Premios Socinfo Digital: "AGE TIC"

Premio Seguridad y Protección del Dato.

Organización candidata: Secretaría General de Salud Digital, Información e Innovación del SNS. Ministerio de Sanidad.

Justificación:

El dictamen de la **Comisión para la Reconstrucción Social y Económica tras el Covid**, del Pleno del Congreso de los Diputados, aprobado en julio de 2022, realizaba **dos recomendaciones** en el ámbito de la salud digital en el Sistema Nacional de Salud (SNS en adelante) tras constatarse la relevancia que los sistemas de información habían jugado en el seguimiento y gestión de la pandemia, y el potencial de la digitalización para reforzar y fortalecer el sistema:

- La puesta en marcha una **Estrategia Nacional de Transformación Digital** del Sistema Nacional de Salud.
- La creación de una **unidad directiva de alto nivel** dependiente del Ministerio de Sanidad para liderar la transformación digital en el Sistema Nacional de Salud, que coordinara la elaboración y el seguimiento posterior de la Estrategia.

La **Secretaria General de Salud Digital, Información e Innovación del Sistema Nacional de Salud** (SGSDII en adelante) es ese órgano directivo, dependiente de la Secretaría de Estado de Sanidad, cuyo objetivo es el de lograr una mayor coordinación y eficacia de cara a abordar los proyectos de modernización, mejora y transformación que requieren los nuevos retos en salud y las expectativas de los ciudadanos sobre nuestro SNS, conforme al Real Decreto 852/2021, que establece sus competencias.

Le corresponde, asimismo, la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica.

Igualmente le compete el control de la información sanitaria, en el ámbito de competencias del Departamento, lo cual incluye:

- Impulsar el uso diligente y ético de los datos utilizados en el ámbito del Sistema Nacional de Salud, en colaboración con las comunidades autónomas y resto de agentes involucrados, así como velar por su integridad y proceder a su difusión, en los términos y condiciones que la normativa aplicable establezca.
- Coordinar y supervisar la política de protección de datos en cumplimiento de la normativa aplicable en esta materia en el ámbito de las competencias del Departamento.
- El aseguramiento de la calidad del dato sanitario y el impulso de su gobernanza, garantizando que se disponga de la información correcta, en el momento preciso, y para el destinatario adecuado, respetando las medidas de seguridad aplicables.
- La explotación y operación de los servicios de tecnologías de la información y las comunicaciones del Sistema Nacional de Salud y la gestión de la seguridad de los mismos y de sus datos.

Se debe tener en cuenta que los datos sanitarios son especialmente sensibles y así se refiere a los mismos la normativa aplicable en el ámbito europeo y nacional respecto de protección de datos personales y de tratamiento de datos sanitarios. El **Ministerio de Sanidad** es responsable

del tratamiento de los datos de salud, por ser quien cuenta con la habilitación legal para el tratamiento de estos datos personales en el ámbito de las competencias del departamento, siendo autoridad sanitaria estatal conforme al art 52.1 de la Ley 33/2011 de 4 de octubre, de Salud Pública.

Es necesario recordar que, desgraciadamente, el sector sanitario es uno de los blancos preferidos de los ciberdelincuentes, como pueden demostrar los recientes ataques realizados a importantes centros hospitalarios del país, como el **Clínic de Barcelona o el Hospital Son Espases, de Palma de Mallorca.**

La SGSDII, tiene entre sus ámbitos estratégicos de actuación, implementar **las medidas de seguridad y de protección de datos personales,** tanto técnicas como administrativas, así como impulsar la **coordinación con las Comunidades y Ciudades Autónomas, responsables** también de tratamiento de datos sanitarios en sus respectivas áreas de competencia.

En concreto, se están llevando a cabo las siguientes **actuaciones**:

- **Política de Seguridad de la Información del Ministerio de Sanidad**, y revisión de su aplicación a través de reuniones periódicas de su **Comité de seguimiento**, con representación de todos los centros directivos del departamento.
- **Elaboración de la nueva Política de Seguridad de la Información del Ministerio de Sanidad**, que sustituirá a la actual, que data de 2014.
- Actualización de **normas** y **procedimientos**:
    - Adecuación del **Marco Normativo de Seguridad de la Información** al nuevo **ENS**.
    - Actualización conforme a la nueva **Política de Seguridad de la Información**
- Actualización **medidas técnicas de ciberseguridad**:
    - Incorporación nuevos requisitos del **ENS 2022**.
    - Actualización continua frente a **nuevas ciberamenazas**.
- **Aseguramiento de la seguridad de la información** mediante **certificaciones oficiales** a través de la entidad certificadora de referencia **AENOR**:
    - desde el año 2008 el Ministerio de Sanidad renueva su certificación en la norma ISO 27000 de seguridad de la información, superando el exigente proceso de auditoría preceptivo, siendo pionero en la Administración General del Estado en su obtención.
    - desde el 2019 certificado en ENS, siendo el primer departamento ministerial en lograrlo. Esta certificación también se renueva anualmente.
    - En 2023, se realizará la auditoría de certificación conforme al nuevo ENS.
- En marcha la implementación de una **nueva arquitectura de explotación y desarrollo basada en micro-servicios y contenedores**, para facilitar el desbordamiento a nube pública en caso de crisis.
- Mantenimiento y operación de la **Intranet Sanitaria** como vía segura para el intercambio de datos clínicos entre Consejerías de Salud.
- A través del rol de **Delegación de Protección de Datos**, asesoramiento legal y administrativo a centros directivos sobre tratamiento de estos datos y actualización continua del Registro de Actividades de Tratamiento (RAT).
- Creación de una **Oficina del Dato Sa**nitario, responsable de elaborar el modelo de gobernanza para el acceso al Espacio de Datos de Salud.

De este modo, los servicios comunes prestados por el Ministerio de Sanidad al resto del SNS, especialmente aquellos que facilitan la **interoperabilidad** de la información sanitaria y tan relevantes como la **tarjeta sanitaria individual, la historia clínica interoperable del SNS, la receta interoperable del SNS, el registro nacional de instrucciones previas, el registro de profesionales sanitarios, el nodo del verificación de medicamentos**, se encuentran securizados con el nivel de protección requerido.

En los **Planes Estratégicos** para la ejecución de la **Estrategia de Salud Digital**, aprobada en diciembre del año 2021, la seguridad de la información está presente como línea transversal. Asimismo, en el **Plan de Transformación Digital para la Atención Primaria**, financiado con 230 millones de euros e incluido dentro del PERTE Salud de Vanguardia, con un horizonte temporal de ejecución hasta junio de 2026, y conjuntamente con las Comunidades Autónomas, se ha creado un **grupo de trabajo de ciberseguridad y protección de la información sanitaria** focalizado en este servicio base de la asistencia sanitaria en nuestro país, con participación de 13 de ellas y liderado por **Illes Balears**, donde las CCAA han definido y están llevando a cabo 14 proyectos colaborativos con una financiación dedicada de más de 38 millones de euros y con estos dos objetivos:

1. Mejora de la seguridad en la prestación de servicios por vía telemática y domiciliaria
2. Facilitar la identidad digital de profesionales y ciudadanos en sus interacciones digitales con servicios del SNS.

El resultado serán **activos reutilizables** en todo el SNS, por ejemplo, los siguientes:

a. Servicio de implantación, configuración y puesta en marcha de sistemas de identificación, catalogación, inventariado y análisis de vulnerabilidades de los **dispositivos médicos**.

b. Servicio de implantación, configuración y puesta en marcha para la implantación de una **herramienta GRC** de gestión de riesgos.

c. Servicio de implantación, configuración y puesta en marcha para la implantación del proyecto de implantación **Sistema de gestión de cuentas privilegiadas (PAM)**

El grupo ya ha definido 14 Documentos de funcionalidades y requisitos técnicos comunes de cada una de los proyectos trabajados y se han elaborado pliegos de prescripciones técnicas tipo para su uso por todas las CCAA en el ámbito de **herramientas GRC y gestión de dispositivos médicos**. Se han recibido **200 ofertas** a varias **consultas preliminares de mercado** que los participantes en el grupos de trabajo están analizando.

Los resultados de este grupo de trabajo podrán también adaptarse y ampliarse a la protección de las herramientas tecnológicas que está previsto desarrollar en el nuevo **Plan de Atención Digital Personalizada,** financiado por la adenda enviada a la Comisión Europea el pasado 6 de junio.

CONCLUSIÓN

La especial sensibilidad de los datos de salud requiere una apuesta decidida por su protección, que se traduce en financiación específica, servicios especializados e implantación de medidas técnicas, administrativas, legales y organizativas llevadas a cabo por el Ministerio de Sanidad y las Comunidades Autónomas. Recordemos que el sector sanitario está definido como esencial

y los centros sanitarios como infraestructuras críticas, por lo que los esfuerzos realizados en este sentido desde todas las administraciones redundarán en la **prestación de los servicios de salud sin interrupciones**.