CIBER EN TACONES

Auditoría interna de seguridad

Evaluación de controles, contraste de evidencias y recomendaciones para Dirección.

CASO DE ESTUDIO SIMULADO

PYME SANITARIA MEDITERRÁNEA

ÍNDICE

1. Plan de auditoría interna.....3

2. Lista de verificación.....4

3. Ejecución y obtención de evidencias.....6

4. Hallazgos clasificados.....8

5. Informe y acciones correctivas.....10

6. Particularidades ISO/IEC 27001:2022.....11

Bibliografía.....11

1. PLAN DE AUDITORÍA INTERNA

Entidad y equipo. PYME Sanitaria Mediterránea, Centro 1 (Valencia); 5–7/10/2026. Auditor jefe independiente del equipo de implantación; auditados: Dirección, Sistemas, DPO, Admisión y responsables asistenciales.
Qué se auditará. Los procesos de admisión de pacientes, gestión de citas e historia clínica electrónica (HCE) del Centro 1, incluidos los datos de pacientes menores. Se revisarán los usuarios, equipos, sistemas, conexiones con la sanidad pública y proveedores necesarios para estos servicios. Los Centros 2 y 3 quedan fuera, excepto las dependencias compartidas que afecten a los procesos auditados.
Con qué criterios. ISO/IEC 27001:2022 (requisitos aplicables y diez controles de su Anexo A), Declaración de Aplicabilidad, análisis de riesgos, políticas y procedimientos del SGSI y obligaciones pertinentes del RGPD. Las entrevistas y pruebas seguirán las directrices de ISO 19011 e ISO/IEC 27007.
Elección de la empresa. Se elige por la criticidad de la HCE y las citas del Centro 1, que tratan datos de salud de adultos y menores.
Objetivos de auditoría. Verificar con registros, entrevistas y pruebas los controles del SGSI y comunicar a Dirección las desviaciones y riesgos detectados.

Selección y justificación de la muestra

Se seleccionan diez controles por los riesgos de acceso indebido, robo de credenciales, pérdida de historias clínicas y exposición de datos sanitarios:

- A.5.15/A.5.18: permisos de admisión y personal sanitario frente a autorizaciones; A.8.5/A.6.3: cuentas clínicas y preparación ante phishing o suplantación.
- A.8.13: respaldos y restauración de la HCE; A.8.15/A.8.16: trazabilidad de consultas y revisión de alertas.
- A.8.24/A.5.24/A.5.34: cifrado clínico, preparación ante incidentes y protección de datos de pacientes y terceros.

Tamaño de muestra previsto. Cinco cuentas (dos asistenciales, dos de admisión y una privilegiada), cuatro modificaciones de permisos, cinco accesos, tres alertas, tres copias, una restauración y tres registros de formación, además de expedientes de incidentes y proveedores cuando existan. Se registrarán las limitaciones de la muestra.

Agenda de auditoría simulada (5–7 de octubre de 2026)

Día 1 · 09:00–13:00	Apertura con Dirección, Seguridad, Sistemas y DPO; alcance, políticas, riesgos y responsabilidades.
Día 2 · 09:00–13:00	Entrevistas y comprobación de permisos, registros, copias y configuraciones.
Día 3 · 09:00–12:00	Evaluación de evidencias y cierre con Dirección y responsables.

Apertura y riesgos de auditoría. Se confirman alcance, criterios, agenda, entrevistados y canal de evidencias. Independencia: el auditor no implantó el SGSI. Ante indisponibilidad de responsables o registros: solicitudes fechadas y seguimiento. Confidencialidad: acceso restringido y datos clínicos ficticios. Toda limitación queda documentada.

2. LISTA DE VERIFICACIÓN DE AUDITORÍA INTERNA

PYME Sanitaria Mediterránea · Centro 1 | ISO/IEC 27001:2022

Se contrastarán requisitos documentados con registros fechados y funcionamiento real. Resultado, gravedad y notas: campos pendientes en el CSV de trabajo.

Acceso clínico ISO 27001:2022 A.5.15	**Pregunta:** ¿Quién aprueba los perfiles de admisión y asistenciales en HCE/citas? ¿Cuándo se revisó la matriz y se comprueba que los permisos funcionan como está previsto? **Evidencia:** Política y matriz vigente con fecha y aprobación; usuarios activos; demostración de permisos reales de 2 cuentas de admisión y 2 asistenciales. **Criterio:** Las 4 cuentas se ajustan a permisos aprobados; admisión no puede consultar datos clínicos ajenos a su función. Desviaciones justificadas y autorizadas.
Derechos de acceso ISO 27001:2022 A.5.18	**Pregunta:** ¿Cada cuánto se revisan los permisos de HCE/citas, quién lo hace y cómo se tramitan bajas y cambios de puesto? **Evidencia:** Procedimiento con frecuencia y plazos; 3 últimas revisiones fechadas, responsables y correcciones; 4 expedientes de cambios de acceso, con al menos una baja y un cambio de función si existen. **Criterio:** Revisiones hechas en plazo y trazables; modificaciones ejecutadas según autorización y plazo aprobado; sin permisos obsoletos injustificados.
Preparación ante incidentes ISO 27001:2022 A.5.24	**Pregunta:** Ante un acceso irregular a HCE, ¿quién recibe el aviso y activa el procedimiento? ¿Cuándo se comprobó por última vez esa preparación? **Evidencia:** Procedimiento vigente, roles y canales; entrevista a Sistemas y DPO; último ejercicio o activación registrada, si existe, y fechas. **Criterio:** Responsables conocen el circuito; los recursos y pasos previstos se acreditan; ejercicios realizados si están exigidos por el procedimiento.
Privacidad clínica ISO 27001:2022 A.5.34	**Pregunta:** ¿Están actualizados los tratamientos de HCE y citas —incluidos datos de menores— y qué proveedores acceden a información personal por cuenta del hospital? **Evidencia:** RAT con fechas de revisión; relación de proveedores y accesos; contratos de encargo art. 28 RGPD para los que actúen como encargados. **Criterio:** RAT refleja operaciones del Centro 1; roles de terceros comprobados y acuerdos exigibles vigentes, con medidas y obligaciones verificables.
Formación ISO 27001:2022 A.6.3	**Pregunta:** ¿Con qué frecuencia se forma al personal de admisión y asistencial sobre phishing/vishing y datos clínicos? ¿Cómo se comprueba su aprendizaje? **Evidencia:** Plan y periodicidad; contenidos; 3 registros fechados de formación/evaluación; entrevista a personal de admisión y clínico. **Criterio:** Formación impartida conforme al plan; asistencia y seguimiento acreditados; entrevistados conocen cómo avisar de una suplantación.

Autenticación ISO 27001:2022 A.8.5	**Pregunta:** ¿Qué autenticación exige el hospital en HCE/citas y para la cuenta privilegiada de Sistemas? ¿Cómo revisa y controla excepciones? **Evidencia:** Requisitos aprobados y fecha de revisión; configuración efectiva de las 5 cuentas previstas, incluida una privilegiada; autorizaciones de excepciones. **Criterio:** Configuración coincide con requisitos definidos por riesgo; mecanismos exigidos activos y excepciones justificadas y vigentes.
Copias HCE ISO 27001:2022 A.8.13	**Pregunta:** ¿Con qué frecuencia se respaldan los datos de HCE? ¿Quién comprueba fallos y cuándo se restauró por última vez una copia? **Evidencia:** Política y programación real; 3 ejecuciones fechadas y alertas; última restauración con fecha, duración, datos recuperados y validación de integridad. **Criterio:** Copias ejecutadas según frecuencia; fallos detectados y tratados; restauración verificada con datos íntegros y utilizables.
Registros HCE ISO 27001:2022 A.8.15	**Pregunta:** ¿Quedan registrados quién consulta o modifica una historia clínica, cuándo y qué operación realiza? ¿Durante cuánto tiempo se conservan los logs? **Evidencia:** Configuración y retención aprobada; 5 eventos fechados de HCE; control de acceso y protección de logs. **Criterio:** Eventos de la muestra atribuibles y completos; captura y conservación acordes con reglas; registros protegidos contra cambios indebidos.
Monitorización ISO 27001:2022 A.8.16	**Pregunta:** ¿Con qué frecuencia se examinan alertas por consultas masivas o accesos atípicos a HCE? ¿Qué plazo y escalado se aplican? **Evidencia:** Reglas y frecuencia; 3 alertas fechadas, hora de detección/revisión, decisión, responsable, actuación y estado. **Criterio:** Las alertas se evalúan dentro de plazos definidos; decisiones y escalados documentados, incluidas las pendientes justificadas.
Cifrado clínico ISO 27001:2022 A.8.24	**Pregunta:** ¿Qué cifrado exige el SGSI para la HCE y el intercambio con sanidad pública? ¿Cuándo se revisó su configuración y certificados? **Evidencia:** Política vigente; configuración observada del almacenamiento HCE y canal externo; certificados, vigencia y revisiones registradas. **Criterio:** Protección criptográfica efectiva según requisitos aprobados; certificados vigentes y excepciones evaluadas y autorizadas.

Método: revisión documental, entrevista y observación de configuraciones. Una declaración verbal no acredita, por sí sola, la ejecución del control.

3. EJECUCIÓN Y OBTENCIÓN DE EVIDENCIAS

PYME Sanitaria Mediterránea · Centro 1 · Auditoría interna ISO/IEC 27001:2022

Ejecución simulada: 5–7 de octubre de 2026. Expediente ficticio creado para este caso (E01–E10). Se contrastan documentos (D), entrevistas (E) y observación técnica (O); ninguna declaración verbal se considera prueba suficiente por sí sola.

A.5.15 · Acceso clínico

Solicitado: Política, matriz de roles y 4 cuentas (2 admisión, 2 asistenciales).

Obtenido: E01: matriz aprobada 03/07/2026; entrevista con admisión; comprobación en HCE/citas de las 4 cuentas: admisión sin permisos de consulta clínica; personal sanitario limitado a su rol.

Técnicas: D+E+O · **Resultado preliminar:** Conforme.

A.5.18 · Derechos de acceso

Solicitado: Procedimiento, tres revisiones y 4 expedientes (2 altas, 1 traslado, 1 baja).

Obtenido: E02: revisiones trimestrales firmadas (15/01, 16/04 y 15/07/2026). En CAMBIO-04, traslado de puesto el 18/08, el perfil anterior seguía activo el 06/10; el procedimiento fija revocación en 24 h. Las revisiones examinadas son anteriores al traslado.

Técnicas: D+E+O · **Resultado preliminar:** No conforme.

A.5.24 · Preparación ante incidentes

Solicitado: Procedimiento, responsables, última prueba y entrevistas a Sistemas/DPO.

Obtenido: E03: procedimiento de 10/02/2026 exige ejercicio semestral; Sistemas y DPO describen el circuito de aviso. Tras solicitud y recordatorio, no se aporta acta, convocatoria ni registro alternativo del primer semestre. No se acredita el ejercicio; tampoco se demuestra que no ocurriera.

Técnicas: D+E · **Resultado preliminar:** Evidencia insuficiente / parcial.

A.5.34 · Privacidad clínica

Solicitado: RAT de HCE y citas; proveedores y acuerdos de encargo cuando procedan.

Obtenido: E04: RAT actualizado 20/07/2026 recoge historia clínica, menores y citas. Se contrastan dos prestadores con acceso por cuenta del centro: acuerdos firmados y vigentes; DPO identifica responsabilidades.

Técnicas: D+E · **Resultado preliminar:** Conforme.

A.6.3 · Formación

Solicitado: Plan anual y 3 registros de personal de admisión/asistencia; entrevistas.

Obtenido: E05: plan 2026 exige formación anual sobre phishing/vishing. De 3 trabajadores, 2 presentan asistencia y evaluación; para FOR-AD-02 no se aporta justificante ni tras requerir evidencia alternativa. En entrevista desconoce el canal de aviso. Conclusión limitada a esa cuenta.

Técnicas: D+E · **Resultado preliminar:** No conforme.

A.8.5 · Autenticación

Solicitado: Requisitos y configuración de las 5 cuentas previstas; excepciones.

Obtenido: E06: se observan 2 cuentas asistenciales, 2 de admisión y 1 privilegiada: autenticación conforme a la política del centro; MFA activo en cuenta privilegiada y sin excepciones no autorizadas.

Técnicas: D+O · **Resultado preliminar:** Conforme.

A.8.13 · Copias HCE

Solicitado: Configuración, 3 últimas ejecuciones, alertas y última restauración.

Obtenido: E07: la política exige copia diaria de la base HCE. La configuración la excluye desde 25/09, aunque los logs de 04–06/10 indican «tarea terminada». En entorno controlado, restauración de datos de prueba del 06/10 no recupera la base; Sistemas valida el fallo.

Técnicas: D+E+O · **Resultado preliminar:** No conforme.

A.8.15 · Registros HCE

Solicitado: Parámetros de auditoría, retención y muestra de 5 operaciones fechadas.

Obtenido: E08: de cinco operaciones HCE, cuatro generan logs trazables. Una modificación clínica de prueba (EVT-04, 05/10) consta en la base, pero no en el registro de auditoría; se reproduce en entorno controlado. No se extrapola a otras operaciones.

Técnicas: D+O · **Resultado preliminar:** No conforme.

A.8.16 · Monitorización

Solicitado: Reglas, periodicidad y 3 alertas con fechas y gestión.

Obtenido: E09: tres alertas con hora de detección, revisión, analista y decisión dentro de plazo. La regla solo alerta desde seis consultas consecutivas; una prueba controlada de cinco consultas a expedientes diferentes no genera aviso. Se propone revisar el umbral según riesgo, sin afirmar incumplimiento.

Técnicas: D+E+O · **Resultado preliminar:** Conforme; oportunidad de mejora.

A.8.24 · Cifrado clínico

Solicitado: Política, configuración de almacenamiento HCE y enlace con sanidad pública; certificados.

Obtenido: E10: configuración observada acredita cifrado de almacenamiento HCE y canal TLS activo hacia la integración; certificado válido hasta 2027 y revisión técnica registrada 01/09/2026.

Técnicas: D+O · **Resultado preliminar:** Conforme.

Límites: expediente enteramente simulado, exclusivo del Centro 1. El resultado por control es preliminar y solo alcanza la muestra identificada E01–E10; su gravedad se fundamentará posteriormente según requisito, evidencia, extensión e impacto.

4. HALLAZGOS CLASIFICADOS

PYME Sanitaria Mediterránea · Centro 1 · Auditoría interna ISO/IEC 27001:2022

Hallazgos derivados del expediente de auditoría simulado (5–7/10/2026). La clasificación se limita a las muestras E01–E10 y diferencia el requisito documentado de la ejecución comprobada.

Hallazgo 01 — No conformidad mayor (NCM-01)

Requisito o medida de referencia: ISO/IEC 27001:2022, A.8.13 — Copias de seguridad de la información; BK-POL-01: copia diaria de la base de datos de la historia clínica electrónica (HCE).

Evidencia objetiva: E07: BK-CONFIG-01 excluye la base clínica desde el 25/09/2026. Los registros BK-LOG-1004/1005/1006 muestran «tarea terminada» al respaldar otros volúmenes. TEST-REST-20261006 no recuperó la base HCE en un entorno aislado; VAL-REST-01 recoge la validación negativa de Sistemas.

Descripción del incumplimiento o mejora: Las tareas reportan finalización, pero no incluyen el activo clínico cuya copia exige BK-POL-01. La restauración ensayada demuestra que ese conjunto de información no es recuperable mediante las copias examinadas.

Clasificación justificada: NCM: fallo material sostenido en la protección y recuperación de un activo central para la atención sanitaria del Centro 1. Compromete la disponibilidad de historias clínicas ante pérdida o ransomware; no se acredita una copia alternativa eficaz.

Hallazgo 02 — No conformidad menor (NCm-01)

Requisito o medida de referencia: ISO/IEC 27001:2022, A.5.18 — Derechos de acceso; PR-IDM-02: retirar en un máximo de 24 horas los permisos del puesto anterior.

Evidencia objetiva: E02: el expediente CAMBIO-04 registra traslado el 18/08/2026; TEST-ACC-02 confirma que el 06/10 continuaba activo el perfil anterior de consulta HCE. Las revisiones trimestrales de 15/01, 16/04 y 15/07 están firmadas y son anteriores al traslado.

Descripción del incumplimiento o mejora: No se revocó el permiso anterior dentro del plazo establecido. No se ha demostrado un acceso indebido ni se atribuye el fallo a las revisiones trimestrales realizadas antes del traslado.

Clasificación justificada: NCm: desviación acreditada en uno de los cuatro expedientes examinados; crea exposición innecesaria de información clínica, sin evidencia suficiente de un fallo generalizado del proceso.

Hallazgo 03 — No conformidad menor (NCm-02)

Requisito o medida de referencia: ISO/IEC 27001:2022, A.6.3 — Concienciación, educación y formación en seguridad de la información; FOR-PLAN-2026: formación anual sobre phishing/vishing.
Evidencia objetiva: E05: dos de tres empleados examinados acreditan asistencia y evaluación; FOR-AD-02 no presenta justificante de formación en 2026 ni alternativa tras AUD-REQ-05 (06/10). En INT-AD-02 no identifica el canal para comunicar una llamada de suplantación.
Descripción del incumplimiento o mejora: En la muestra de admisión no se acredita la formación anual exigida ni el conocimiento operativo del canal de aviso por parte de esa persona.
Clasificación justificada: NCm: caso individual de tres examinados, con incidencia en la detección temprana de vishing dirigido al personal que gestiona citas y datos de pacientes; no se extrapola a los 220 empleados.

Hallazgo 04 — No conformidad menor (NCm-03)

Requisito o medida de referencia: ISO/IEC 27001:2022, A.8.15 — Registro de eventos; LOG-POL-02: registrar lecturas y modificaciones en la HCE.
Evidencia objetiva: E08: de cinco operaciones examinadas, EVT-04 (modificación de episodio clínico ficticio el 05/10) consta en DB-TEST-04, sin entrada correlativa en LOG-HCE-05. TEST-LOG-01 reproduce la misma operación sin generar evento.
Descripción del incumplimiento o mejora: Una modalidad de modificación de información clínica no produce la traza exigida, aunque las otras cuatro operaciones de la muestra sí resultaron registradas.
Clasificación justificada: NCm: defecto técnico reproducible y acotado al tipo de operación probado; dificulta reconstruir modificaciones de episodios clínicos, pero no acredita pérdida general de todos los registros de auditoría.

Hallazgo 05 — Observación (OBS-01)

Requisito o medida de referencia: ISO/IEC 27001:2022, A.8.16 — Actividades de monitorización; MON-POL-01 y regla de detección MON-RULE-03.
Evidencia objetiva: E09: ALERT-01/02/03 acreditan revisión diaria y tratamiento en plazo. MON-RULE-03 alerta desde seis consultas consecutivas a historias distintas por cuenta; TEST-MON-01 ejecutó cinco consultas a expedientes ficticios sin generar aviso.
Descripción del incumplimiento o mejora: Se recomienda contrastar el umbral con el riesgo de consultas sucesivas no justificadas a historias clínicas y valorar reglas adicionales por perfil y contexto asistencial; no se ha demostrado vulneración de la configuración aprobada.
Clasificación justificada: OBS: oportunidad fundamentada de mejorar la detección temprana, sin incumplimiento acreditado. Las tres alertas revisadas sí se gestionaron según el procedimiento.
Comprobación pendiente (no clasificada): E03/A.5.24: no se aportó registro del simulacro semestral tras dos requerimientos. Se mantiene como evidencia insuficiente; debe ampliarse el contraste antes de afirmar que no se ejecutó el ejercicio.

5. INFORME DE AUDITORÍA INTERNA Y ACCIONES CORRECTIVAS

PYME Sanitaria Mediterránea · Centro 1, Valencia · ISO/IEC 27001:2022 · Auditoría simulada: 5–7 de octubre de 2026

Resumen ejecutivo

Se examinaron diez controles: una no conformidad mayor, tres menores y una observación. La base clínica HCE queda excluida de las copias y no se recupera en la prueba, lo que amenaza la continuidad asistencial. Dictamen previo a certificación: desfavorable mientras NCM-01 permanezca abierta y sin cierre eficaz acreditado.

Alcance, criterios y método

Centro 1: admisión, citas y HCE, incluidos menores y dependencias compartidas. Criterios: ISO/IEC 27001:2022, SoA y procedimientos; método: documentos, entrevistas y observación técnica. Entrevistados: Sistemas, DPO, Admisión y personal asistencial. Revisados: matriz de acceso, cambios de permisos, RAT, formación, copias, restauración, logs, alertas y cifrado (E01–E10).

Hallazgos y valoración

NCM-01 (E07): respaldo HCE sin base clínica y restauración fallida. NCm-01 (E02): permiso antiguo sin revocar. NCm-02 (E05): formación anual no acreditada en un empleado de admisión. NCm-03 (E08): modificación HCE sin traza. OBS-01 (E09): evaluar umbral de consultas consecutivas.

Plan de acciones correctivas propuesto

ID	Acción propuesta	Responsable	Plazo*	Prueba de cierre
NCM-01	Proteger los datos clínicos de inmediato; incluir base HCE, investigar causa y restaurar en prueba.	Sistemas + responsable HCE	Ahora; 15 días	Copia íntegra, restauración validada por clínica y registros posteriores sin errores.
NCm-01	Revocar permiso; investigar fallo y corregir proceso de traslados.	Sistemas + RR. HH.	24 h; 30 días	Registro de revocación y muestra posterior con bajas en ≤24 h.
NCm-02	Formar al empleado y corregir seguimiento de formación de admisión.	GRC + Admisión	30 días	Asistencia, evaluación y nueva muestra con canal de aviso conocido.
NCm-03	Corregir trazas de modificaciones HCE e investigar causa.	Sistemas + proveedor HCE	30 días	Pruebas fechadas con usuario, operación y traza; muestra posterior.
OBS-01	Valorar umbral de consultas sucesivas según perfiles clínicos.	Seguridad + responsable HCE	60 días	Análisis de riesgo, prueba de alerta y decisión justificada.

* Plazos desde aprobación de Dirección. La contención de NCM-01 es inmediata; 15 días para su corrección y prueba.

Prioridades: en 90 días, cerrar hallazgos y verificar restauración y alertas; a 12 meses, consolidar revisiones de accesos, formación y trazas, sujeto a Dirección. Esta asignará recursos y Auditoría Interna verificará cierres. E03 sigue pendiente de contraste, sin clasificación.

6. Particularidades de la auditoría ISO/IEC 27001:2022

La auditoría interna realizada en el Centro 1 de PYME Sanitaria Mediterránea permite evaluar la conformidad y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al apartado 9.2 de ISO/IEC 27001:2022. Sus conclusiones sirven a Dirección para corregir las desviaciones antes de solicitar una certificación por tercera parte.

La certificación comprende dos etapas. En la Etapa 1 (Stage 1), el organismo certificador revisa la documentación, el alcance y la preparación del SGSI. En la Etapa 2 (Stage 2), contrasta su implantación mediante entrevistas, registros y comprobaciones operativas. En España, la certificación debe realizarla un organismo con la acreditación correspondiente, otorgada por ENAC o reconocida conforme a los acuerdos aplicables.

Nuestro informe anticipa cuestiones que examinará el auditor de certificación. En particular, la no conformidad mayor detectada en las copias de seguridad de la historia clínica electrónica exige corregir la configuración y demostrar una restauración satisfactoria. La existencia de una política de respaldo no acredita por sí sola la recuperación efectiva de los datos clínicos.

Una vez obtenida la certificación, el SGSI queda sujeto a auditorías de vigilancia, normalmente anuales, y a una recertificación cada tres años. Por ello, la conformidad requiere seguimiento continuo y verificación de la eficacia de las acciones correctivas.

Bibliografía

ISO/IEC. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

ISO/IEC. (2022). ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.

ISO. (2018). ISO 19011:2018. Guidelines for auditing management systems.

ISO/IEC. (2020). ISO/IEC 27007:2020. Information security management systems auditing — Guidelines.

Unión Europea. (2016). Reglamento (UE) 2016/679 (RGPD), arts. 5, 9, 28 y 32.