Protección de datos sanitarios

Registro de tratamientos, gestión de brechas y privacidad desde el diseño en un entorno sanitario simulado.

Índice

1. Auditoría de privacidad por diseño 3
2. Registro de Actividades de Tratamiento (RAT) 3
3. Bases de legitimación 5
4. Protocolo de gestión de brechas + simulacro 6
5. Diseño del nuevo tratamiento con privacidad por diseño 9
6. Conexión con el SGSI y el análisis de riesgos 10
Resumen ejecutivo de cumplimiento 11
Bibliografía 11

1. Auditoría de privacidad por diseño

Proceso revisado: formulario **simulado** de solicitud de cita ambulatoria del Centro 1 de PYME Sanitaria Mediterránea.

El formulario solicita datos identificativos y de contacto, especialidad, motivo de consulta, cobertura sanitaria, datos de representación y autorizaciones para comunicaciones comerciales y con terceros.

Hallazgo	Criterio afectado	Corrección
Motivo de consulta obligatorio en texto libre.	**Minimización:** puede provocar la recogida anticipada de información clínica más detallada de la necesaria para asignar una cita.	Sustituir por selección de especialidad o tipo de consulta y dejar un campo complementario opcional.
Aseguradora y número de póliza se solicitan también a pacientes particulares.	**Minimización:** se recogen datos no necesarios cuando la asistencia no se tramita mediante seguro.	Mostrar estos campos solo cuando se seleccione “Aseguradora”.
Los datos del representante se requieren para todos los pacientes.	**Minimización:** supone recoger datos de terceros cuando no existe representación.	Activarlos únicamente para menores o pacientes representados.
Una sola autorización agrupa asistencia, recordatorios, marketing y comunicaciones con terceros.	**Limitación de la finalidad:** mezcla tratamientos necesarios y opcionales bajo una única aceptación.	Separar finalidades y dejar el marketing y las comunicaciones opcionales en decisiones independientes.
Casillas comerciales premarcadas y ausencia de información suficiente sobre el tratamiento.	**Privacidad por defecto y transparencia:** la configuración inicial no es la más protectora y la información facilitada es insuficiente.	Dejar las casillas opcionales desmarcadas e incorporar información básica de privacidad y acceso a la información ampliada.

Formulario corregido. La solicitud se limita a los datos necesarios para identificar al paciente y gestionar la cita. Los campos de aseguradora y representación solo aparecen cuando proceda; el motivo de consulta deja de ser obligatorio en texto libre; y las finalidades opcionales se separan y permanecen desactivadas por defecto.

2. Registro de Actividades de Tratamiento (RAT)

T01 — Gestión de la historia clínica y asistencia sanitaria

Campo	Contenido
ID	T01
Actividad de tratamiento	Gestión de la historia clínica y asistencia sanitaria
Finalidad	Prestación de asistencia sanitaria, diagnóstico, tratamiento, seguimiento y continuidad asistencial; documentación y conservación de la historia clínica.
Base legitimadora — art. 6	Art. 6.1.b RGPD para la prestación asistencial; art. 6.1.c RGPD para las obligaciones legales de documentación, custodia y conservación clínica.
Categorías de interesados	Pacientes, incluidos menores atendidos en pediatría.
Categorías de datos	Identificativos y de contacto; antecedentes, diagnósticos, tratamientos, pruebas, resultados y demás información integrante de la historia clínica.
Datos especiales — art. 9	Datos de salud: art. 9.2.h RGPD, para diagnóstico y asistencia sanitaria por profesionales sujetos a secreto profesional.
Destinatarios	Profesionales sanitarios autorizados; Administración sanitaria cuando exista obligación legal de comunicación.
Transferencias internacionales	No previstas.

Campo	Contenido
Plazos de supresión / conservación	Documentación clínica: mínimo 5 años desde el alta de cada proceso asistencial, conforme al art. 17.1 Ley 41/2002 y art. 46.12 Ley 10/2014 de Salud de la Comunitat Valenciana, sin perjuicio de conservaciones superiores legalmente justificadas.
Medidas de seguridad	SGSI — ISO/IEC 27001:2022: A.5.15, A.5.18, A.8.13, A.8.15, A.8.16 y A.8.24.
DPO consultado	Sí.

T03 — Gestión de citas y agenda de pacientes

Campo	Contenido
ID	T03
Actividad de tratamiento	Gestión de citas y agenda de pacientes
Finalidad	Solicitud, asignación, confirmación, modificación y cancelación de citas asistenciales.
Base legitimadora — art. 6	Art. 6.1.b RGPD, al ser necesario para gestionar la asistencia solicitada por el paciente.
Categorías de interesados	Pacientes y representantes legales cuando proceda.
Categorías de datos	Identificativos, contacto, especialidad, fecha y hora y, únicamente cuando resulte necesario, motivo de consulta limitado.
Datos especiales — art. 9	Cuando especialidad o motivo revelen información de salud: art. 9.2.h RGPD.
Destinatarios	Personal autorizado de admisión y administración.
Transferencias internacionales	No previstas.
Plazos de supresión / conservación	Datos administrativos de agenda: hasta realización o cancelación de la cita; posteriormente, bloqueo durante 5 años para atender posibles responsabilidades y supresión al finalizar. Si se incorporan a documentación clínica: mínimo 5 años desde el alta del proceso asistencial.
Medidas de seguridad	SGSI — ISO/IEC 27001:2022: A.5.15, A.8.5, A.8.13 y A.8.15.
DPO consultado	Sí.

T04 — Gestión de recursos humanos y nóminas del personal

Campo	Contenido
ID	T04
Actividad de tratamiento	Gestión de recursos humanos y nóminas del personal
Finalidad	Gestión de la relación laboral, nóminas, cotización a la Seguridad Social, obligaciones fiscales y prevención de riesgos laborales.
Base legitimadora — art. 6	Art. 6.1.b RGPD para la relación laboral; art. 6.1.c RGPD para obligaciones laborales, fiscales, de Seguridad Social y preventivas.
Categorías de interesados	Empleados de PYME Sanitaria Mediterránea (220 trabajadores).
Categorías de datos	Identificativos y de contacto; laborales y profesionales; bancarios; retributivos; fiscales; afiliación/cotización y datos necesarios para PRL.
Datos especiales — art. 9	Datos de salud de vigilancia laboral: arts. 9.2.b y 9.2.h RGPD, según la operación realizada.
Destinatarios	TGSS, AEAT, mutua colaboradora, entidad bancaria, servicio de prevención y personal sanitario competente.
Transferencias internacionales	No previstas.

Campo	Contenido
Plazos de supresión / conservación	Recibos salariales y boletines de cotización: 4 años. Afiliación, altas, bajas y variaciones de Seguridad Social: 4 años. Documentación mercantil/contable: 6 años. Documentación tributaria: 4 años. Vigilancia de la salud: plazos específicos exigibles según riesgo o exposición.
Medidas de seguridad	SGSI — ISO/IEC 27001:2022: A.5.15, A.5.18, A.8.13 y A.8.24; acceso a información médica limitado al personal sanitario autorizado.
DPO consultado	Sí.

3. Bases de legitimación

T01 — Gestión de la historia clínica y asistencia sanitaria

Base elegida y justificación.

La prestación de asistencia sanitaria se fundamenta en el **art. 6.1.b RGPD**, al ser necesario el tratamiento para gestionar la relación asistencial solicitada por el paciente. Las obligaciones de documentación, custodia y conservación de la historia clínica se apoyan en el **art. 6.1.c RGPD**, por derivar de obligaciones legales. Al tratarse de datos de salud, se aplica además el **art. 9.2.h RGPD**, relativo al diagnóstico, tratamiento y asistencia sanitaria prestados por profesionales sujetos al deber de secreto.

Bases descartadas.

No se utiliza el **consentimiento del art. 6.1.a RGPD** como base para la asistencia sanitaria ordinaria, ya que esta y las obligaciones legales asociadas no pueden depender de una autorización libremente revocable. Tampoco resulta necesario acudir al interés legítimo o a la misión de interés público, al existir bases contractuales y legales específicas para las operaciones realizadas.

T03 — Gestión de citas y agenda de pacientes

Base elegida y justificación.

La gestión de citas se fundamenta en el **art. 6.1.b RGPD**, puesto que los datos identificativos, de contacto y de agenda son necesarios para atender la solicitud del paciente y organizar la prestación asistencial. Cuando la especialidad o el motivo de consulta permitan revelar información relativa a la salud, se aplica además el **art. 9.2.h RGPD**.

Bases descartadas.

No se utiliza el consentimiento para la gestión ordinaria de la cita porque el tratamiento es necesario para prestar el servicio solicitado y no responde a una finalidad opcional. Tampoco se recurre al interés legítimo al existir una base directamente vinculada a la relación asistencial. Las finalidades independientes, como las comunicaciones comerciales, deberán mantenerse separadas y disponer de su propia base legitimadora.

T04 — Gestión de recursos humanos y nóminas

Base elegida y justificación.

La gestión de la relación laboral se fundamenta en el **art. 6.1.b RGPD**, mientras que las obligaciones fiscales, de Seguridad Social y de prevención de riesgos laborales se amparan en el **art. 6.1.c RGPD**. Cuando se traten datos de salud derivados de la vigilancia laboral, resulta aplicable el **art. 9.2.b RGPD** para el cumplimiento de obligaciones y ejercicio de derechos en el ámbito laboral y, cuando corresponda a medicina del trabajo, el **art. 9.2.h RGPD**.

Bases descartadas.

El consentimiento no constituye una base adecuada para la gestión ordinaria de nóminas, cotizaciones o prevención de riesgos laborales, porque estos tratamientos derivan de la relación laboral y de obligaciones legales que no pueden quedar condicionadas a una decisión revocable del trabajador. Tampoco se acude al interés legítimo cuando existen bases contractuales y legales específicas.

4. Protocolo de gestión de brechas + simulacro

Parte A. Protocolo de notificación de brechas de seguridad

PYME Sanitaria Mediterránea considerará brecha de datos personales cualquier violación de seguridad que ocasione la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales. El protocolo se activa desde el momento en que exista conocimiento suficiente de una posible brecha y seguirá las fases de detección, evaluación, contención, notificación, documentación y cierre.

1. Detección, registro y contención inicial (T0)

Elemento	Procedimiento
Quién puede detectar	Cualquier empleado, Sistemas, proveedor o tercero que identifique una posible brecha.
Canal de aviso interno	Buzón corporativo específico de **Incidentes de Seguridad**, con distribución simultánea al DPO y a Sistemas. Para incidentes urgentes se complementará con el teléfono de guardia de Sistemas.
Quién registra	El **DPO**, que abrirá el expediente de brecha y dejará constancia de fecha y hora de conocimiento, origen del aviso, sistemas afectados y hechos inicialmente conocidos.
Contención	Sistemas adoptará de inmediato las medidas necesarias para limitar el incidente: bloqueo o cambio de credenciales, cierre de sesiones, revocación de accesos remotos, aislamiento del componente afectado y preservación de logs y evidencias.
Responsables	Sistemas ejecuta la contención; el DPO coordina el registro y seguimiento; el responsable del servicio afectado facilita la información necesaria.

El momento registrado como **T0** inicia el cómputo de las 72 horas. El plazo comienza cuando PYME Sanitaria Mediterránea tiene conocimiento de la brecha, no cuando ocurrió el incidente.

2. Evaluación inicial (T+2 h)

El DPO, Sistemas y el responsable del servicio afectado realizarán una evaluación inicial utilizando como apoyo la herramienta **ASESORA BRECHA de la AEPD**.

Pregunta	Criterio de evaluación
¿Hay datos personales afectados?	Confirmar si la brecha afecta a información relativa a personas identificadas o identificables.
Volumen aproximado de afectados	Determinar el número conocido o estimado de personas y registros afectados.
¿Hay categorías especiales del art. 9?	Identificar especialmente datos de salud y otros datos especialmente sensibles.
¿Existe riesgo para derechos y libertades?	Valorar naturaleza de los datos, volumen, personas afectadas, medidas de protección existentes y posibles consecuencias.
¿Requiere notificación a la AEPD?	Sí cuando la brecha pueda entrañar riesgo para los derechos y libertades de las personas.
¿Requiere comunicación a los afectados?	Sí cuando la brecha pueda entrañar **alto riesgo** para sus derechos y libertades.

3. Notificación a la AEPD — máximo 72 horas desde T0

Cuando proceda la notificación, el **DPO preparará la documentación** y PYME Sanitaria Mediterránea, como responsable del tratamiento, realizará la comunicación a través de la **sede electrónica de la AEPD**.

Contenido mínimo	Información a comunicar
Naturaleza de la brecha	Descripción del incidente y categorías de datos implicadas.
Afectados y registros	Número conocido o aproximado de interesados y registros comprometidos.
Punto de contacto	DPO de PYME Sanitaria Mediterránea. Correo: dpo@pymesanitaria.example
Consecuencias probables	Posibles efectos de la brecha sobre las personas afectadas.
Medidas adoptadas o	Actuaciones de contención, corrección y mitigación aplicadas o

Contenido mínimo	Información a comunicar
propuestas	previstas.

Si dentro de las 72 horas no se dispone todavía de toda la información, se notificará con los datos disponibles y se completará posteriormente. Si la notificación se realizase fuera de plazo, deberá documentarse y justificarse el retraso.

4. Comunicación a los afectados

Cuando la evaluación determine **alto riesgo**, el DPO coordinará la comunicación a los interesados **sin dilación indebida**.

La comunicación será individual mediante los datos de contacto asistenciales disponibles y utilizará lenguaje claro y sencillo. Indicará qué ha ocurrido, qué datos pueden haberse visto afectados, cuáles son las consecuencias probables, qué medidas ha adoptado el hospital, qué acciones preventivas puede realizar el interesado y cómo contactar con el DPO. Cuando el afectado sea menor y proceda, la comunicación se dirigirá a su representante legal registrado.

5. Documentación interna

El DPO mantendrá un **Registro de Brechas de Datos Personales** dentro del repositorio documental del SGSI, con acceso restringido al DPO, Sistemas y Dirección cuando resulte necesario.

Toda brecha quedará documentada, se notifique o no a la AEPD. El expediente incluirá hechos y cronología, sistemas y datos afectados, evaluación del riesgo, decisiones adoptadas, comunicaciones realizadas, evidencias disponibles, análisis de causa raíz y medidas correctoras y preventivas.

6. Lecciones aprendidas y cierre (T+30 días)

Una vez finalizada la investigación y aplicadas las medidas correctoras, el DPO, Sistemas y Dirección revisarán el incidente. El cierre deberá confirmar que se ha completado la documentación, implantado las acciones correctoras y actualizado, cuando corresponda, el SGSI, los procedimientos de acceso, la formación del personal y los mecanismos de detección.

Parte B. Simulacro de brecha

Incidente: acceso no autorizado al sistema de laboratorio (LIS)

El viernes **13 de marzo de 2026**, alrededor de las 17:30, una persona que se hizo pasar por personal de soporte del proveedor del LIS solicitó credenciales para aplicar un supuesto parche urgente. Un trabajador del turno de tarde facilitó su usuario y permitió el acceso remoto.

Entre las **17:40 y las 19:10** se registraron consultas y descargas anómalas desde una IP no reconocida y fuera de la franja habitual del proveedor. Sistemas detectó la actividad durante la mañana del sábado 14 al revisar los logs.

El acceso alcanzó la base de datos del laboratorio, que contiene datos identificativos y resultados analíticos, incluidos registros de pacientes pediátricos. Las tablas consultadas pueden contener entre **5.000 y 18.000 historiales**. Los datos no estaban cifrados en reposo y existen indicios de descarga masiva. Todavía no se conoce el número exacto de afectados ni puede confirmarse si los datos fueron efectivamente exfiltrados o si un tercero conserva una copia.

Como medidas iniciales, Sistemas aisló el módulo LIS, forzó el cambio de credenciales, confirmó con el proveedor legítimo que no había realizado ninguna intervención y puso en marcha el análisis forense.

Inicio del plazo de 72 horas

El **T0** deberá fijarse en la hora exacta del sábado 14 en que Sistemas tuvo conocimiento suficiente de la brecha. Esa hora deberá recuperarse de los registros internos, ya que el aviso disponible solo indica “sábado por la mañana”.

El correo remitido el lunes 16 a las 08:42 no inicia el plazo si el hospital ya tenía conocimiento suficiente desde el sábado.

Factor	Valoración
Tipo de datos	Datos identificativos y datos de salud del art. 9 RGPD.
Personas afectadas	Entre 5.000 y 18.000 historiales potencialmente comprendidos, incluidos menores.
Protección existente	Los datos no estaban cifrados en reposo.
Naturaleza del acceso	Acceso por tercero no autorizado mediante credenciales legítimas obtenidas por vishing.
Indicios de extracción	Existen consultas y descargas masivas anómalas; la exfiltración no está todavía confirmada.
Consecuencias posibles	Pérdida de confidencialidad sanitaria, fraude o ingeniería social dirigida, exposición de información clínica y posibles perjuicios personales o discriminatorios.

Aplicando la lógica de **ASESORA BRECHA**, la combinación de datos de salud, menores, elevado volumen potencial, ausencia de cifrado y acceso no autorizado impide considerar improbable el riesgo. Además, la naturaleza y sensibilidad de la información determinan un **alto riesgo para los derechos y libertades de los afectados**.

Decisión: procede notificar la brecha a la **AEPD conforme al art. 33 RGPD** y comunicarla a los **interesados conforme al art. 34 RGPD**.

Notificación a la AEPD

Campo	Contenido
Naturaleza de la brecha	Acceso remoto no autorizado al LIS mediante credenciales obtenidas por vishing, con consultas y posibles descargas masivas.
Categorías de datos	Datos identificativos y resultados analíticos; incluye información correspondiente a pacientes pediátricos.
Número aproximado de afectados y registros	Número exacto pendiente de investigación; entre 5.000 y 18.000 historiales potencialmente comprendidos.
Punto de contacto	dpo@pymesanitaria.example
Consecuencias probables	Pérdida de confidencialidad sanitaria y posible utilización de la información para fraude, ingeniería social, discriminación u otros perjuicios personales.
Medidas adoptadas	Aislamiento del LIS, cambio forzado de credenciales, confirmación con el proveedor legítimo y análisis forense.
Medidas propuestas	Autenticación reforzada para accesos remotos, prohibición de compartir credenciales, cifrado de datos en reposo, alertas ante descargas anómalas y formación específica frente a vishing.

La notificación se realizará dentro de las **72 horas desde T0**. Si al vencimiento del plazo aún no se conoce el número exacto de afectados o no puede confirmarse la exfiltración, se notificará con la información disponible y se completará posteriormente.

Comunicación a los interesados

PYME Sanitaria Mediterránea ha detectado un acceso no autorizado a su sistema de laboratorio que puede haber afectado a sus datos identificativos y a determinados resultados analíticos. El acceso ha sido bloqueado y se está analizando su alcance. Existen indicios de descarga de información, aunque todavía no se ha confirmado si los datos llegaron a salir de los sistemas del hospital.

Como consecuencia, la información afectada podría ser utilizada para intentos de fraude, suplantación o comunicaciones dirigidas utilizando datos personales o sanitarios. El hospital ha aislado el sistema afectado, ha forzado el cambio de credenciales, ha confirmado con el proveedor legítimo que no realizó la intervención y mantiene en curso el análisis forense para determinar el alcance del incidente.

Como medida preventiva, le recomendamos extremar la precaución ante llamadas, correos o mensajes que soliciten información personal o sanitaria haciéndose pasar por el hospital o por alguno de sus

proveedores. Para cualquier consulta relacionada con este incidente puede dirigirse al Delegado de Protección de Datos de PYME Sanitaria Mediterránea en dpo@pymesanitaria.example.

La comunicación se remitirá **sin dilación indebida** a los afectados identificados y, cuando corresponda a pacientes menores, a su representante legal registrado.

5. Diseño del nuevo tratamiento con privacidad por diseño

Proyecto / servicio: MediMédite — App del paciente: portal de citas y resultados
Responsable de producto: Gonzalo Briones, Director de Transformación Digital
Fecha de revisión: 03/10/2026
Finalidad: permitir al paciente gestionar citas, consultar resultados de laboratorio validados e historial de visitas y recibir recordatorios asistenciales.

7 principios de privacidad por diseño aplicados.

Principio	Aplicación	Evidencia
1. Proactivo, no reactivo	La revisión de privacidad y la EIPD se realizarán antes del despliegue.	Lanzamiento condicionado a la evaluación previa y validación de las medidas.
2. Privacidad por defecto	Solo se activarán los tratamientos imprescindibles para las funciones asistenciales. Marketing, ubicación y biometría serán opcionales.	Configuración inicial restrictiva y opciones voluntarias desactivadas.
3. Privacidad embebida en el diseño	Se eliminan la geolocalización continua e histórica, contactos, galería, origen étnico, religión y cuestionario general de hábitos.	Especificación funcional revisada antes del desarrollo.
4. Funcionalidad total	Citas, resultados, historial y recordatorios funcionan sin recopilar información ajena a esas finalidades.	No se condicionan las funciones asistenciales a perfiles comerciales ni datos adicionales.
5. Seguridad de extremo a extremo	Cifrado, autenticación reforzada, control de accesos, registro de actividad, copias de seguridad y control de sesiones.	Controles del SGSI A.5.15, A.5.18, A.8.5, A.8.13, A.8.15, A.8.16 y A.8.24.
6. Visibilidad y transparencia	Información de privacidad accesible desde el alta y permanentemente desde la aplicación.	Finalidades, bases, conservación, destinatarios y derechos informados de forma diferenciada.
7. Respeto por la privacidad del usuario	Ejercicio de derechos desde la app y alternativa a la autenticación biométrica.	Área específica de privacidad y acceso mediante credenciales y segundo factor.

Aplicación operativa

Pregunta de diseño	Decisión
¿Tratamos solo los datos mínimos necesarios?	Nombre y apellidos, email/teléfono y número de historia para identificar y vincular al paciente. DNI y fecha de nacimiento únicamente cuando sean necesarios para la verificación inicial. Resultados e historial se consultan en los sistemas clínicos existentes, sin crear copias innecesarias. Se eliminan geolocalización continua e histórica, contactos, galería, cuestionario general de hábitos, origen étnico y religión. La ubicación podrá solicitarse puntualmente para localizar un centro y no se conservará.
¿Cuál es la base legitimadora?	Gestión de citas, consulta de resultados e historial y recordatorios asistenciales: art. 6.1.b RGPD y, cuando se traten datos de salud, art. 9.2.h RGPD. Marketing: consentimiento específico, separado y revocable (art. 6.1.a). La eventual comunicación de datos a una aseguradora no queda amparada por un consentimiento único: deberá definirse previamente su finalidad, datos y base jurídica.
¿Quién accede a cada categoría de datos?	El paciente solo a sus propios datos; Admisión a la información necesaria para citas; el personal sanitario a los datos clínicos

Pregunta de diseño	Decisión
	correspondientes a su función. Los accesos quedan sujetos a control por perfiles y registro.
¿Cifrado en tránsito y en reposo?	Sí. La información se protegerá mediante cifrado tanto durante su transmisión como en almacenamiento, conforme al SGSI.
¿Pseudonimización donde sea posible?	Sí. En desarrollo, pruebas y análisis se utilizarán datos sintéticos o pseudonimizados cuando no sea necesario emplear información identificativa real.
¿Plazo de conservación definido?	Información clínica: plazos establecidos para T01; datos de citas: criterios de T03. Los datos propios de la cuenta se conservarán mientras permanezca activa y se suprimirán cuando deje de ser necesaria, salvo obligación de conservación. La geolocalización puntual no se almacenará. Los datos utilizados exclusivamente para marketing dejarán de tratarse para esa finalidad cuando se retire el consentimiento.
¿Información transparente al interesado?	Sí. Se utilizará información por capas antes del alta y accesible permanentemente desde la app, diferenciando las finalidades asistenciales de las opcionales.
¿Configuración restrictiva por defecto?	Sí. Marketing desactivado; geolocalización solo bajo solicitud del usuario; sin permisos generales sobre contactos o galería. La biometría será opcional y se utilizará únicamente la autenticación local del dispositivo, sin almacenar plantillas biométricas en servidores del hospital.
¿Mecanismo de ejercicio de derechos?	Área “Privacidad y derechos” para acceso, rectificación, supresión, limitación, oposición y portabilidad, con remisión al DPO. Plazo general de respuesta: un mes, prorrogable cuando legalmente proceda. La baja de la app no implica la eliminación de documentación clínica sometida a conservación legal.
¿Necesita EIPD?	Sí, antes del despliegue. El tratamiento permite acceso sistemático a datos de salud, puede afectar a menores y utiliza una aplicación móvil como nuevo canal de acceso a información clínica. Estas circunstancias, junto con la sensibilidad y alcance del tratamiento, requieren evaluar previamente los riesgos para los derechos y libertades. No se desarrolla aquí la EIPD completa.

Decisión

Bloqueado: requiere EIPD previa. MediMédite no pasará a producción hasta completar la EIPD, verificar las medidas técnicas y organizativas previstas y confirmar que la versión definitiva respeta la minimización y la configuración de privacidad por defecto.

6. Conexión con el SGSI y el análisis de riesgos

Las medidas de seguridad definidas en el RAT se apoyan en el SGSI de PYME Sanitaria Mediterránea y en los controles ya establecidos para proteger la información clínica. En T01 —Historia clínica y asistencia sanitaria—, el control de acceso, el registro de eventos y la monitorización mediante **A.5.15, A.8.15 y A.8.16** responden al riesgo **R01**, asociado al acceso no autorizado o fuga de historias clínicas. Las copias de seguridad y la gestión de privilegios mediante **A.8.13 y A.5.18** se relacionan, a su vez, con **R03**, orientado a evitar la pérdida definitiva o eliminación indebida de información.

La gestión de identidades y privilegios constituye otra conexión directa con el análisis de riesgos. **R10** aborda el robo de credenciales mediante autenticación reforzada y formación (**A.8.5 y A.6.3**); **R11** trata los permisos excesivos mediante revisión de derechos (**A.5.18**); y **R12** el abuso de privilegios mediante monitorización, revisión y trazabilidad (**A.8.16, A.5.18 y A.8.15**). Estos mismos controles sustentan las restricciones de acceso incorporadas en los tratamientos del RAT, aunque cada actividad mantenga sus propias finalidades, usuarios autorizados y necesidades de acceso.

MediMédite aplica desde su diseño este mismo modelo de protección: autenticación reforzada, acceso por perfiles, cifrado, registro y monitorización de accesos y copias de

seguridad, apoyándose en **A.5.15, A.5.18, A.8.5, A.8.13, A.8.15, A.8.16 y A.8.24**. De esta forma, el nuevo canal móvil reutiliza controles ya integrados en el SGSI para proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información sanitaria.
El cumplimiento del **art. 32 RGPD** queda así integrado en la gestión general de seguridad: el RAT identifica los tratamientos y las medidas que requieren; el análisis de riesgos determina las amenazas relevantes; y el SGSI proporciona los controles técnicos y organizativos para reducirlas. La puesta en producción de MediMédite deberá mantener esta trazabilidad y quedará condicionada, además, a la EIPD previa definida en el Paso 5.

Resumen ejecutivo de cumplimiento

La revisión ha permitido corregir deficiencias en la gestión de datos de pacientes y empleados y establecer criterios claros sobre qué información puede utilizarse, durante cuánto tiempo y quién puede acceder a ella. También se ha definido un procedimiento para responder ante una fuga o acceso indebido a datos sanitarios, con responsables y plazos concretos para actuar y comunicar el incidente. El nuevo proyecto MediMédite se ha rediseñado para evitar la recogida innecesaria de información y reforzar la seguridad desde su puesta en marcha. Con estas medidas se reduce el riesgo de accesos no autorizados, pérdida de información sanitaria, uso excesivo de datos y respuestas tardías ante incidentes. **MediMédite no deberá ponerse en producción hasta completar su evaluación previa de riesgos de privacidad y verificar que las medidas previstas estén implantadas.**

Bibliografía

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Ley 10/2014, de 29 de diciembre, de Salud de la Comunitat Valenciana.

Agencia Española de Protección de Datos (AEPD). Guía para la gestión de brechas de datos personales y herramienta ASESORA BRECHA.

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

Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social (LISOS), art. 21.1.

Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio, art. 30.

Ley 58/2003, de 17 de diciembre, General Tributaria, arts. 66 y 70.

Código Civil, art. 1964.2, plazo general de cinco años de las acciones personales que no tengan plazo especial.