CIBER EN TACONES

Análisis y tratamiento de riesgos

Valoración de activos, amenazas y riesgos con MAGERIT v3 y propuestas de tratamiento para Dirección.

CASO DE ESTUDIO SIMULADO

PYME SANITARIA MEDITERRÁNEA

ÍNDICE

1. Caracterización y valoración de activos....3
1.1. Dependencias entre activos....4
2. Caracterización de amenazas y riesgo potencial....4
3. Caracterización de salvaguardas....6
4. Mapa de riesgo priorizado....7
5. Tratamiento del riesgo....8
5.1. Registro de tratamiento de riesgos....8
6. Conexión con la Declaración de Aplicabilidad (SoA)....10
7. Reflexión metodológica y resumen ejecutivo....11
8. Bibliografía....12

1. Caracterización y valoración de activos

El análisis se centra en el Centro 1 de PYME Sanitaria Mediterránea: admisión, gestión de citas e historia clínica electrónica, incluidos los sistemas, equipos, comunicaciones y servicios que los soportan. Los Centros 2 y 3 quedan fuera salvo dependencias compartidas que afecten directamente al alcance.

Los activos se valoran en Disponibilidad, Integridad, Confidencialidad, Trazabilidad y Autenticidad (DICTA), de 1 a 10: 1–2 bajo, 3–4 moderado-bajo, 5–6 medio, 7–8 alto y 9–10 crítico. La puntuación refleja el impacto para el Centro 1 si se pierde o degrada cada dimensión.

ID	Activo	Tipo	DICTA	Justificación
A01	Historias clínicas electrónicas	Información	D9 · I9 · C10 · T9 · A9	Su pérdida o alteración puede afectar la atención; una exposición compromete datos de salud.
A02	Datos de admisión y citas	Información	D8 · I8 · C8 · T7 · A7	Errores de identificación o cita pueden causar duplicidades, retrasos o asignaciones incorrectas.
A03	Sistema de historia clínica electrónica	Aplicación	D9 · I9 · C9 · T8 · A8	Una caída bloquea historias; un compromiso permite consultas o cambios clínicos indebidos.
A04	Sistema de admisión y gestión de citas	Aplicación	D8 · I8 · C7 · T7 · A7	Un fallo impide admisiones o agendas y puede generar citas o datos incorrectos.
A05	Portal de citas online	Servicio	D7 · I7 · C6 · T6 · A7	Su caída elimina el canal online; una manipulación puede generar citas o datos incorrectos.
A06	Integración con sistema público de salud	Comunicaciones	D8 · I9 · C9 · T9 · A9	Una interrupción detiene el intercambio público; una interceptación puede exponer datos clínicos.
A07	Cuentas e identidades de usuario	Información	D6 · I8 · C9 · T10 · A10	Una cuenta comprometida puede acceder como usuario legítimo y ocultar la autoría real.
A08	Equipos de usuario	Equipamiento	D7 · I7 · C7 · T6 · A6	Un equipo comprometido puede interrumpir el trabajo o abrir acceso a información clínica.

ID	Activo	Tipo	DICTA	Justificación
A09	Red y conectividad	Comunicaciones	D8 · I8 · C8 · T7 · A7	Una caída afecta HCE, admisión e integración; manipular el tráfico compromete los datos.
A10	Instalaciones físicas del Centro 1	Instalaciones	D8 · I7 · C4 · T4 · A4	Una indisponibilidad grave puede impedir la actividad asistencial y afectar equipos, comunicaciones y puestos; el impacto directo en C/T/A es menor que en activos digitales.

1.1. Dependencias entre activos

Activo	Depende de
A01	A03 · A07 · A08 · A09
A02	A04 · A07 · A08 · A09
A05	A04 · A09
A06	A03/A04 · A07 · A09
A10	A03 · A04 · A08 · A09

Activos raíz: A01 Historias clínicas electrónicas y A02 Datos de admisión y citas, porque concentran la información esencial de los procesos incluidos y dependen de los activos de soporte representados en el esquema.

2. Caracterización de amenazas y riesgo potencial

El análisis se concentra en A01, A03, A06 y A07 por ser los activos que presentan mayor criticidad dentro del alcance. Para cada uno se identifican tres amenazas relevantes, tomando como referencia el catálogo de amenazas de MAGERIT v3, Libro II. Para cada amenaza se estima su frecuencia, la degradación que produciría sobre las dimensiones DICTA afectadas y el riesgo potencial resultante.

Al no disponerse de históricos reales de incidentes, las valoraciones se basan en el tipo de activo, su utilización y las consecuencias que tendría cada amenaza para el Centro 1. Para mantener un criterio homogéneo, se utiliza una escala cualitativa de frecuencia y una degradación de 0 a 10 por dimensión.

ID	Activo / amenaza	MAGERIT / frecuencia	Degradación	Riesgo potencial	Justificación
R01	A01 · Acceso no autorizado o fuga	A.11 · Acceso no autorizado / Media	C10 · T8	C10,0 · T7,2	Puede exponer datos de salud y dificultar identificar quién accedió o extrajo información.

ID	Activo / amenaza	MAGERIT / frecuencia	Degradación	Riesgo potencial	Justificación
R02	A01 · Alteración accidental	E.15 · Alteración accidental de la información / Media	I10 · T8	I9,0 · T7,2	Un dato clínico incorrecto puede afectar decisiones asistenciales y exige poder atribuir el cambio.
R03	A01 · Pérdida o destrucción accidental	E.18 · Destrucción de información / Baja	D9 · I9 · T7	D0,81 · I0,81 · T0,63	Una pérdida puede impedir acceso, eliminar datos o dejar registros incompletos y dificultar reconstruir lo ocurrido.
R04	A03 · Ransomware o cifrado	A.8 · Difusión de software dañino / Media	D10 · I8	D9,0 · I7,2	Puede impedir el acceso a las historias clínicas y comprometer información necesaria para la atención.
R05	A03 · Error de configuración	E.4 · Errores de configuración / Media	D8 · I7	D7,2 · I6,3	Puede provocar indisponibilidad o un tratamiento inadecuado de la información clínica.
R06	A03 · Fallo técnico o mantenimiento incorrecto	E.21 · Errores de mantenimiento/actualización de software / Media	D9 · I7	D8,10 · I6,30	Una intervención defectuosa puede dejar el sistema clínico indisponible o funcionando incorrectamente.
R07	A06 · Acceso no autorizado o exfiltración	A.11 · Acceso no autorizado / Baja	C10 · T8	C0,90 · T0,72	Puede exponer información intercambiada con el sistema público de salud.
R08	A06 · Corte de comunicaciones	I.8 · Fallo de servicios de comunicaciones / Media	D9	D7,2	Impide temporalmente el intercambio de información necesario para los procesos incluidos.

ID	Activo / amenaza	MAGERIT / frecuencia	Degradación	Riesgo potencial	Justificación
R09	A06 · Modificación deliberada de información transmitida	A.15 · Modificación deliberada de la información / Baja	I10 · T9 · A9	I0,90 · T0,81 · A0,81	Una alteración puede comprometer contenido, origen, destino y autenticidad del intercambio.
R10	A07 · Robo de credenciales o phishing	A.5 · Suplantación de la identidad del usuario / Media	C9 · T10 · A10	C8,1 · T10,0 · A10,0	Permite actuar como usuario legítimo y dificulta la atribución real de las acciones.
R11	A07 · Asignación incorrecta de permisos	E.2 · Errores del administrador / Media	C8 · I7	C7,2 · I5,6	Puede permitir consultar o modificar información ajena a las funciones del usuario.
R12	A07 · Uso indebido de credenciales legítimas / abuso de privilegios	A.6 · Abuso de privilegios de acceso / Media	C9 · T10 · A10	C8,10 · T10,00 · A10,00	Una identidad válida usada fuera de su necesidad autorizada puede permitir accesos indebidos y dificultar atribuir la finalidad.

Riesgo potencial = Valor DICTA × (Degradación / 10) × Frecuencia anual. La degradación se divide entre 10 porque se valora en escala 0–10. Para el cálculo se adopta Media = 1 vez/año y Baja = 0,1 veces/año. Ejemplos: R10-T = 10 × (10/10) × 1 = 10,0; R07-C = 9 × (10/10) × 0,1 = 0,90.

3. Caracterización de salvaguardas

Las salvaguardas son medidas destinadas a reducir la probabilidad de materialización de una amenaza o limitar sus consecuencias. La información disponible del caso no permite acreditar qué medidas están implantadas ni su eficacia real; por ello se identifican salvaguardas propuestas para el Centro 1 y una eficacia estimada que deberá comprobarse posteriormente mediante evidencias de funcionamiento.

Criterio de eficacia. Se utilizan valores del 40–50 % cuando la eficacia depende especialmente de la actuación humana; del 60–70 % para medidas preventivas, organizativas o de recuperación con efecto directo; y hasta el 75 % cuando la protección actúa de forma especialmente directa. Cuando varias salvaguardas afectan al mismo factor se utiliza la media de sus eficacias, no la suma.

ID	Salvaguardas propuestas / eficacia	Control Anexo A	Qué reducen
R01	Acceso por función (70 %); registro/seguimiento (50 %)	A.5.15 · A.8.15 · A.8.16	Reduce accesos indebidos y permite identificar anomalías.

ID	Salvaguardas propuestas / eficacia	Control Anexo A	Qué reducen
R02	Permisos de modificación (70 %); historial/recuperación (60 %)	A.5.15 · A.8.15 · A.8.13	Reduce cambios accidentales y facilita recuperar información.
R03	Copias verificadas (75 %); revisión de borrados (60 %)	A.8.13 · A.5.18	Limita pérdida definitiva y operaciones accidentales con privilegios innecesarios.
R04	Copias restaurables (75 %); respuesta/aislamiento (60 %)	A.8.13 · A.5.24	Reduce consecuencias del cifrado y facilita recuperación y contención.
R05	Autorización de cambios (70 %); reversión (60 %)	A.5.18 · A.5.30	Reduce errores de configuración y facilita volver a estado funcional.
R06	Mantenimiento/ recuperación (65 %); restauración (75 %)	A.5.30 · A.8.13	Reduce impacto de fallos y acelera recuperación del HCE.
R07	Acceso entre sistemas (70 %); cifrado (75 %); minimización (60 %)	A.5.14 · A.5.15 · A.8.24 · A.8.12	Reduce acceso/exfiltración durante el intercambio.
R08	Conexión redundante (70 %); disponibilidad del proveedor (50 %)	A.5.30 · A.5.31	Reduce duración de interrupciones y facilita recuperación.
R09	Cifrado/integridad (75 %); registro de intercambios (60 %)	A.8.24 · A.8.15 · A.5.14	Reduce alteración no detectada y mejora trazabilidad.
R10	MFA (75 %); formación/simulaciones de phishing (45 %)	A.8.5 · A.6.3	Dificulta que una credencial robada baste y reduce el engaño.
R11	Altas/cambios/bajas (70 %); revisión de permisos (60 %)	A.5.18	Reduce permisos excesivos, incorrectos u obsoletos.
R12	Monitorización de privilegios (65 %); revisión periódica (60 %)	A.8.16 · A.5.18 · A.8.15	Reduce abuso de privilegios y mejora atribución.

4. Mapa de riesgo priorizado

Para representar cada riesgo se toma como referencia el mayor valor obtenido entre las dimensiones DICTA afectadas, por ser la consecuencia más severa asociada a la amenaza. El potencial refleja la exposición sin salvaguardas; el residual estima la exposición que permanecería tras aplicar las medidas propuestas con la eficacia indicada. Riesgo residual ≈ Riesgo potencial × (1 − eficacia conjunta).

ID	Potencial	Eficacia conjunta	Residual
R01	10,00	60 %	4,00
R02	9,00	65 %	3,15
R03	0,81	67,5 %	0,26
R04	9,00	67,5 %	2,93
R05	7,20	65 %	2,52
R06	8,10	70 %	2,43

ID	Potencial	Eficacia conjunta	Residual
R07	0,90	68,3 %	0,29
R08	7,20	60 %	2,88
R09	0,90	67,5 %	0,29
R10	10,00	60 %	4,00
R11	7,20	65 %	2,52
R12	10,00	62,5 %	3,75

Impacto	Potencial Baja	Potencial Media	Residual Baja	Residual Media
Crítico	R03 · R07 · R09	R01 · R02 · R04 · R06 · R10 · R12	—	—
Alto	—	R05 · R08 · R11	—	—
Medio	—	—	—	—
Moderado-bajo	—	—	R03 · R07 · R09	R01 · R02 · R04 · R05 · R06 · R08 · R10 · R11 · R12
Bajo	—	—	—	—

Nivel	Intervalo	Potencial	Residual
Crítico	8,01–10	R01, R02, R04, R06, R10, R12	—
Alto	6,01–8	R05, R08, R11	—
Medio	4,01–6	—	—
Moderado-bajo	2,01–4	—	R01, R02, R04–R06, R08, R10–R12
Bajo	0–2	R03, R07, R09	R03, R07, R09

Ejemplo de lectura: R10 — Robo de credenciales o phishing. Potencial 10,00; eficacia conjunta media 60 % por MFA (75 %) y formación/simulaciones (45 %). Residual: 10 × (1 − 0,60) = 4,00.

5. Tratamiento del riesgo

Apetito de riesgo. La Dirección acepta riesgos residuales de nivel Bajo, Moderado-bajo y Medio cuando las medidas previstas son adecuadas y no se mantiene una exposición relevante sobre datos de salud, identidades o continuidad clínica. Los riesgos Altos o Críticos deberán ser tratados antes de su aceptación.

A partir del riesgo residual obtenido y del apetito definido, se establece la decisión de tratamiento. Para cada riesgo se documenta la opción elegida y su justificación, el residual objetivo y el responsable. Los riesgos sensibles pueden mantenerse en tratamiento aunque su residual inicial ya esté dentro del apetito.

5.1. Registro de tratamiento de riesgos

Riesgo	Opción / justificación	Residual objetivo	Responsable
R01	Reducir — dato de salud C=10 y residual 4,00; se refuerza por sensibilidad.	Bajo	Seguridad/GRC + DPO + clínica
R02	Reducir — una alteración puede afectar decisiones asistenciales.	Bajo	Sistemas + clínica

Riesgo	Opción / justificación	Residual objetivo	Responsable
R03	Aceptar condicionado — residual bajo tras recuperación; Dirección acepta tras verificar medidas.	Bajo	Dirección; Sistemas ejecuta
R04	Reducir — ransomware afecta continuidad del HCE.	Bajo	Sistemas + Seguridad/GRC
R05	Evitar — eliminar cambios de producción fuera del proceso autorizado.	Bajo	Sistemas
R06	Reducir — fallo técnico afecta disponibilidad del HCE.	Bajo	Sistemas
R07	Reducir — intercambio de datos de salud exige protección reforzada.	Bajo	Sistemas + DPO + Seguridad/GRC
R08	Transferir parcialmente + reducir — parte depende del proveedor, manteniendo continuidad propia.	Bajo	Sistemas + Dirección
R09	Aceptar condicionado — residual bajo con integridad/cifrado; Dirección acepta tras verificar medidas.	Bajo	Dirección; Sistemas ejecuta
R10	Reducir — credencial robada da acceso a sistemas clínicos.	Bajo	Seguridad/GRC + Sistemas
R11	Reducir — permisos excesivos pueden persistir sin control del ciclo de vida.	Bajo	Sistemas + responsables de área
R12	Reducir — afecta trazabilidad y autenticidad y requiere control de privilegios.	Bajo	Seguridad/GRC + Sistemas

Detalle de tratamiento

Riesgo	Salvaguardas a implantar	Coste estimado	Plazo
R01	Revisión de accesos, alertas y perfiles	4.000–7.000 €	2–3 meses
R02	Validaciones, registro de cambios y recuperación	2.000–4.000 €	2 meses
R03	Copias verificadas y pruebas de restauración	Incluido en continuidad/copias	1–2 meses
R04	Copias separadas, restauración y respuesta	5.000–9.000 €	2–4 meses
R05	Gestión formal de cambios y reversión	1.000–2.500 €	1–2 meses

Riesgo	Salvaguardas a implantar	Coste estimado	Plazo
R06	Mantenimiento documentado y recuperación	2.000–4.000 €	2–3 meses
R07	Cifrado, autenticación y minimización	3.000–6.000 €	2–3 meses
R08	SLA, conexión alternativa y contingencia	3.000–6.000 € primer año	2–4 meses
R09	Integridad, cifrado y trazabilidad	Incluido en integración	2–3 meses
R10	MFA, formación, phishing y monitorización	5.000–8.000 €	2–3 meses
R11	Altas/bajas y recertificación	1.500–3.000 €	1–2 meses
R12	Monitorización de privilegios y alertas	4.000–7.000 €	2–3 meses

Estimación económica consolidada del tratamiento

Bloque de tratamiento	Riesgos relacionados	Estimación
Control/monitorización de accesos clínicos	R01	4.000–5.000 €
Integridad y gestión de cambios	R02, R05	3.000–4.000 €
Copias, recuperación y continuidad HCE	R03, R04, R06	6.000–8.000 €
Seguridad de integración con sistema público	R07, R09	3.000–4.000 €
Continuidad de comunicaciones	R08	3.000–4.000 €
Identidades, MFA, formación y privilegios	R10, R11, R12	7.000–11.000 €
Total estimado de tratamiento	—	26.000–36.000 €

Nota presupuestaria. La estimación consolida medidas compartidas para evitar duplicidades. Los importes son orientativos y deberán validarse mediante análisis técnico y presupuestos antes de la aprobación definitiva.

6. Conexión con la Declaración de Aplicabilidad (SoA)

El análisis permite actualizar y fundamentar la Declaración de Aplicabilidad iniciada para el Centro 1. Se agrupan los riesgos por control para mantener trazabilidad sin duplicar información: cada control del Anexo A mostrado se vincula a riesgos concretos y a la necesidad de tratamiento que justifica su aplicabilidad.

Control Anexo A	Riesgos	Decisión SoA	Justificación
A.5.14 Transferencia de información	R07, R09	Aplicable	Protege confidencialidad, integridad y trazabilidad del intercambio.
A.5.15 Control de acceso	R01, R02, R07	Aplicable	Limita accesos y modificaciones a usuarios/sistemas autorizados.

Control Anexo A	Riesgos	Decisión SoA	Justificación
A.5.18 Derechos de acceso	R03, R05, R11, R12	Aplicable	Revisa y retira privilegios para evitar accesos o cambios excesivos.
A.5.24 Preparación para gestión de incidentes	R04	Aplicable	Organiza respuesta y recuperación ante ransomware.
A.5.30 Preparación TIC para continuidad	R05, R06, R08	Aplicable	Recupera HCE, configuraciones y comunicaciones críticas.
A.5.31 Requisitos legales/regulatorios/contractuales	R08	Aplicable	Fija disponibilidad y obligaciones exigibles al proveedor.
A.6.3 Concienciación, educación y formación	R10	Aplicable	Reduce phishing y entrega de credenciales.
A.8.5 Autenticación segura	R10	Aplicable	MFA evita que una contraseña robada sea suficiente.
A.8.12 Prevención de fuga de datos	R07	Aplicable	Limita extracción no autorizada en la integración.
A.8.13 Copias de seguridad	R02, R03, R04, R06	Aplicable	Recupera información/servicio ante error, pérdida o cifrado.
A.8.15 Registro de eventos	R01, R02, R09, R12	Aplicable	Aporta evidencia de accesos, cambios e intercambios.
A.8.16 Monitorización de actividades	R01, R10, R12	Aplicable	Detecta consultas, accesos y privilegios anómalos.
A.8.24 Uso de criptografía	R07, R09	Aplicable	Protege datos en tránsito y dificulta alteraciones.

7. Reflexión metodológica y resumen ejecutivo

Reflexión metodológica

Se ha utilizado MAGERIT v3 porque permite relacionar de forma estructurada los activos del Centro 1 con las amenazas que pueden afectarlos, su impacto en las dimensiones DICTA, las salvaguardas necesarias y el riesgo residual. Esta trazabilidad resulta especialmente adecuada en un entorno sanitario, donde una misma incidencia puede comprometer datos de salud, alterar información clínica o interrumpir sistemas necesarios para la atención.

Para una organización de 220 empleados y un alcance inicial limitado al Centro 1, el análisis se concentra en los activos de mayor criticidad para mantener un nivel de detalle proporcionado. El método permite conectar cada riesgo con medidas concretas y con los controles de la Declaración de Aplicabilidad de ISO 27001:2022, evitando seleccionar controles sin una justificación vinculada al riesgo.

En este contexto, MAGERIT facilita documentar de forma coherente las decisiones necesarias para proteger información clínica y mantener la continuidad de los servicios, al tiempo que sirve de apoyo a la gestión de las obligaciones aplicables en materia de protección de datos y ciberseguridad.

Resumen ejecutivo

El análisis ha identificado 9 riesgos potenciales altos o críticos: 6 críticos y 3 altos, relacionados principalmente con historias clínicas, sistema HCE, identidades y continuidad de las comunicaciones. Las medidas propuestas permiten reducir todos ellos por debajo de los niveles Alto y Crítico. La Dirección aceptaría expresamente R03 (residual 0,26) y R09 (0,29) una vez verificadas las salvaguardas previstas. La inversión necesaria para ejecutar las medidas de tratamiento se estima entre 26.000 y 36.000 €, pendiente de validación técnica y presupuestaria. El marco considerado incluye RGPD y NIS2, utilizando ISO 27001:2022 como marco de gestión.

8. Bibliografía

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT, versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método.

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT, versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II: Catálogo de elementos.

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

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD).

Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2).