CIBERDELITOS Y REGULACIÓN DE LA CIBERSEGURIDAD

Actividad 1: Confección de una evaluación de impacto en protección de datos (EIPD)

Descripción breve

Documento que justifica la idoneidad, necesidad y proporcionalidad de la migración de los datos sanitarios del Hospital de Gotan a un entorno cloud (SaaS). Sirve como base legal y metodológica para la posterior Evaluación de Impacto en Protección de Datos (EIPD).

Julio Ortiz Bort

julio.ortiz176@comunidadunir.net

Ignacio Alcalde Torrescusa

ignacio.alcalde193@comunidadunir.net

Ainhoa García-Ruiz Fuentes

ainhoa.garciaruiz426@comunidadunir.net

Contenido

Asignatura	Datos del alumno	Fecha
Ciberdelitos y Regulación de la Ciberseguridad	- Ignacio Alcalde Torrescusa - Ainhoa Garcia-Ruiz Fuentes - Julio Ortiz Bort	13/12/2025

1. Datos de Interés

El presente documento establece el contexto y la justificación del tratamiento proyectado mediante el triple juicio de idoneidad, necesidad y proporcionalidad, según lo exige el artículo 35.7.b) del Reglamento General de Protección de Datos (RGPD) para operaciones de alto riesgo.

Esta evaluación se enmarca en un contexto de crisis generada por un ataque masivo de ciberseguridad realizado por el Comodín contra la cuidad de Gotan. Este incidente ha comprometido datos sensibles de los ciudadanos y ha puesto en grave riesgo la seguridad pública, específicamente, la infraestructura informática del hospital público de Gotan. La urgencia radica en la necesidad inmediata de salvaguardar los datos personales y garantizar la continuidad asistencial, razón por la cual la policía de Gotan y la empresa de Bruno Vaine han determinado que la mejor solución es trasladar los datos a un entorno más seguro.

El responsable del tratamiento es el hospital público de Gotan y la medida acordada con el fin de asegurar la continuidad asistencial y la protección del interés público esencial, consiste en la migración completa de los datos sanitarios alojados actualmente en modo local (infraestructura on-premise) a un nuevo software en la nube (Software as a Service – SaaS).

Para ello, deben migrar todos los datos desde el proveedor de software local anterior (SW System Mantenimiento Informático, S.L.) hacia la plataforma *Software as a Service* (SaaS) y alojamiento cloud provista por el nuevo Encargado del Tratamiento, No problem Cloud Solutions, S.L.

2. Juicio de Idoneidad

Definición (Artículo 35.7.b) RGPD): El tratamiento proyectado (migración a SaaS) debe ser idóneo es decir, si es un medio apto, adecuado y eficaz para conseguir el objetivo propuesto, que es salvaguardar los datos de salud y garantizar la continuidad asistencial en un entorno seguro tras el ataque.

2.1 Fallo del Sistema Anterior y Justificación del Cambio

La infraestructura local (on-premise) operada y mantenida por SW System S.L. ha sido vulnerada por el ataque masivo, lo que demuestra una clara inidoneidad para los requisitos de seguridad actuales. Mantener los datos en un entorno cuya seguridad ha sido comprometida y cuya vulnerabilidad ha sido explotada no es una opción idónea, ya que el riesgo residual de una nueva brecha es bastante alto. El sistema actual ha resultado ser ineficaz para garantizar los principios de confidencialidad, integridad y disponibilidad del RGPD.

Asignatura	Datos del alumno	Fecha
Ciberdelitos y Regulación de la Ciberseguridad	- Ignacio Alcalde Torrescusa - Ainhoa Garcia-Ruiz Fuentes - Julio Ortiz Bort	13/12/2025

2.2 Justificación de Idoneidad de la Solución SaaS (No problem Cloud Solutions, S.L.)

La migración a un servicio SaaS especializado resulta ser la solución idónea dado que aborda directamente las deficiencias del sistema anterior mediante la provisión de una infraestructura de seguridad robusta y gestionada por un tercero experto.

- **Mitigación Inmediata de la Brecha:** El traslado de los datos a un nuevo entorno físico y lógico (el CPD de No problem S.L. en España) es el mecanismo más rápido y eficaz para cortar el acceso que el atacante (en este caso el Comodín) pudiera haber mantenido sobre el sistema comprometido.
- **Adopción de Medidas Técnicas Avanzadas:** La contratación de un servicio cloud especializado permite al Hospital de Gotan acceder inmediatamente a estándares de ciberseguridad superiores sin incurrir en los largos procesos de adquisición y puesta en marcha de hardware local. Esto incluye medidas como cifrado avanzado de datos en reposo y en tránsito, sistemas de detección y prevención de intrusiones (IDS/IPS), y gestión automatizada de parches y actualizaciones.
- **Garantía de Disponibilidad y Resiliencia:** Un CPD profesional gestionado por No problem S.L. proporciona redundancia y planes de recuperación ante desastres que son esenciales para la continuidad asistencial. Esto asegura que, incluso ante un fallo, los datos del historial clínico seguirán accesibles, cumpliendo el principio de disponibilidad de los datos.

El tratamiento proyectado es IDÓNEO porque representa el medio más apto, eficaz y rápido para restaurar y superar el nivel de seguridad exigido para los datos de salud tras el ataque. El Hospital de Gotan logra, mediante este cambio, el objetivo de asegurar la integridad y la disponibilidad de los datos, elementos fundamentales para la prestación del servicio público esencial.

3. Juicio de Necesidad

Definición (Art. 35.7.b) RGPD): El tratamiento proyectado es necesario si no existe otro tratamiento menos intrusivo en los derechos de las personas afectadas, que posea una eficacia igual o comparable para la consecución del objetivo propuesto (salvaguardar los datos de salud tras el ataque).

3.1 Consideración de Alternativas Menos Intrusivas

Se han analizado las posibles alternativas a la migración a la nube (SaaS), las cuales implicarían una menor injerencia en la privacidad al no externalizar el alojamiento de los datos.

Alternativa A: Refuerzo y Aislamiento del Sistema Local Comprometido

Consistiría en mantener el Sistema Informático de Historias Clínicas (SIHC) en el entorno on-premise y contratar expertos para limpiar, auditar y fortificar la infraestructura existente.

Dada la naturaleza del ataque masivo del Comodín, la identificación y erradicación de todas las posibles puertas traseras o vulnerabilidades ocultas es un proceso extremadamente lento e incierto. Cualquier fallo en la detección podría llevar a una nueva explotación inminente de datos de salud. Además, la inversión en hardware y software para alcanzar los niveles de resiliencia de un CPD especializado llevaría meses, comprometiendo la continuidad del servicio médico a corto plazo.

Alternativa B: Adquisición e Instalación de un Nuevo Sistema Local (Greenfield)

Comprar hardware y software totalmente nuevos, instalarlo en un nuevo centro de datos interno y migrar los datos a esta infraestructura local limpia.

Si bien se garantizaría un entorno limpio, el tiempo de adquisición, instalación, configuración y migración de un SIHC es prolongado (varios meses). Esta demora es inaceptable en una situación de emergencia donde la vida de los pacientes depende del acceso a sus historiales. Además, el coste y la necesidad de personal especializado 24/7 para gestionar la ciberseguridad avanzada en este entorno local superarían la capacidad administrativa del Hospital de Gotan.

3.2 Justificación de la Necesidad de la Migración a SaaS

La migración a la solución SaaS de No problem Cloud Solutions, S.L. (Alternativa Propuesta) es la única vía que ofrece la Alta Eficacia requerida para el contexto de emergencia ya que entre otras cosas permite:

- **Respuesta Inmediata a la Crisis**: Permite un traslado de datos e inicio de operaciones en un entorno seguro en un plazo de tiempo significativamente menor que cualquier solución de implementación local.
- **Garantía de Seguridad Especializada**: Ofrece un nivel de protección técnica y resiliencia gestionado por expertos en seguridad cloud, superando el nivel que el Hospital de Gotan podría alcanzar a nivel local con la rapidez necesaria.

La migración a la nube se considera NECESARIA en el contexto actual. Ninguna de las alternativas (A y B) analizadas puede ofrecer una respuesta inmediata y con igual garantía de eficacia para mitigar el alto riesgo de compromiso de los datos de salud y asegurar la continuidad asistencial del Hospital de Gotan. Por lo tanto, el tratamiento no es meramente conveniente, sino que resulta la única opción *necesaria* para cumplir con la obligación de proteger los datos en una situación de emergencia de seguridad.

Asignatura	Datos del alumno	Fecha
Ciberdelitos y Regulación de la Ciberseguridad	- Ignacio Alcalde Torrescusa - Ainhoa Garcia-Ruiz Fuentes - Julio Ortiz Bort	13/12/2025

4. Juicio de Proporcionalidad

Definición (Art. 35.7.b) RGPD): El tratamiento es proporcional si el beneficio o ventaja que se deriva de su aplicación para el interés general (seguridad y salud pública) es mayor y más equilibrado que el perjuicio, menoscabo o injerencia que la operación pueda causar sobre los derechos y libertades fundamentales de los interesados (derecho a la protección de datos y privacidad).

4.1 Perjuicios sobre los Derechos y Libertades de los Interesados

El principal perjuicio para los ciudadanos de Gotan derivado del tratamiento del proveedor cloud, es la externalización del control del alojamiento y gestión de los datos de salud a un tercero (No problem Cloud Solutions, S.L.). Este cambio de control introduce riesgos como:

- **Dependencia del Proveedor:** Se genera una dependencia crítica respecto al proveedor externo, lo que implica la cesión del control directo sobre la infraestructura física y la gestión del software base
- **Riesgo Contractual/Legal:** Posibilidad de fallos o ambigüedades en la definición de las responsabilidades legales y operativas dentro del Contrato de Encargado del Tratamiento (EIT). Un contrato inadecuado afectaría directamente la capacidad del Responsable (Hospital de Gotan) para garantizar el cumplimiento del RGPD.
- **Riesgo de Acceso No Autorizado:** La operación de traslado de datos desde el entorno local comprometido al nuevo sistema cloud genera una ventana de riesgo temporal. Este periodo de transición es vulnerable a incidentes de seguridad (ej. corrupción de datos, intercepción o acceso no autorizado a datos en tránsito) a pesar de que la migración se gestione bajo protocolos de seguridad reforzados.

4.2 Beneficios y Ventajas para el Interés General

Las ventajas obtenidas por la migración a la nube en esta situación de crisis son de naturaleza fundamental y afectan a derechos y bienes jurídicos de máxima protección:

- **Protección de la Vida y la Salud Pública:** La migración garantiza la disponibilidad ininterrumpida de los historiales clínicos, lo cual es vital para la atención médica inmediata. La interrupción del servicio o la pérdida de datos de salud supondría un perjuicio directo y catastrófico para la vida y la seguridad de los ciudadanos.
- **Restauración de la Confidencialidad e Integridad:** El traslado a una infraestructura certificada y especializada restablece la confidencialidad de los datos, demostrando a la ciudadanía que la Administración está tomando medidas efectivas para proteger su información más sensible del atacante.
- **Cumplimiento del Deber Legal del Responsable:** La medida permite al Hospital de Gotan cumplir con su obligación esencial de garantizar un nivel de seguridad adecuado a los riesgos que, evidentemente, no se cumplía en el sistema local comprometido.

4.3 Justificación de la Proporcionalidad de la Migración a SaaS

El tratamiento de migración de datos a la plataforma SaaS de No problem S.L. es PROPORCIONAL. El grave perjuicio que implicaría el no tratamiento (colapso sanitario y total pérdida de control de los datos a manos del Comodín) es inmensamente superior al riesgo controlado que implica el cambio de proveedor, siempre que se implementen las medidas técnicas y organizativas adecuadas para garantizar la seguridad en el nuevo entorno y durante la transición. Para la transición resulta de vital importancia la obligación de firmar un Contrato de Encargado del Tratamiento (EIT) robusto con No problem S.L., que impone las cláusulas de seguridad y confidencialidad del RGPD.

5. Referencias Bibliográficas

1. Agencia Española de Protección de Datos (AEPD)

Agencia Española de Protección de Datos. (2018). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Recuperado de https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

2. Autoridad Catalana de Protección de Datos (APDCAT)

Autoritat Catalana de Protecció de Dades. (s.f.). Guia d'avaluació d'impacte relativa a la protecció de dades (EIPD). Recuperado de https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-EIPD.pdf