los tratamientos de datos personales.

**Conclusión.** La integración reutiliza políticas, configuraciones, registros y pruebas, pero exige contrastar por separado las obligaciones legales. Prioridades: acceso remoto LIS, cifrado, restauración HCE y respuesta a incidentes. La eficacia debe acreditarse con pruebas; NIS2 (art. 23) y RGPD (arts. 33–34) mantienen procedimientos y destinatarios propios.

## 3. Análisis de cobertura y solapamiento

El Centro 1 dispone de análisis de riesgos, SoA, RAT y pruebas simuladas de auditoría interna reutilizables en ISO 27001, NIS2 y RGPD. No equivalen a una declaración de cumplimiento de los tres marcos.

**Cobertura y brechas.** Los diez controles seleccionados tienen correspondencias funcionales con NIS2 y RGPD; no se cuantifica su cobertura legal como porcentaje. Permanecen NCM-01 (copias HCE), permisos y trazas HCE, cifrado LIS y E03 sin evidencia suficiente.

NIS2 exige además supervisión de Dirección y notificación sectorial (arts. 20 y 23); RGPD, evaluar y notificar brechas (arts. 33–34). Una evidencia común no elimina estas obligaciones.

**Estimación del esfuerzo de auditoría-consultoría GRC**

Cálculo ex ante para el mismo alcance GRC, no horas medidas: por actividad se estiman revisión, entrevistas y evidencias separadas para tres marcos, frente a una revisión común más comprobaciones normativas específicas.

| Actividad prevista | Por separado | Integrado | Horas evitadas |
|---|---|---|---|
| Actualización de riesgos HIS/LIS y SoA | 22 h | 14 h | 8 h |
| Revisión del proveedor LIS y accesos remotos | 24 h | 16 h | 8 h |
| Evaluación del cifrado del LIS | 16 h | 12 h | 4 h |
| Revisión del incidente de marzo y notificaciones | 20 h | 15 h | 5 h |
| Verificación de copias HCE y continuidad | 20 h | 14 h | 6 h |
| Consolidación de evidencias y seguimiento | 28 h | 16 h | 12 h |
| **Total** | **130 h** | **87 h** | **43 h** |

Supuesto de ahorro: se evita revisar varias veces el mismo soporte, sin suprimir validaciones legales. Ejemplo: consolidación de evidencias, 28 h por separado y 16 h integrada; horas sujetas a validación.

**Resultado económico estimado — Centro 1**

| Indicador | Gestión separada | Gestión integrada |
|---|---|---|
| Horas profesionales estimadas | 130 h | 87 h |
| Tarifa de referencia, sin IVA | 65 €/h | 65 €/h |
| Coste estimado | 8.450 € | 5.655 € |
| **Ahorro frente a gestión separada** | — | **2.795 € (33,1 %)** |

Tarifa de referencia: 65 €/h sin IVA, precio unitario de licitación para consultor sénior de Cyberzaintza (exp. 001/2025; enlace oficial en bibliografía). Las dedicaciones son supuestos de consultoría, no importes contratados.

**Conclusión.** El escenario integrado evita 43 h y 2.795 € GRC (33,1 %). Excluye correcciones HCE/MFA/LIS, herramientas y certificación.

## 4. Orden de implementación

Se priorizan los riesgos acreditados para HCE (restauración, permisos y trazas) y el incidente LIS. ISO 27001 sigue siendo la base del SGSI, con las obligaciones NIS2 y RGPD integradas cuando corresponda.

Proyecto: 01/11/2026–28/02/2027, sujeto a Dirección. Plazos del plan de acciones correctivas desde aprobación: NCM-01, contención inmediata y prueba ≤15 días; NCm-01, revocación ≤24 h; NCm-01/02/03, cierres ≤30 días; OBS-01, ≤60 días. Revisión jurídica LIS inmediata.

| Fase y período | Actuaciones prioritarias | Responsables y evidencias de cierre |
|---|---|---|
| 1. Correcciones críticas 01–30/11/2026 | Contener la exclusión HCE; incluir su base y probar restauración ≤15 días. Revocar acceso obsoleto ≤24 h; restringir conexiones LIS, implantar MFA y cifrar resultados. Revisar urgentemente comunicaciones del incidente de marzo. | Sistemas, responsable HCE/LIS y DPO. Restauración validada por clínica, permisos revocados, MFA y cifrado probados, expediente de brecha contrastado. |
| 2. Consolidación del SGSI 01–31/12/2026 | Actualizar riesgos/SoA y verificar hipótesis de causa NCM-01: cambio de configuración 25/09 y control de contenido de copias. Revisar terceros, registros y vulnerabilidades; cerrar NCm-01/02/03 en ≤30 días. | SGSI, Sistemas, RR. HH. y proveedor HCE. SoA/riesgos revisados, causa contrastada y pruebas nuevas de permisos, formación y trazas. |
| 3. Integración normativa 01–31/01/2027 | Integrar notificación NIS2 (art. 23) diferenciada de RGPD (arts. 33–34), gobierno de Dirección y formación contra vishing, sin diferir plazos exigibles. | Dirección, SGSI y DPO. Procedimientos y responsabilidades aprobados, evidencia de formación y simulación. |
| 4. Verificación y mejora 01–28/02/2027 | Verificar eficacia de cierres de la auditoría interna y continuidad de admisión, citas y HCE. Documentar evaluación de preparación para certificación. | SGSI, Sistemas y revisor independiente. Pruebas de continuidad, cierres verificados y acta de Dirección. |

**Justificación del orden.** La recuperación HCE y la contención de accesos preceden al perfeccionamiento documental por impacto asistencial. Las obligaciones de notificación RGPD se evalúan con urgencia desde la detección: art. 33, regla de 72 h cuando procede, no desde el inicio de la fase 1.

ISO 27001 sigue siendo el marco de gestión; NIS2 añade gobierno, riesgos y notificaciones (arts. 20, 21 y 23), y RGPD exige seguridad y gestión de brechas (arts. 32–34). ENS y DORA no generan fases obligatorias.

**Resultado previsto:** al cierre de febrero de 2027, SGSI integrado consolidado y correcciones verificadas, sin alterar los plazos inmediatos. Una futura certificación ISO dependerá de evidencia de eficacia y cierre de NCM-01, no de la mera ejecución del calendario.

## 5. Mapa de cumplimiento integrado

Se propone consolidar un único Sistema de Gestión de Seguridad de la Información (SGSI) para el Centro 1 de PYME Sanitaria Mediterránea, aprovechando los análisis de riesgos, la Declaración de Aplicabilidad (SoA), el Registro de Actividades de Tratamiento (RAT) y las evidencias de auditoría existentes. El alcance incluye admisión, citas, historia clínica electrónica (HCE) y las dependencias tecnológicas y proveedores que intervienen en estos servicios.

**Arquitectura integrada.** ISO/IEC 27001:2022 constituye la base del SGSI: organiza riesgos, controles, responsables, auditorías y mejora continua. Sobre esta estructura se incorporan los requisitos de gestión de riesgos y supervisión de NIS2 (arts. 20 y 21) y las obligaciones de protección de datos del RGPD. Los controles transversales comparten procedimientos y evidencias; las obligaciones específicas conservan su propia gestión.

**Declaración de Aplicabilidad integrada (SoA)**

| Control ISO 27001:2022 | Relación NIS2 / RGPD | Estado y evidencia del Centro 1 |
|---|---|---|
| **A.5.1** — Políticas | NIS2 21.2.a; RGPD 24, 32 | Por acreditar la aprobación de política y responsables del HIS/LIS. Aportar documento vigente firmado y matriz de responsabilidades. |
| **A.5.19** — Proveedores | NIS2 21.2.d; RGPD 28, 32 | Mantenimiento remoto LIS tras vishing. Sistemas y SGSI: contrastar cláusulas del proveedor, autorizaciones, cuentas activas y registros de conexión. |
| **A.5.18** — Derechos de acceso | NIS2 21.2.i; RGPD 32 | NCm-01: permiso HCE activo tras traslado. Sistemas y RR. HH.: revocar, corregir la causa y verificar bajas de permisos mediante nueva muestra. |
| **A.8.5** — Autenticación segura | NIS2 21.2.i–j; RGPD 32 | Control por roles; MFA comprobado en una cuenta privilegiada HCE. Sistemas: acreditar también MFA del acceso remoto LIS mediante configuración y logs. |
| **A.8.24** — Criptografía | NIS2 21.2.h; RGPD 5.1.f, 32 | Cifrado HCE probado; cifrado LIS incompleto. Sistemas y proveedor LIS: completar protección y probarla sobre datos analíticos. |
| **A.5.24** — Gestión de incidentes | NIS2 21.2.b, 23; RGPD 33–34 | Expediente del incidente LIS: incidente LIS notificado a AEPD, justificante no contrastado en la auditoría interna. E03: no aportado registro del simulacro; no implica por sí solo incumplimiento. DPO/SGSI: contrastar expediente, avisos y ejercicio. |

| Control ISO 27001:2022 | Relación NIS2 / RGPD | Estado y evidencia del Centro 1 |
|---|---|---|
| **A.8.13** — Copias de seguridad | NIS2 21.2.c; RGPD 32.1.c | NCM-01/E07: base HCE excluida desde 25/09 y prueba de restauración fallida. Verificar como hipótesis la gestión de cambios (A.8.32) y la comprobación del contenido respaldado; subsanar, restaurar y validar con clínica, sin presumir causa probada. |
| **A.8.15** — Registros de eventos | NIS2 21.2.b; RGPD 32 | NCm-03/E08: una modalidad de modificación HCE sin traza, no todos los logs. Sistemas y proveedor HCE: corregir el defecto y demostrar trazabilidad de usuario, operación y fecha. |
| **A.8.8** — Vulnerabilidades técnicas | NIS2 21.2.e; RGPD 32 | Sin resultados técnicos suficientes de HIS/LIS. Sistemas: aportar análisis de vulnerabilidades, tratamiento priorizado y evidencias de cierre. |
| **A.6.3** — Formación | NIS2 21.2.g; RGPD 24, 32 | NCm-02: formación no acreditada en una persona. GRC y Admisión: formar, evaluar y ampliar la muestra sobre canal de aviso. |

Los diez controles son transversales por su capacidad de generar evidencias reutilizables, no por acreditar implantación total. OBS-01 exige verificar si mejora el umbral; E03 continúa como evidencia insuficiente sin clasificación de no conformidad.

**Obligaciones específicas que no se absorben en el SGSI común**

NIS2: dirección y supervisión (art. 20); incidentes significativos y esquema de aviso del art. 23 (24 h de alerta, 72 h de notificación y cierre en un mes), sujeto a clasificación, transposición y requisitos exigibles en España.

RGPD: RAT (art. 30), evaluación y notificación de brechas (arts. 33–34), derechos de interesados y evaluación de impacto cuando corresponda (art. 35).

ISO 27001: auditoría interna, revisión por Dirección, mantenimiento de la SoA y mejora continua, dentro del alcance definido para el Centro 1.

ENS y DORA no son obligaciones exigibles en el escenario identificado. El alcance ISO del Centro 1 no limita las obligaciones legales corporativas.

**Conclusión.** El cierre de NCM-01 exige recuperar la HCE y verificar su integridad, pero también analizar la gestión de cambios y la comprobación real de las copias. Ningún hallazgo se cerrará sin verificar su eficacia ni se atribuirá una causa raíz sin contraste.

## 6. Recomendación ejecutiva

Se solicita a Dirección aprobar un SGSI común ISO/IEC 27001:2022 para el Centro 1, con controles reutilizables para NIS2 y RGPD. No se presupuestan certificaciones ENS ni exigencias DORA sin fundamento aplicable. La prioridad es subsanar las brechas que comprometen la historia clínica antes de evaluar la certificación ISO.

**Decisiones inmediatas.** Ordenar la contención de NCM-01 y una restauración íntegra validada por clínica (≤15 días desde aprobación), comprobando gestión de cambios y verificación del contenido de las copias. Revocar el permiso obsoleto (24 h), corregir trazas, aplicar MFA remoto y cifrar LIS. El DPO debe contrastar de inmediato el expediente del vishing, la notificación AEPD y las comunicaciones pendientes.

**Seguimiento y aprobación.** Ratificar el plan noviembre de 2026–febrero de 2027 sin desplazar los plazos del plan de acciones correctivas: restantes NCm, 30 días; OBS-01, 60 días desde aprobación. Encargar informe mensual de avances, responsables, obstáculos y pruebas. Una certificación futura exige eficacia demostrada.

**Impacto económico y exposición.** Revisión GRC: 5.655 € integrada frente a 8.450 € separada; ahorro estimado de 2.795 € (33,1 %), a 65 €/h sin IVA, sin correcciones técnicas ni certificación. No actuar prolonga el riesgo asistencial y de exposición de datos. El RGPD prevé para incumplimientos de seguridad/notificación (arts. 32–34) sanciones de hasta 10 M€ o el 2 % de la facturación mundial anual, el importe mayor (art. 83.4), sin afirmar que aquí exista infracción. NIS2 exige a los Estados fijar para entidades importantes máximos sancionadores de al menos 7 M€ o el 1,4 % de la facturación mundial anual, el importe mayor (art. 34.5), sujeto al marco nacional aplicable.

**Bibliografía**

ISO/IEC (2022). ISO/IEC 27001:2022, requisitos de SGSI. Fuente oficial
UE (2022). Directiva (UE) 2022/2555, NIS2 (arts. 20–23 y 34). Fuente oficial
UE (2016). Reglamento (UE) 2016/679, RGPD (arts. 32–34 y 83). Fuente oficial
España (2022). Real Decreto 311/2022, ENS (art. 2). Fuente oficial
UE (2022). Reglamento (UE) 2022/2554, DORA. Fuente oficial
CCN-CERT (28/03/2025). Retirada de la versión previa CCN-STIC 892. Fuente oficial
Cyberzaintza (2025). Exp. 001/2025: consultor sénior, 65 €/h sin IVA. Fuente oficial