

COMPUTERWORLD

MAYO 2026 | WWW.COMPUTERWORLD.ES

ESPECIAL SANIDAD

índice
SEIS 2025



COMPUTERWORLD

www.computerworld.es

✉ computerworld@foundryco.com ✉ @computerworldes

REDACCIÓN

Directora editorial:

Esther Macías ✉ esther.macias@foundryco.com

Redactores y colaboradores:

Víctor Manuel Fernández ✉ vm.fernandez@foundryco.com

María Ramos

Gonzalo Díaz

Raquel C. Pico

Fotografía: Javier Presa

Diseño y producción digital: Agustín Sánchez

PUBLICIDAD

Director comercial: Julio Benedetti ✉ julio.benedetti@foundryco.com

Account Manager: Sergio Quero ✉ sergio.quero@foundryco.com

ATENCIÓN AL LECTOR

✉ notas@foundryco.com

EVENTOS

Directora de Eventos de Foundry España: Romy Tuin

Directora de operaciones de eventos

y captación de ponentes:

Marta García ✉ marta.garcia@foundryco.com

CIO EXECUTIVE FOUNDRY ESPAÑA

Director: Fernando Muñoz ✉ fernando.munoz@foundryco.com

Depósito legal: M-16.14171981

ISSN: 0212-2456

FOUNDRY
an IDG, Inc. company

SUMARIO

- Editorial
- **La salud digital en España: avances y retos**
Por Luciano Sáez, presidente de la Sociedad Española de Informática de la Salud (SEIS)
- **Índice SEIS 2025**
Estudio sobre la inversión TIC en sanidad en España
- **Entrevista**
Juan Fernando Muñoz Montalvo, secretario general de Salud Digital, Información e Innovación del Sistema Nacional de Salud
- **Debate**
Los desafíos de un SNS más digitalizado que nunca
- **Caso de éxito**
El viaje de la Comunitat Valenciana hacia una salud digital más inclusiva, ética y eficiente
- **Reportaje**
Los hospitales frente al cibercrimen: así gestionan las amenazas de ciberseguridad
- **Comentarios al hilo del Índice SEIS 2025**
Por Carlos García Codina, coordinador del Índice SEIS





El salto digital y cultural definitivo de la sanidad pública española

La sanidad española es digital en la operativa, pero no invierte lo suficiente para lograr su transformación digital". Esta frase, lapidaria, es de Luciano Sáez Ayerra, el presidente de la Sociedad Española de Informática de la Salud (SEIS), la entidad científica junto a la que COMPUTERWORLD ESPAÑA publica, desde hace años, el tradicional especial anual de Sanidad que ahora tiene en sus manos (o, mejor dicho, ante sus ojos) y que integra en exclusiva el Índice SEIS, informe que analiza de forma pormenorizada el estado de la implantación de las TI en el Sistema Nacional de Salud.

El experto y su equipo conocen como nadie la realidad de la sanidad pública española, cuyos avances en modernización TIC y digitalización (sobre todo a raíz de la crisis de la pandemia) son innegables, gracias, en gran parte, a la inyección de capital europeo (los famosos fondos Next Generation) pero también gracias a un loable esfuerzo y colaboración entre el Ministerio de Sanidad, en particular de la Secretaría General de Salud Digital liderada por Juan Fernando Muñoz, y las distintas organizaciones de sanidad y digitalización de las comunidades autónomas, donde recaen las competencias sanitarias en España y, por tanto, quienes afrontan en primera línea el despliegue e implantación de las TIC. No obstante, es

un hecho que el Sistema Nacional de Salud afronta aún grandes retos para que sus sistemas de información operen de forma verdaderamente estratégica, interoperable, eficiente y sostenible, como desgranar sus protagonistas en las páginas de este especial.

En el futuro, ya sin los fondos europeos a la vista (al menos de momento), los actores sanitarios deberán garantizar la inversión necesaria para asegurar la continuidad de los proyectos en marcha y la adopción de la innovación que requiere este nuevo escenario en el que habitamos, marcado por una vertiginosa aceleración tecnológica con la explotación del dato y la inteligencia artificial como máximos estandartes.

No, no es suficiente que España destine a las TIC dentro del SNS el 1,62% del presupuesto sanitario. Urge, de una vez, comprender que la inversión en tecnología no es un gasto, sino una garantía de futuro para un activo tan valioso para el país como la sanidad pública.

Y es preciso aplicar también, como insisten desde la SEIS, cambios estructurales que vayan más allá de la tecnología. Poner el foco en las personas, en el talento necesario para afrontar el nuevo escenario sanitario hiperconectado, inteligente e hiperpersonalizado, es hoy más necesario que nunca. Solo así llegará la verdadera transformación de la sanidad pública española. **CW**

La salud digital en España: avances y retos

La información generada a partir de datos fiables y precisos es la base de todo sistema sanitario moderno. Cada acto clínico, cada proceso asistencial y cada decisión de gestión depende de datos. Generar esa información requiere un ecosistema de aplicaciones e infraestructura, en el que la digitalización es solo un requisito básico.

El ÍNDICE SEIS, elaborado por la Sociedad Española de Informática de la Salud, los Servicios de Salud de las comunidades autónomas, el Ministerio de Sanidad y Red.es, revela en su edición del año 2025 una paradoja persistente: el Sistema Nacional de Salud (SNS) ha avanzado de forma notable en su digitalización, pero aún no ha desarrollado plenamente las capacidades organizativas ni ha realizado las inversiones necesarias para consolidar un sistema de información verdaderamente estratégico.

Según los datos del ÍNDICE SEIS 2025, el gasto total en Tecnologías de la Infor-

Luciano Sáez Ayerra

Presidente de la Sociedad Española de Informática de la Salud (SEIS)



mación y la Comunicación (TIC) en el SNS ha alcanzado el 1,62% del presupuesto sanitario. Es una cifra en crecimiento — casi un 20% más que el año anterior—, pero todavía insuficiente para un sistema que depende estructuralmente de la gestión masiva de datos. Dicho de otro modo: la sanidad española es digital en la operativa, pero no invierte lo suficiente para lograr su transformación digital.

No obstante, sería injusto ignorar los avances. España ha logrado consolidar uno de los pilares fundamentales de cualquier sistema sanitario moderno: la Historia Electrónica de Salud (HES). Todas las comunidades autónomas disponen ya de sistemas que permiten el acceso longitudinal a la información clínica del paciente, y los ciudadanos pueden consultar sus datos a través de internet y, en la mayoría de los casos, mediante aplicaciones móviles. Asimismo, el

esfuerzo coordinado por el Ministerio de Sanidad en materia de interoperabilidad y en el desarrollo de proyectos conjuntos, sitúa al SNS en una posición destacada en el contexto internacional.

Sin embargo, el sistema tiene limitaciones, ya que es esencialmente unidireccional. El acceso a sus datos está garantizado pero la capacidad del ciudadano para interactuar con su propia información clínica es limitada. Solo una minoría de comunidades permite la incorporación de datos por parte del paciente, y el uso efectivo de estas funcionalidades sigue siendo reducido.

El ÍNDICE SEIS 2025 también confirma que la inteligencia artificial es uno de los grandes vectores de cambio del sistema sanitario. El informe muestra que la mayoría de las comunidades autónomas ya han iniciado proyectos en IA, especialmente en el análisis de imagen médica, procesamiento del lenguaje natural, genómica y en el apoyo al diagnóstico. Además, la integración

de la inteligencia artificial en la práctica asistencial se sitúa entre las principales prioridades estratégicas del sistema.

Pero el ÍNDICE SEIS también detecta una de las principales debilidades estructurales: la gobernanza. Menos de la mitad de las comunidades cuentan con unidades específicas de inteligencia artificial, y aún menos disponen de modelos formales de gobernanza. La tecnología avanza más rápido que la capacidad institucional para gestionarla. Y ese desfase no es menor: en sanidad, la adopción sin gobernanza no solo es ineficiente, sino potencialmente arriesgado.

El problema se intensifica a medida que el volumen de datos sanitarios crece de forma exponencial, impulsado por la expansión de la imagen médica, los proyectos de big data, el internet de las cosas o la medicina de precisión. Sin embargo, las estructuras de gestión del dato siguen siendo incipientes. Iniciativas como la denominada Oficina del Dato de Salud, identificada como línea estratégica emergente, continúan siendo más una intención que una realidad consolidada.

En paralelo, la ciberseguridad ha ganado relevancia en los últimos años,

con incrementos en inversión y en el despliegue de centros de operaciones de seguridad. Aun así, en muchos casos sigue tratándose como una capa técnica y no como un elemento central de la estrategia sanitaria. En un entorno donde los datos clínicos son especialmente sensibles y críticos, esta aproximación resulta claramente insuficiente.

No basta con digitalizar procesos; es necesario rediseñar el modelo asistencial en torno al dato, la inteligencia y el valor generado para el paciente

En conjunto, el ÍNDICE SEIS 2025 dibuja un sistema que ha completado con éxito la fase de digitalización básica, pero que aún no ha dado el salto hacia una transformación profunda basada en el uso inteligente de la información. Las prioridades identificadas —integración de la inteligencia artificial, análisis

de datos, ciberseguridad, optimización de flujos asistenciales— apuntan en la dirección correcta. Pero su materialización requiere cambios estructurales que van más allá de la tecnología.

Y uno de estos cambios pendientes es mejorar la formación de los profesionales sanitarios en todas estas tecnologías. Resulta urgente fortalecer los

recursos humanos propios, consolidando perfiles profesionales especializados en salud digital. No se dispone aún de programas estructurados de formación en salud digital para profesionales sanitarios. Este dato es especialmente revelador: mientras la tecnología avanza con rapidez, el sistema no está preparando

adecuadamente a quienes deben utilizarla, interpretarla y gobernarla.

El riesgo es evidente. Sin una formación específica, la inteligencia artificial puede convertirse en una herramienta infrutilizada o, peor aún, mal aplicada. La interpretación de modelos, la validación de resultados o la integración en la práctica clínica requieren competencias que hoy no forman parte del núcleo formativo de la mayoría de los profesionales sanitarios. La alfabetización digital básica ya no es suficiente; es necesario avanzar hacia una verdadera capacitación en salud digital.

Pero la necesidad de formación no se limita al ámbito clínico. El SNS también adolece de una masa crítica insuficiente de profesionales TIC con un buen conocimiento del entorno sanitario. Aunque el número de especialistas TIC en las organizaciones sanitarias ha crecido, la dependencia de personal externo es muy elevada. Esta situación compromete la capacidad estratégica del sistema, ya que la transformación digital no puede delegarse completamente en proveedores externos. Se requiere un cuerpo profesional propio, con perfiles híbridos que combinen conocimiento



tecnológico y comprensión del proceso asistencial. Solo desde esta convergencia será posible diseñar soluciones realmente útiles, seguras y alineadas con las necesidades del sistema.

En este contexto, la formación debe entenderse como una prioridad estratégica, no como un complemento. Es necesario abordar tres líneas de actuación claras. En primer lugar, incorporar de forma sistemática competencias digitales avanzadas en los planes formativos de grado y posgrado de las profesiones sanitarias. En segundo lugar, desarrollar programas de formación continua en ámbitos como inteligencia artificial, analítica de datos o ciberseguridad, adaptados a la realidad asistencial. Y, en tercer lugar, consolidar una carrera profesional específica en salud digital que permita atraer y retener talento tecnológico dentro del sistema sanitario.

La brecha entre tecnología y capacidades se manifiesta en múltiples ámbitos. La limitada participación del ciudadano en la gestión de su propia información clínica, la escasa gobernanza estructurada del dato o las dificultades para escalar proyectos de inteligencia artificial

son, en gran medida, consecuencia de esta falta de formación. La tecnología está disponible; lo que falta es el conocimiento para explotarla de forma eficiente y segura.

En esta línea, el papel de la Sociedad Española de Informática de la Salud (SEIS) resulta especialmente relevante. A lo largo de los últimos años, la SEIS

ros específicos como el de inteligencia artificial, el impulso del comité de medicina digital o iniciativas formativas como el Máster en Dirección de Sistemas y TIC para la Salud y en Digitalización Sanitaria y las “píldoras de conocimiento” reflejan un compromiso claro con la formación y el desarrollo de capacidades de los profesionales en el sector.

Además, la creciente colaboración con sociedades científicas y su papel como interlocutor entre sector público y privado consolidan a la SEIS como un agente clave no solo en la difusión del conocimiento, sino en la articulación de una estrategia compartida para la salud digital en España.

El ÍNDICE SEIS 2025 deja claro que el SNS ha superado la fase inicial de digitalización. La tecnología está implantada, los sistemas funcionan y los datos se generan a gran escala. Pero la siguiente etapa —la de la transformación real— dependerá más de la capacidad del sistema para desarrollar talento. Pero no basta con digitalizar procesos; es necesario rediseñar el modelo asistencial en torno al dato, la inteligencia y el valor generado para el paciente.

Porque la verdadera palanca de cambio no es la tecnología, sino el conocimiento. Sin profesionales formados, la digitalización se queda en superficie; con ellos, se convierte en una herramienta de transformación permanente. El reto no es menor: no se trata solo de incorporar tecnología al sistema sanitario, sino de capacitar al sistema sanitario para entenderla, utilizarla y liderarla. **CW**

La verdadera palanca de cambio no es la tecnología, sino el conocimiento

ha reforzado su posicionamiento como espacio de encuentro entre administraciones, profesionales sanitarios, industria y comunidad científica, impulsando una visión multidisciplinar de la transformación digital en salud.

La puesta en marcha de su Plan Estratégico 2024–2028, la creación de fo-

Sin embargo, el propio entorno en el que opera la SEIS evidencia que este esfuerzo debe escalar. La formación en TIC para la salud no puede depender únicamente de iniciativas voluntaristas o sectoriales; requiere una apuesta decidida a nivel institucional, integrada en las políticas sanitarias y educativas.

ESPECIAL SANIDAD

índice SEIS 2025



I. Introducción

El Sistema Nacional de Salud (SNS) es un sistema de salud de cobertura universal, financiado por impuestos, y cuya gestión está descentralizada en las comunidades autónomas. Los principales retos a los que en la actualidad se enfrenta el SNS son:

- El incremento de la frecuentación, que se debe entre otros factores a mayor esperanza de vida de la población y al aumento de enfermedades crónicas.
- Las crecientes expectativas y exigencias de los pacientes, cada vez más y mejor formados e informados.
- La coordinación entre los niveles del sistema y la continuidad de la atención.
- La incorporación de nuevas tecnologías sanitarias, en algunos casos muy costosas y que no siempre sustituyen a otras más antiguas.
- Las limitaciones presupuestarias.
- La falta de recursos humanos tanto asistenciales como de otras profesiones.

En España, y tomando como referencia los Presupuestos Generales

del Estado, el presupuesto sanitario público inicial para las 17 CCAA fue, para el año 2025, 86.498 millones de euros, lo que representa aproximadamente un 6% del PIB, que está algo por encima de la media de los países de la UE; sin embargo, el gasto por habitante sigue estando por debajo de la media de la UE. La crisis de la pandemia (COVID-19) propició un importante incremento de la inversión en el sector salud. Habrá que esperar unos

Objetivos del ÍNDICE SEIS

Ser una fuente de información útil y concisa para los socios de la SEIS, el SNS, el sector sanitario en general y las empresas del sector TIC.

Contribuir a la planificación e implantación de las TIC, y también a la evaluación de su impacto en la mejora de la eficiencia y calidad, y por lo tanto en la sostenibilidad del sistema.

años para analizar la tendencia de la inversión pública española en sanidad en relación con el PIB.

La actividad propia de los servicios de salud se caracteriza por un procesamiento masivo de información, motivo por el que las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un instrumento imprescindible en todas las facetas de dicha actividad: las de prevención y promoción de la salud, las puramente asistenciales, las de evaluación y las de gestión de calidad, todas ellas requieren tratar una gran cantidad de información de muy alto valor, y todas han incorporado las TIC a su quehacer diario.

La Sociedad Española de Informática de la Salud (SEIS) considera que las TIC, por su capacidad para mejorar el acceso, la equidad, la seguridad, la integración, la continuidad asistencial y la calidad de los servicios sanitarios, así como la convergencia con los servicios sociales, son imprescindibles para afrontar los retos actuales de los sistemas de salud en sus procesos de innovación y racionalización y lograr la transformación digital del sector salud. Además, la utilización intensiva de las TIC en el sec-

tor salud favorece el tejido industrial, la innovación y la economía del país.

Con el objetivo de ayudar a conocer el estado real de la implantación de las TIC en el sector sanitario público español, la SEIS y los responsables TIC de los Servicios de Salud de las Comunidades Autónomas, en colaboración con el Ministerio de Sanidad, Servicios Sociales e Igualdad (actual Ministerio de Sanidad) y de la entidad pública empresarial Red.es abordaron en 2012 la elaboración de un informe, denominado ÍNDICE SEIS, para registrar un conjunto de indicadores significativos que permitieran valorar y cuantificar la implantación de las TIC en la sanidad pública española. Este informe es de periodicidad anual y en este documento se presenta el correspondiente al año 2025.

La SEIS es una sociedad científica, sin ánimo de lucro, independiente de directrices políticas o empresariales, por lo que es una institución adecuada para ejercer el liderazgo en la elaboración del ÍNDICE. Además, al asumir la SEIS el liderazgo de este proyecto cumple con uno de sus objetivos fundacionales: "Promover la utilización eficiente de las TIC en el sector salud".

De acuerdo con los principios establecidos, la SEIS adquirió los siguientes compromisos:

- Garantizar la confidencialidad de los datos originalmente suministrados

Principios seguidos en el 'ÍNDICE SEIS'

En la definición del ÍNDICE se estableció que éste debería estar sujeto a los siguientes principios:

- Para evitar sesgos de cualquier tipo tenía que ser gobernado por una entidad independiente de directrices políticas y empresariales.
- Para garantizar el anonimato de los datos sólo se publicarían datos agregados a escala nacional, valores medios o proporciones, de forma que no se pudieran obtener datos absolutos o individualizados de cada Servicio de Salud.
- Que fuera una publicación anual que permitiera evaluar los avances producidos en la utilización de las TIC en Sanidad y su impacto en el SNS.

trados y el anonimato en los resultados obtenidos.

- Mantener la estructura general del ÍNDICE en las futuras ediciones. Permitiendo introducir modificaciones, como consecuencia del análisis de los resultados obtenidos o por la aparición de nuevos sistemas o técnicas que surjan de la implantación de las TIC y que se consideren estratégicos para el sector.

II. Metodología

La metodología utilizada para la elaboración del ÍNDICE SEIS se basa en una encuesta anual dirigida a los responsables TIC de los Servicios de Salud de todas las Comunidades Autónomas (CCAA), sin incluir para este estudio a las ciudades autónomas de Ceuta y Melilla.

El cuestionario de captura de datos para el ÍNDICE SEIS 2012 incluía 59 indicadores (algunos de ellos con preguntas múltiples). Para adecuar el cuestionario a la evolución experimentada en la implantación de las TIC en el sector, en cada edición es necesario concretar, ampliar o eliminar algunos indicado-

res. El cuestionario de captura de datos para el 2025, que se adjunta como Anexo 1, se ha ampliado con respecto a la edición del 2024 con los nuevos indicadores siguientes:

- Del T.112 al T.116 (sobre Servicios sanitarios para el ciudadano basados en TIC)
- Del T.117 al T.143 (sobre la implantación de la inteligencia artificial)
- Del T.144 al T.146 (sobre la Oficina del Dato de Salud)

Cabe señalar que los ordinales de los indicadores eliminados no se reutilizan, por ello en el cuestionario hay ordinales de indicadores hasta el 146, aunque el cuestionario para el 2025 realmente contiene 73 indicadores.

La información que se solicita en el cuestionario de captura de datos se agrupa en las siguientes categorías:

Plataforma tecnológica

- Número de puestos de trabajo instalados
- Gasto en Plataforma Tecnológica (PT), desglosado por gastos en:
 - CPD
 - Puestos de trabajo
 - Comunicaciones de datos

- Software base de Sistemas y Comunicaciones
 - Sistemas gestores de bases de datos (SGBD)
 - Contratación de servicios externos
 - Gastos en personal propio dedicado a la operación y explotación de la PT
- Desglosados, a su vez (excepto en contratación de servicios externos y gastos en personal propio) por tipo del gasto: adquisiciones, arrendamientos y mantenimientos.

Gasto en sistemas de información

- Gasto en personal propio en Sistemas de Información (SI)
- Gasto en SI horizontales. Se consideran SI horizontales aquellos que proporcionan servicios de tipo general (gestión de recursos humanos, gestión económica y presupuestaria, tarjeta sanitaria, cita previa, ofimática, etc.)
- Gasto en SI verticales. Se consideran SI verticales aquellos que dan soporte a las actividades asistenciales (HCE y/o HES, Farmacia, Radiología, Laboratorios, Anatomía Patológica, etc.)

Grado de implantación de proyectos tecnológicos significativos

- Historia Electrónica de Salud
- Servicios sanitarios para el ciudadano basados en TIC
- Telemedicina
- Telemonitorización y Teleconsultas
- Equipos de electromedicina
- Citaciones para consultas
- Volumen de almacenamiento generado por las imágenes médicas

Gestión de las TIC

- RRHH propios dedicados a las TIC y su distribución por nivel de titulación exigida para el desempeño del puesto de trabajo
- Personal externo disponible a través de contratos de servicios
- Nivel orgánico de la unidad TIC y de la unidad superior de la que depende
- Participación del responsable de la unidad TIC en el comité de dirección del SS

Seguridad de los sistemas de información corporativos

- Nivel orgánico de la unidad de seguridad de los SI corporativos y de

- la unidad superior de la que depende
- Número de técnicos (propios y externos) dedicados en exclusiva a la seguridad de los SI
- Derechos ejercidos por los ciudadanos acordes con el RGPD
- Gasto en seguridad de los SI
- Nivel de implantación de certificados digitales reconocidos entre los profesionales asistenciales
- Implantación de los SOC/CERT (Centro de Operaciones de Ciberseguridad/ Equipo de Respuesta ante Emergencias Informáticas)

Datos generales de la Comunidad Autónoma

- Población protegida
- Presupuesto TIC procedente de fondos propios de la CA
- Presupuesto global sanitario de la CA

Tendencias y proyectos prioritarios

- Proyectos de tendencias tecnológicas implantados y previstos implantar el próximo año
- Inteligencia artificial

- Proyectos prioritarios previstos abordar por el Servicio de Salud en los próximos años
 - Oficina del Dato de Salud
- Para que el ÍNDICE tenga la calidad y fiabilidad exigibles, los datos suministrados en los cuestionarios se analizan bajo una perspectiva global y se comprueba la congruencia y coherencia de la información suministrada. Los datos

Categorías en el cuestionario

- Plataforma tecnológica
- Gasto en sistemas de información
- Grado de implantación de proyectos tecnológicos significativos
- Gestión de las TIC
- Seguridad de los sistemas de información corporativos
- Datos generales de la Comunidad Autónoma
- Tendencias y proyectos prioritarios

inconsistentes se reenvían al correspondiente Servicio de Salud para su depuración y, en algún caso, si se considera necesario se ponderan para el cálculo de valores acumulados a escala nacional.

Para garantizar el anonimato en los resultados obtenidos, y antes de cualquier procesamiento de los datos suministrados en los cuestionarios, una única persona de la Junta Directiva de la SEIS se encarga de convertir cualquier elemento identificador de la comunidad autónoma origen de los datos en códigos anónimos. Para ello, los datos susceptibles de permitir la posible identificación de la comunidad autónoma de procedencia se promedian por 100.000 personas de población protegida.

El tratamiento de los datos consta de tres partes diferenciadas:

- Cálculo de valores acumulados a escala nacional.
- Cálculo de valores relativos correspondientes a cada CA con respecto a 100.000 personas de su población protegida.
- Agregación de los valores relativos de cada indicador a lo largo de los últimos años

Para el cálculo de los valores relativos se toma la población protegida proporcionada por cada Comunidad Autónoma en el cuestionario de captura de datos.

III. Resultados

En este apartado se muestran los resultados correspondientes a datos del año 2025. Estos resultados se basan exclusivamente en los datos suministrados en los cuestionarios, excepto cuando específicamente se indique otra fuente.

De acuerdo con el tipo de tratamiento indicado en la metodología, se presentan cuatro tipos de resultados:

- Tablas con los datos acumulados a escala nacional
- Gráficas con datos relativos de cada comunidad autónoma
- Gráficas con la evolución temporal de algunos indicadores
- Tablas y gráficas de frecuencias

Estas tablas y gráficas permiten conocer parámetros y tendencias relativas al grado de implantación de las TIC en el SNS. Para observar la evolución temporal de los indicadores, tanto en las tablas como en las gráficas, se incluyen

Tabla 1: Población protegida

Población protegida	2022	2023	2024	2025	% vari. 2025-2024
	47.230.055	47.542.316	48.045.583	48.492.006	0,93%

datos de años anteriores.

En la mayoría de las tablas se indica, en la última columna, el porcentaje de variación del 2025 con respecto al 2024 “% vari. 2025-2024”, que se calcula de acuerdo con la siguiente fórmula: (valor del 2025-valor del 2024) /valor del 2024

Las gráficas con datos relativos de cada comunidad autónoma permiten establecer comparaciones entre comunidades autónomas y sus características generales son:

- En la mayoría de estas gráficas se representan los valores del año actual y de los dos años anteriores
- La numeración de las CCAA que aparece en las gráficas es aleatoria, no siguiendo ningún criterio de asignación que permita identificar a qué comunidad autónoma (CA) pertenece un dato. El número (posición) asignado a una CA se conserva a lo largo de todas las gráficas y en las series correspondientes a todos los años.

- El responsable TIC de una comunidad autónoma puede conocer, para un determinado indicador, su situación con respecto al resto de comunidades, pero no sabe a qué comunidad corresponden el resto de los valores relativos que aparecen en las gráficas.
- Para facilitar la comparación y ayudar a conocer el grado de dispersión de los datos, en la mayoría de estas gráficas se representa, en el eje de ordenadas, el valor medio de los valores representados en las mismas. Hay que señalar que estos valores medios no tienen por qué coincidir con los valores medios indicados en las tablas con los acumulados a escala nacional.
- Cuando no aparecen referencias se debe a que no se dispone de los datos necesarios para obtener esa información, situación excepcional. En las gráficas de evolución se indican, para todos los años de los que se disponen datos, los valores medios, del

correspondiente año, de los valores relativos por comunidad autónoma representados en las gráficas anteriores, así como el índice de ajuste R² de la curva de regresión calculada. Para dar mayor visibilidad a estas gráficas, se ha decidido solamente incluir los valores correspondientes a los puntos representados en los tres últimos años, excepto en las gráficas de evolución de los presupuestos TIC que, por su importancia, se indican los valores de todos los puntos representados en las gráficas.

En todas las gráficas también se indica, bajo la forma “Tnn”, el número del indicador o de los indicadores del cuestionario de captura de datos de los que se ha obtenido la información representada en la gráfica correspondiente.

En las tablas y gráficas de frecuencias se indican, el número de veces que una aplicación o proyecto se ha implantado en las diversas CCAA, ordenadas de mayor a menor frecuencia.

Como información general, en la **Tabla 1** se indica el total nacional de la población protegida proporcionada por las CCAA, excepto Ceuta y Melilla, correspondiente a los años 2022, 2023, 2024 y 2025

Tabla 2: Gastos e Inversiones TIC frente a Presupuesto Sanitario

Presupuesto Sanitario, Gastos e Inversiones TIC (en miles de €)	2022	2023	2024	2025	% vari. 2025-2024
PRESUPUESTO GLOBAL SANITARIO	70.920.202	75.743.401	79.758.331	82.329.473	3,22%
GASTO TOTAL EN TIC DE LAS CCAA	896.662	956.084	1.011.078	1.240.373	22,68%
INVERSIÓN TIC DIRECTA DEL MINISTERIO DE SANIDAD EN EL SNS, PROCEDENTE DE LOS PGE Y DEL PRTR (*)	54.803	158.923	93.992	91.301	-2,86%
INVERSIÓN EN SALUD DIGITAL DE RED.ES PARA EL SNS (**)	8.768	31.300	6.000	0	-100,00%
TOTAL GASTO DE LAS CCAA MÁS INVERSIÓN DEL MS Y DE RED.ES	960.233	1.146.307	1.111.070	1.331.674	19,86%
% GASTO DE LAS CCAA MÁS INVERSIÓN DEL MS Y DE RED.ES RESPECTO PRESUPUESTO SANITARIO	1,35%	1,51%	1,39%	1,62%	16,11%

(*) Datos de inversión directa suministrados por el Ministerio de Sanidad

(**) Datos suministrados por Red.es. Red.es informa que 2025 ha sido un año de transición y que en el segundo semestre se han firmado buena parte de los convenios del nuevo programa de Servicios Digitales Inteligentes en el Sistema Nacional de Salud, que dotado con 223 millones de euros, se financiará, junto con el Ministerio de Sanidad, a través de fondos europeos FEDER, pero que se contabilizarán conforme se vayan ejecutando.

Datos de presupuestos y de gastos e inversiones

En la **Tabla 2** se indican, a nivel nacional, el Presupuesto Global Sanitario y los gastos e inversiones TIC ejecutadas en el SNS, desde el 2022 al 2025. En 2025, los gastos e inversiones TIC fueron de

1.331.674 miles de euros, esta cantidad es la suma del gasto global TIC de las CCAA, más las inversiones TIC realizadas en el SNS por el Ministerio de Sanidad (MS), y por la entidad pública Red.es, y representa el 1,62% del Presupuesto Global Sanitario.

Tabla 3: Datos presupuestarios TIC para el SNS

Datos Presupuestarios	2022	2023	2024	2025	% vari. 2025-2024
PRESUPUESTO GLOBAL SANITARIO (en miles de €)	70.920.202	75.743.401	79.758.331	82.329.473	3,22%
PRESUPUESTO TIC DE LAS CCAA (en miles de €)	957.809	883.477	848.419	1.027.571	21,12%
% PRESUPUESTO TIC DE LAS CCAA RESPECTO AL GLOBAL SANITARIO	1,35%	1,17%	1,06%	1,25%	17,33%
FONDOS PROCEDENTES DE PLANES Y PROYECTOS ESTRATÉGICOS TIC, TRANSFERIDOS POR EL MS A LAS CCAA (*)	--	160.000	149.000	--	-100,00%
FONDOS TRANSFERIDOS POR EL MS A RED.ES PARA CUBRIR LA COFINANCIACIÓN NACIONAL DEL PROGRAMA POPE PARA LA LÍNEA SANIDAD (*)	--	--	84.105	--	-100,00%

(*) Datos suministrados por el Ministerio de Sanidad

En la **Tabla 3** se indican los siguientes datos:

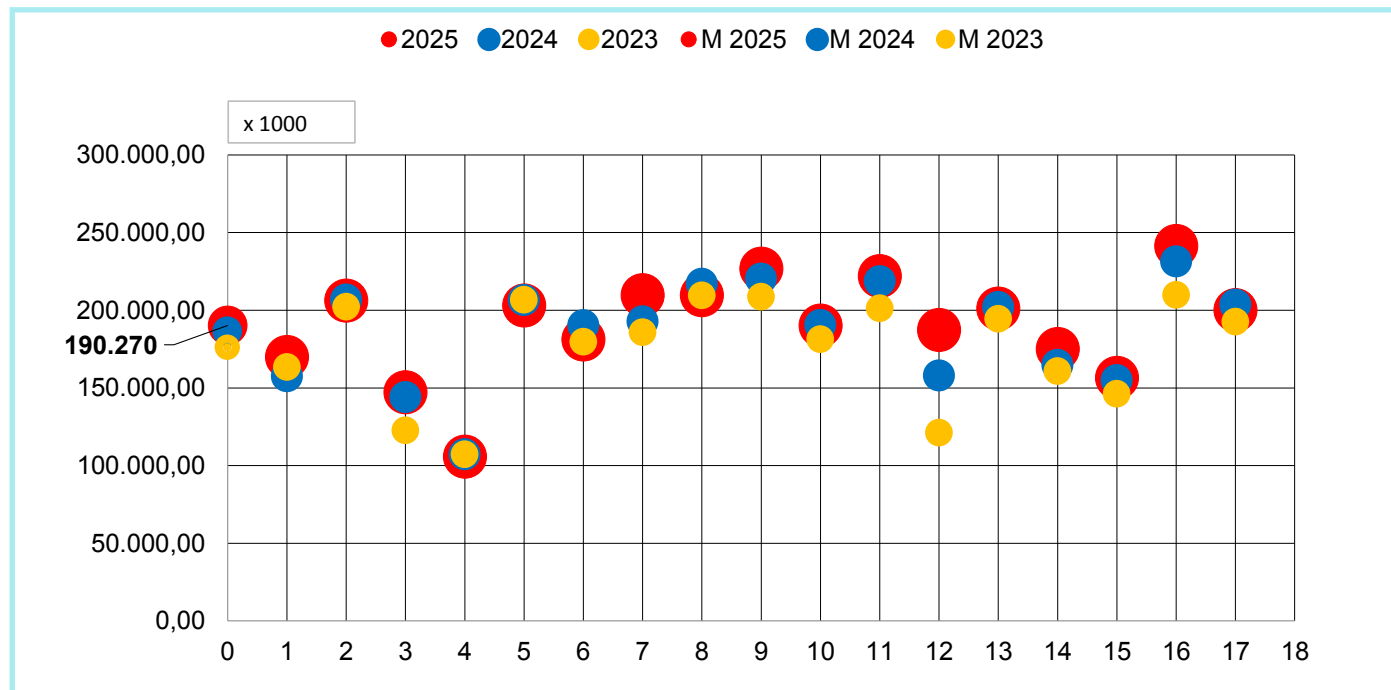
- El presupuesto global sanitario público del conjunto de las 17 CCAA, que en 2025 asciende a 82.329.473 miles de euros, que supone un incremento del 3,22% respecto al presupuesto del 2023.
- El presupuesto global en TIC del conjunto de las CCAA, que en 2025 es de 1.027.571 miles de euros que repre-

senta una variación del 21,12% respecto al de 2024.

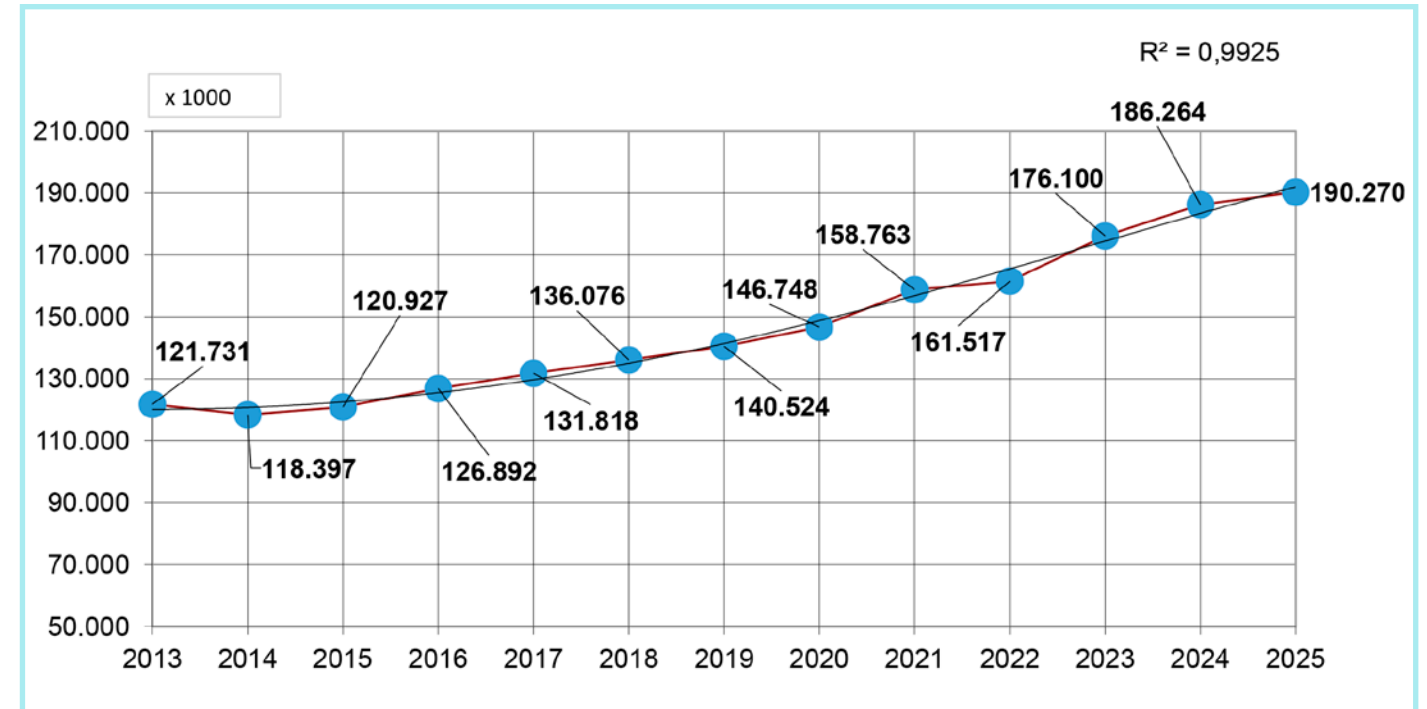
- El porcentaje del presupuesto TIC respecto al presupuesto global sanitario, que en 2025 es el 1,25%, con un incremento del 17,33% sobre el porcentaje del 2024.
- En 2025 el Ministerio de Sanidad (MS) no efectuó transferencias directas a las CCAA ni a través de Red.es para la cofinanciación nacional del programa POPE para la línea Sanidad.

En la **Gráfica 1** se representa, por comunidades autónomas, el presupuesto global sanitario de 2023, 2024 y 2025 en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica en el 2025 es 190.270 (columna 0).

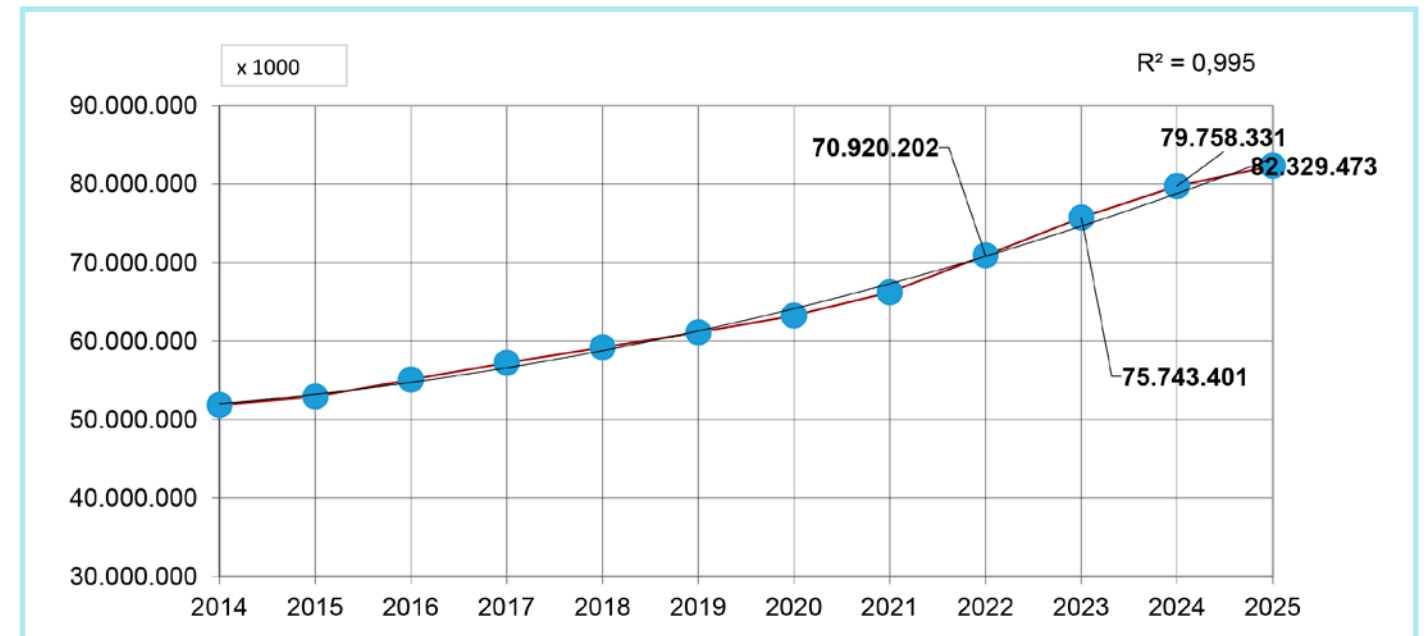
Gráfica 1: Presupuesto global sanitario por 100.000 personas de población protegida



Gráfica 2: Evolución de los valores medios del presupuesto global sanitario por 100.000 personas de población protegida

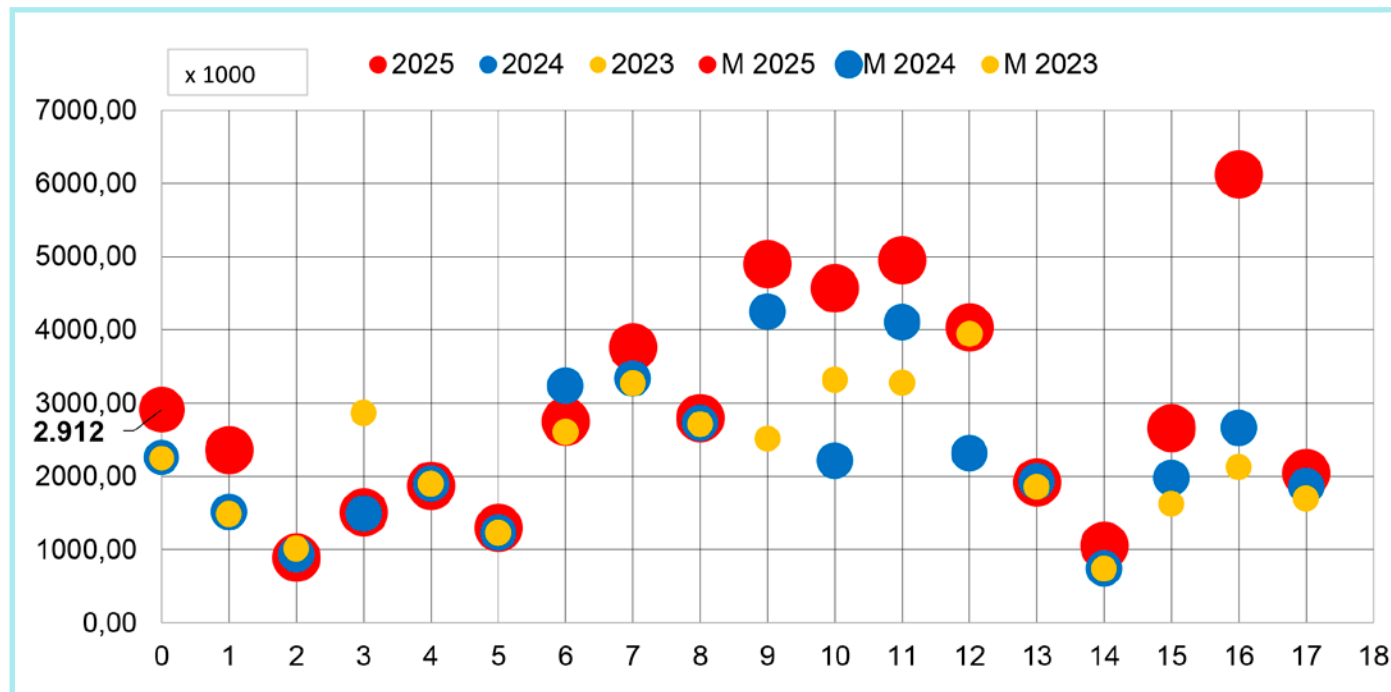


Gráfica 3: Evolución del presupuesto global sanitario en valores absolutos, en miles de euros

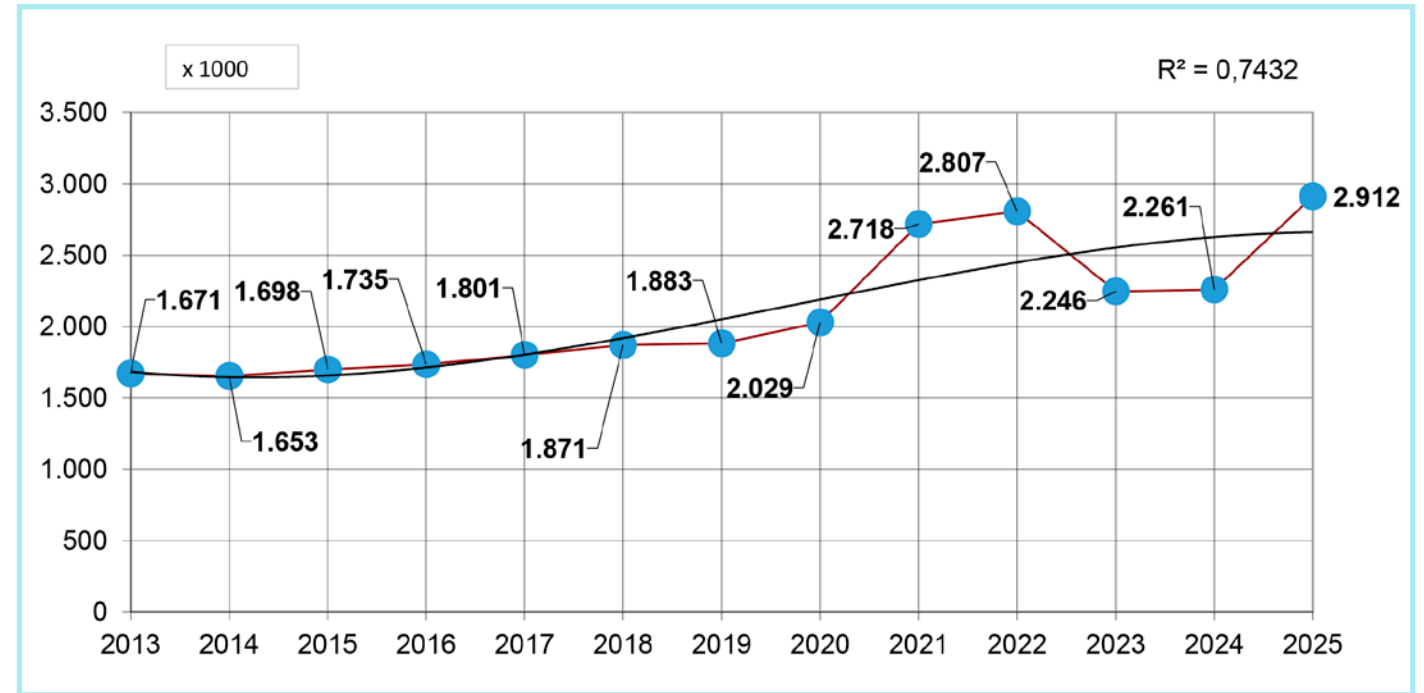


En la **Gráfica 4** se representa, por comunidades autónomas, el presupuesto global TIC en miles de euros, ponderado por 100.000 personas de población protegida, en los años 2023, 2024 y 2025. La media de los valores representados en la gráfica para el 2025 es 2.912 miles de € (columna 0).

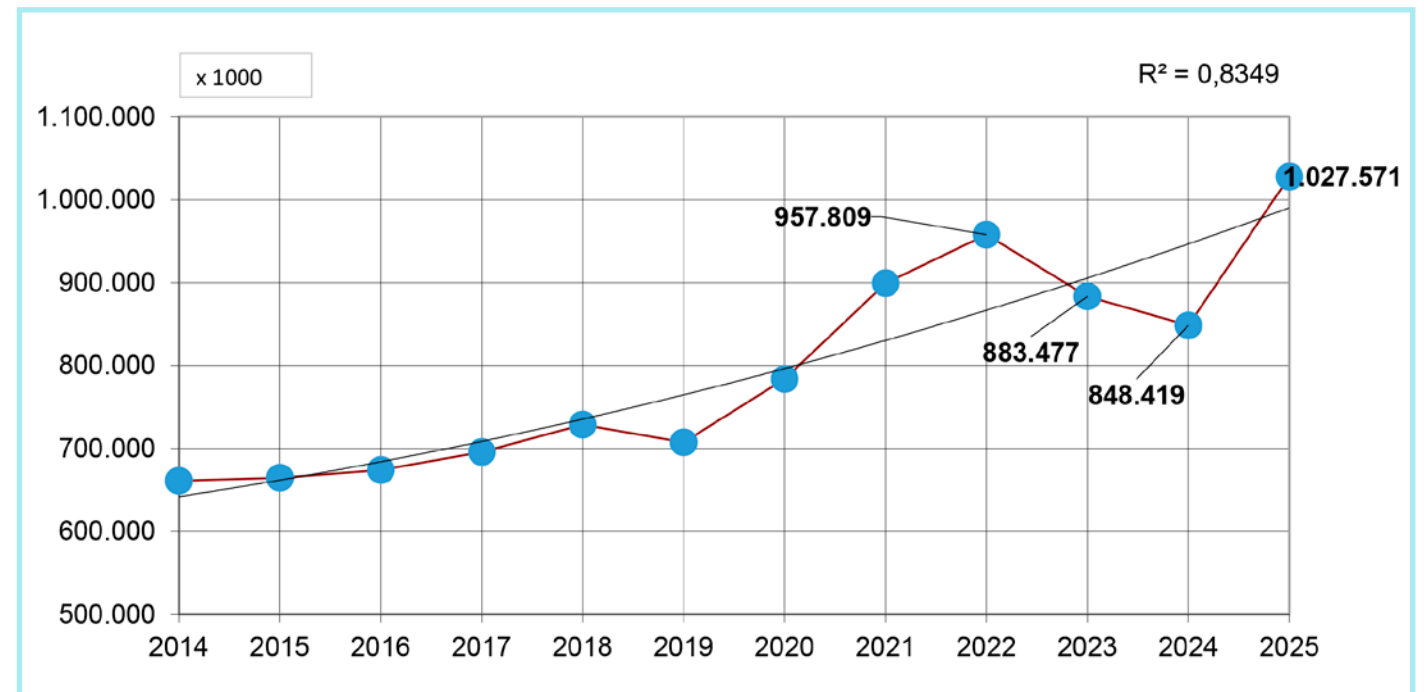
Gráfica 4: Presupuesto global TIC por 100.000 personas de población protegida



Gráfica 5: Evolución de los valores medios del presupuesto global TIC por 100.000 personas de población protegida

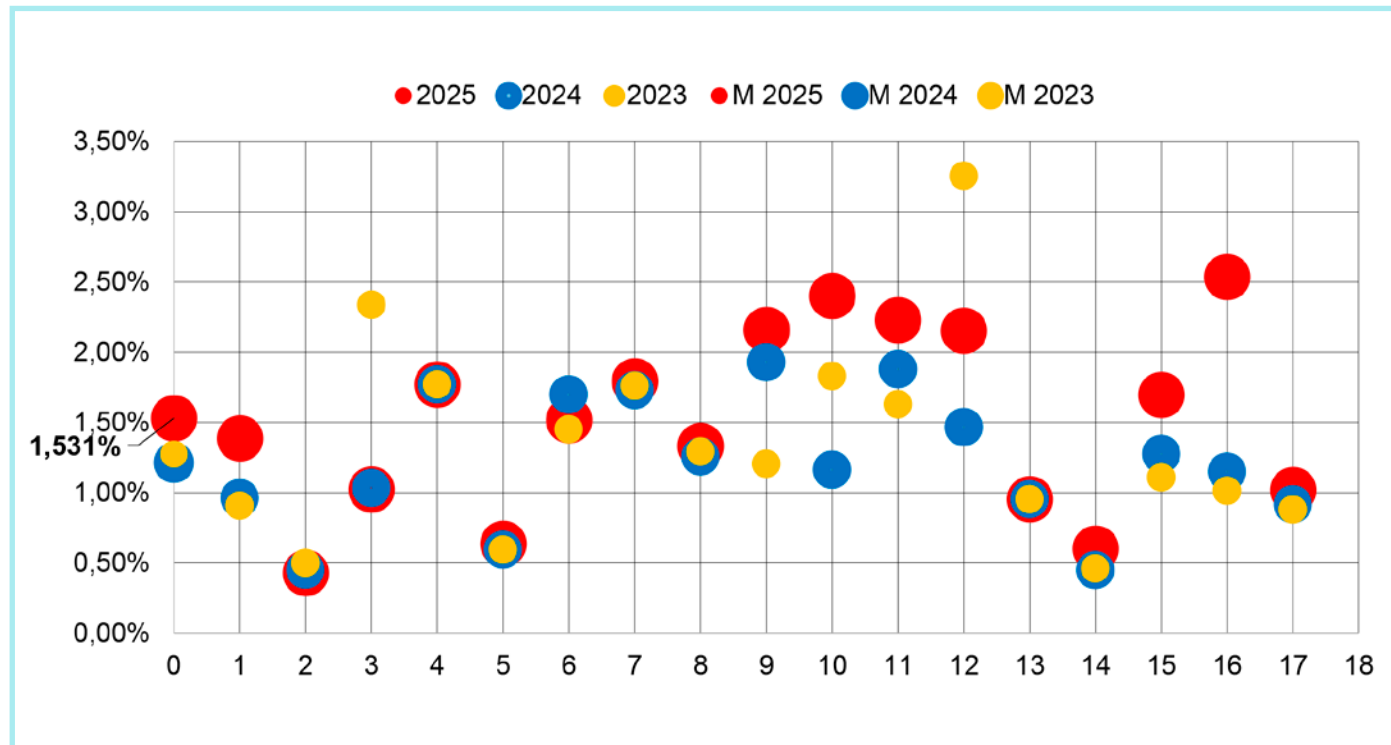


Gráfica 6: Evolución del presupuesto global TIC de las CCAA en valores absolutos

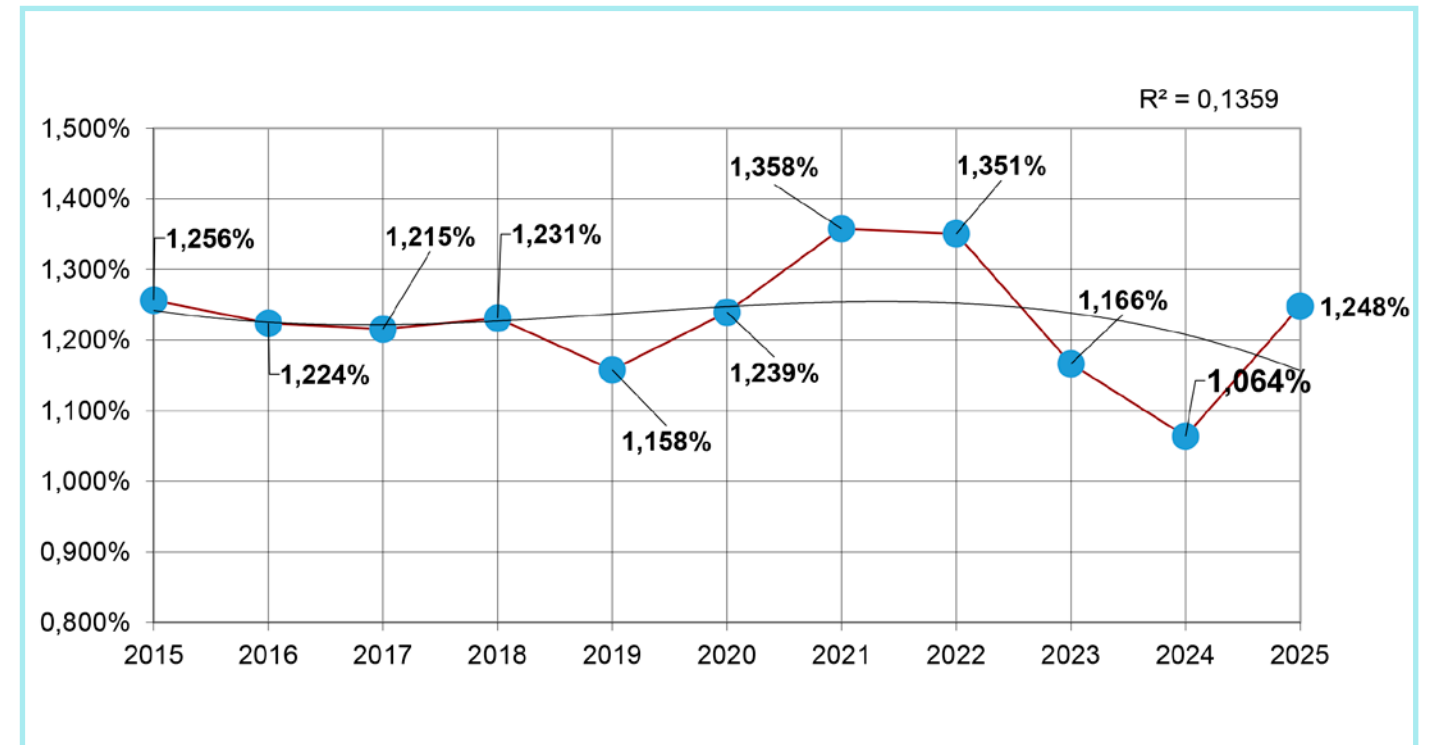


En la **Gráfica 7** se representa, por comunidades autónomas, el porcentaje del presupuesto global TIC con respecto al presupuesto global sanitario de los años 2023, 2024 y 2025. La media de los valores representados en la gráfica para el 2025 es 1,531% (columna 0).

Gráfica 7: Ratio del presupuesto global TIC respecto al presupuesto global sanitario en % por 100.000 personas de población protegida



Gráfica 8: Evolución del ratio del presupuesto global TIC de las comunidades autónomas respecto al presupuesto global sanitario (en valores absolutos) en %



Puestos de trabajo y espacio de almacenamiento generado por las imágenes médicas

La **Tabla 4** muestra el número total de puestos de trabajo instalados y el espacio de almacenamiento generado por las imágenes médicas en 2022, 2023, 2024 y 2025.

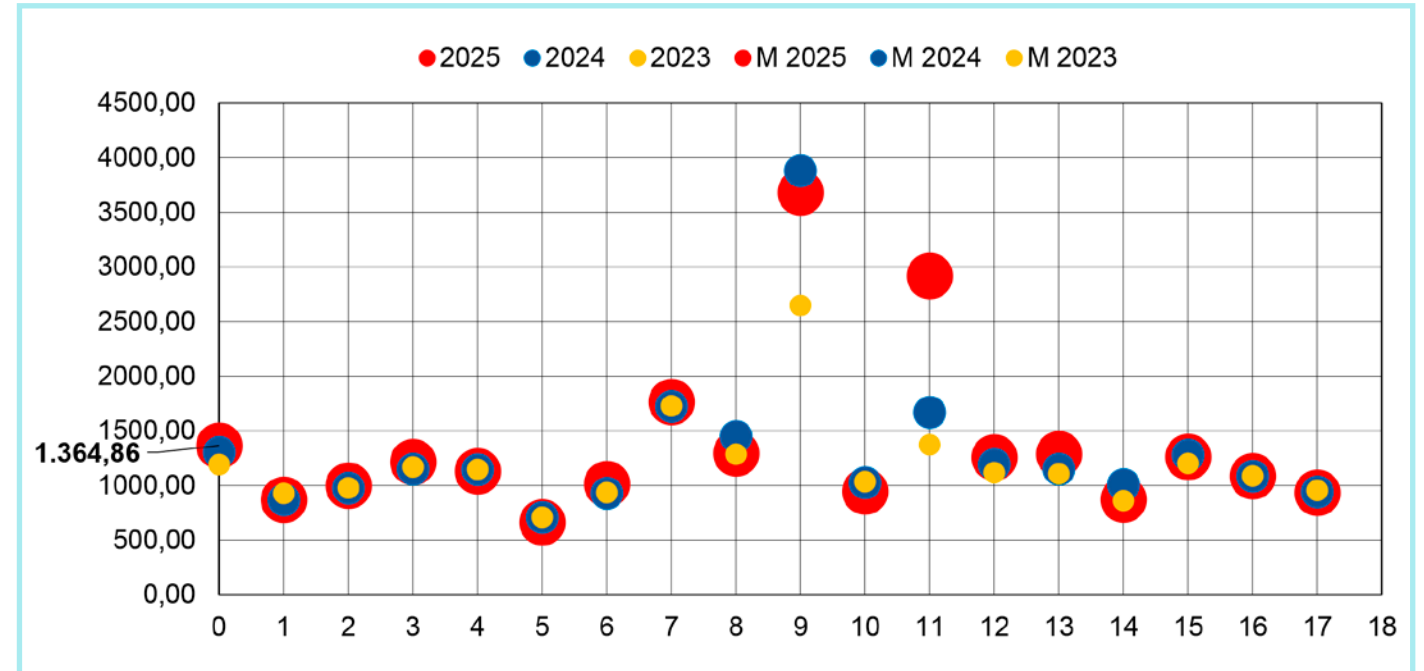
Tabla 4: Plataforma tecnológica

Plataforma tecnológica (infraestructura)	2022	2023	2024	2025	% vari. 2025-2024
Número de puestos de trabajo (1)	484.321	528.223	574.820	577.533	0,47%
Terabytes generados en las exploraciones médicas (imágenes)	3.918	5.417	4.518	5.190	14,88%

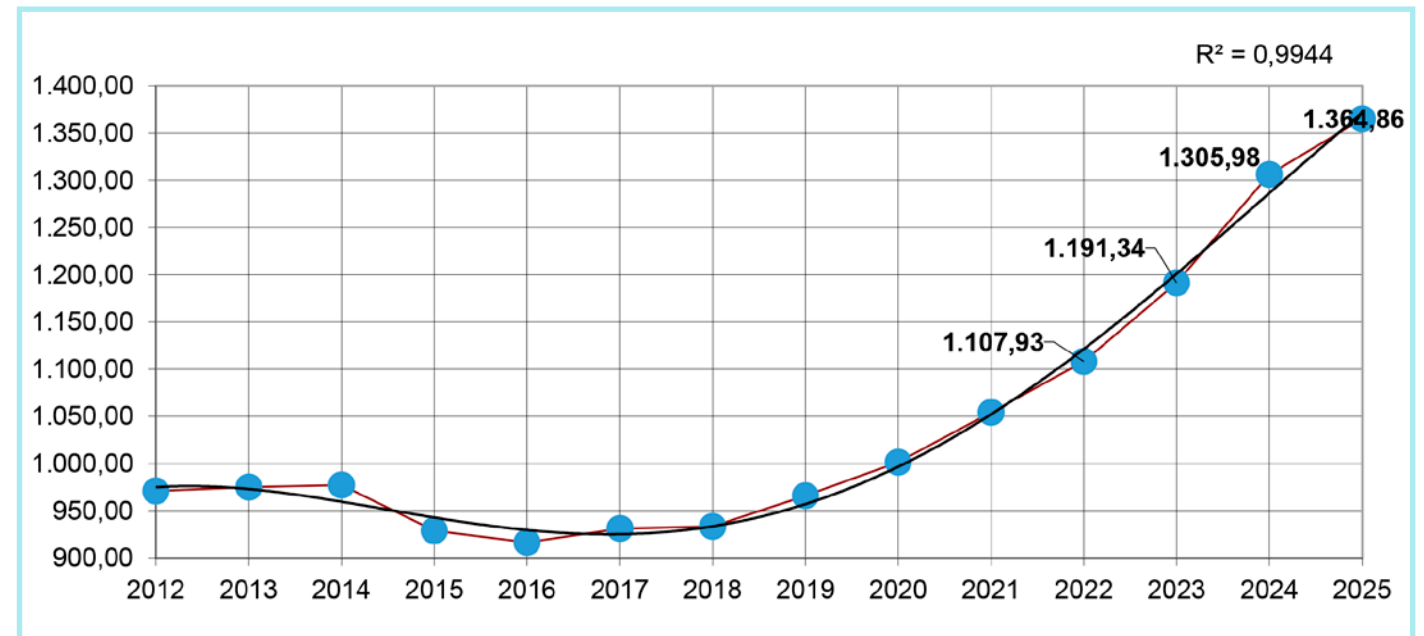
(1) Se considera puesto de trabajo a la infraestructura informática que utiliza el usuario final (PC, impresoras, portátiles, tabletas, entre otros).

En la **Gráfica 9** se representa, por comunidades autónomas, el número de puestos de trabajo instalados en 2023, 2024 y 2025, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 1.364,86 (columna 0).

Gráfica 9: Puestos de trabajo por 100.000 personas de población protegida

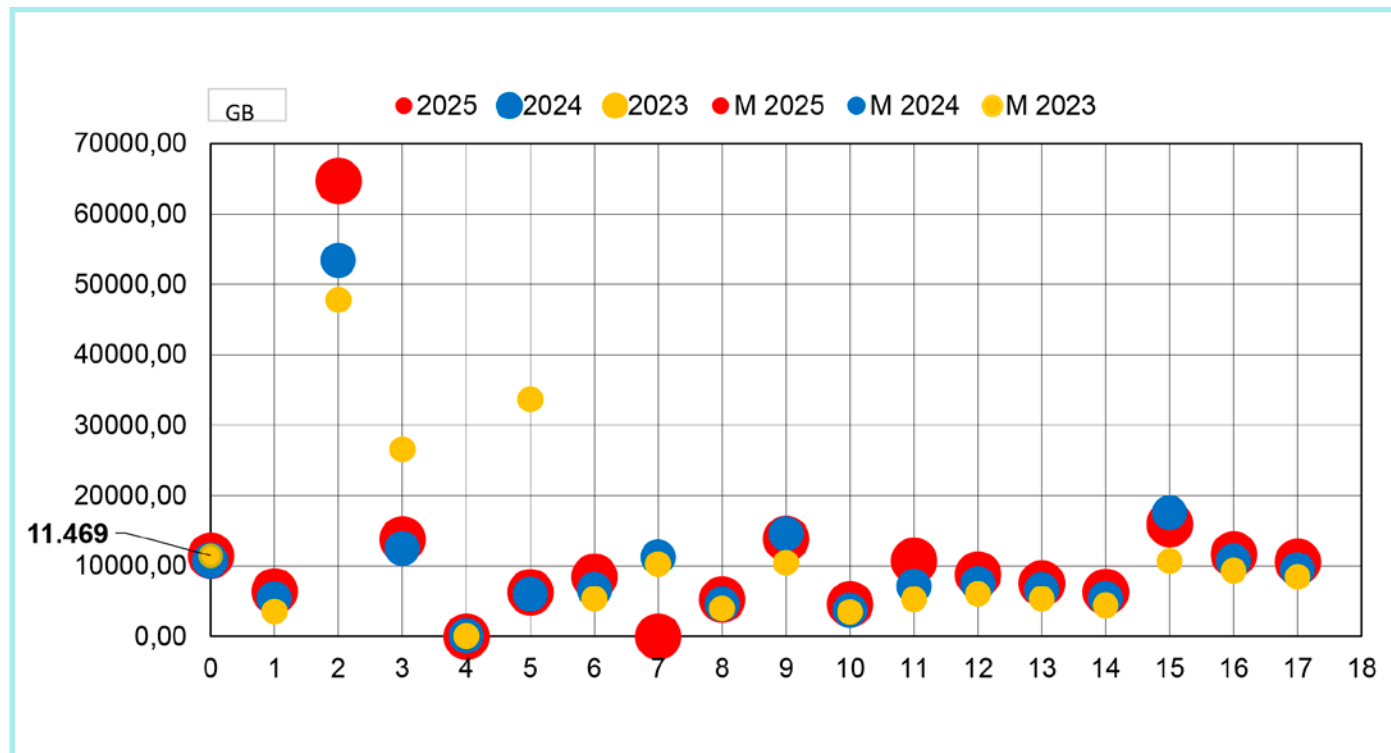


Gráfica 10: Evolución de los valores medios del número de puestos de trabajo por 100.000 personas de población protegida

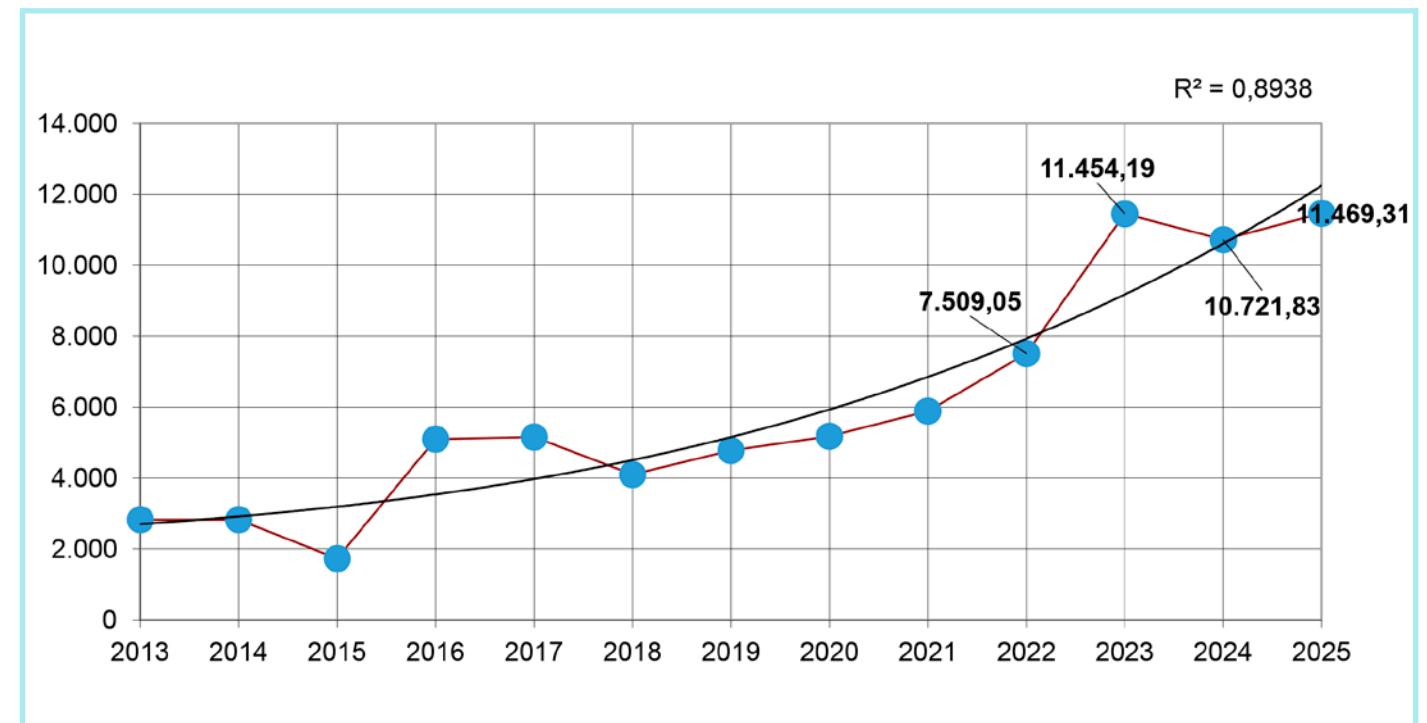


En la **Gráfica 11** se representa, por comunidades autónomas, el espacio de almacenamiento consumido, en GB, para almacenar las imágenes médicas generadas en el correspondiente año, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 11.469 GB (columna 0). Por motivos de coherencia con las gráficas de ediciones anteriores GB, en esta gráfica se mantiene como referencia la unidad de medida de almacenamiento en GB, aunque en el cuestionario y en tabla correspondiente se mida en TB.

Gráfica 11: Espacio de almacenamiento generado en las exploraciones médicas (imágenes) en GB por 100.000 personas de población protegida



Gráfica 12: Evolución de los valores medios del espacio consumido, en GB, para almacenar las imágenes médicas generadas por cada 100.000 personas de población protegida



Gasto en TIC

En la **Tabla 5** se muestran los gastos en TIC a nivel nacional de 2022, 2023, 2024 y 2025 desglosados en: plataforma tecnológica (PT), sistemas de información (SI); en ambos casos está incluido el gasto en personal propio. También se indican los gastos en seguridad, que se piden de forma independiente por lo que ya están incluidos en los gastos indicados anteriormente.

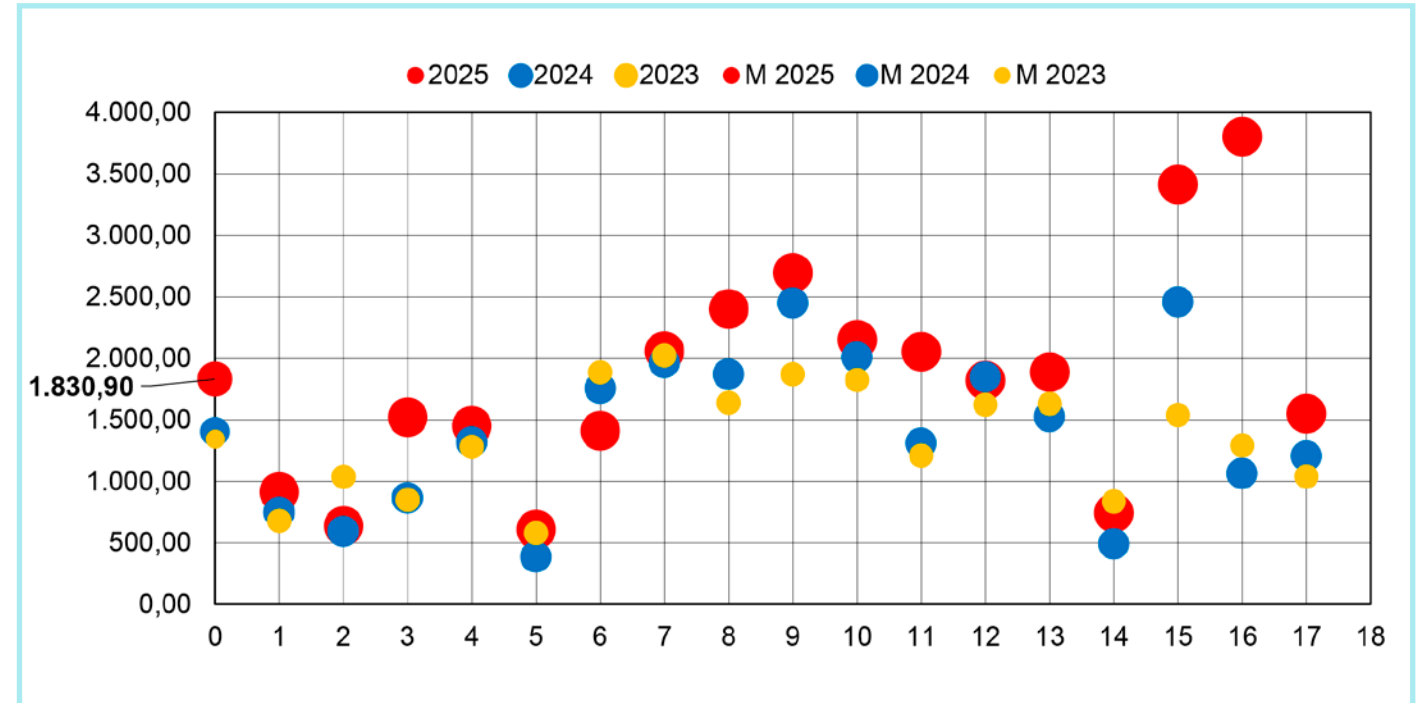
En la **Gráfica 13** se representa, por comunidades autónomas, el gasto global en plataforma tecnológica, en miles de euros, ponderando por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 1.830,90 (columna 0).

Tabla 5: Desglose de los gastos en TIC a escala nacional

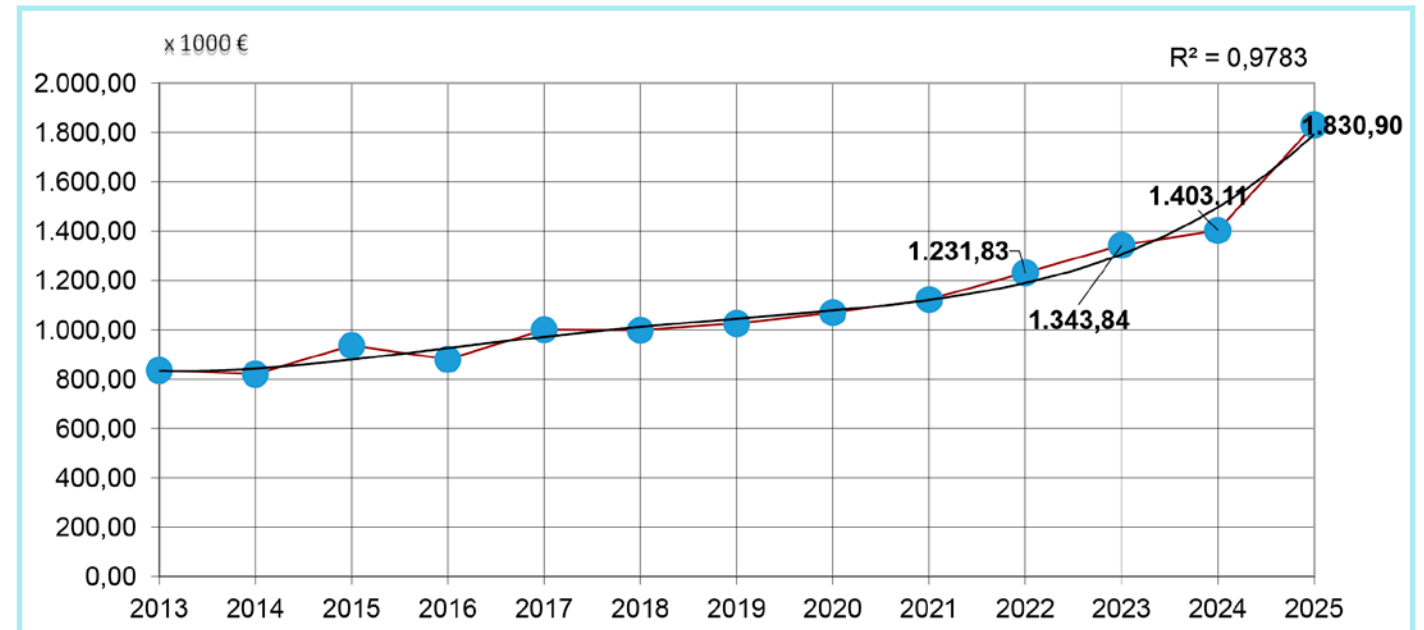
Desglose de los gastos TIC	2022	2023	2024	2025		% vari. 2025-2024
	En miles €	En miles €	En miles €	En miles €	% sobre el Presupuesto TIC	
Gasto global en plataforma tecnológica (incluido personal propio)	467.510	538.896	532.198	696.209	67,75%	30,82%
Gasto global en sistemas de información (incluido personal propio)	418.400	408.518	453.758	528.191	51,40%	16,40%
Otros gastos no incluidos	10.752	8.671	25.122	15.973	1,55%	-36,42%
en PT ni en SI	896.662	956.084	1.011.078	1.240.373	120,71%	22,68%
Gasto Total en TIC de las CCAA	26.471	26.986	37.039	49.624	4,83%	33,98%

(*) El gasto en seguridad se calcula de forma independiente, no suma a los otros gastos. Está incluido en los gastos anteriores

Gráfica 13: Gasto global en plataforma tecnológica por 100.000 personas de población protegida

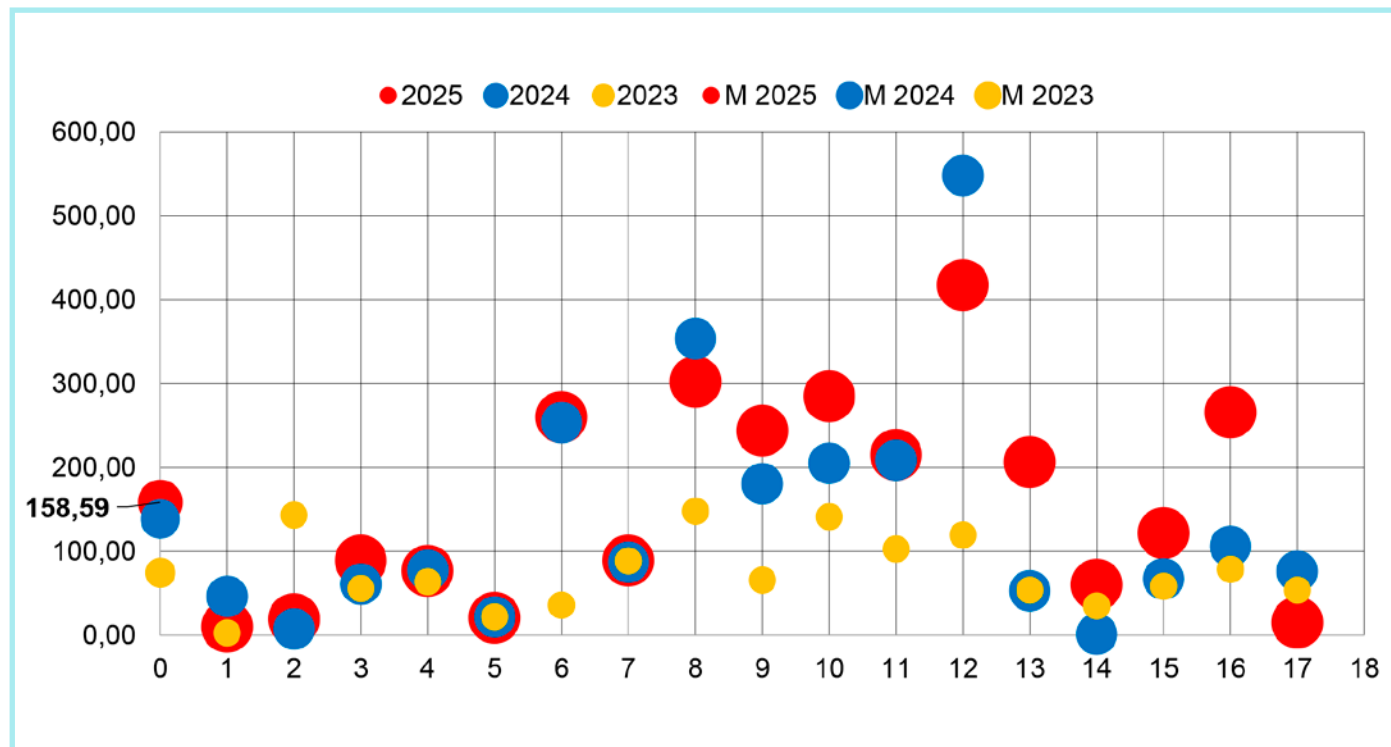


Gráfica 14: Evolución del gasto global medio en plataforma tecnológica por 100.000 personas de población protegida

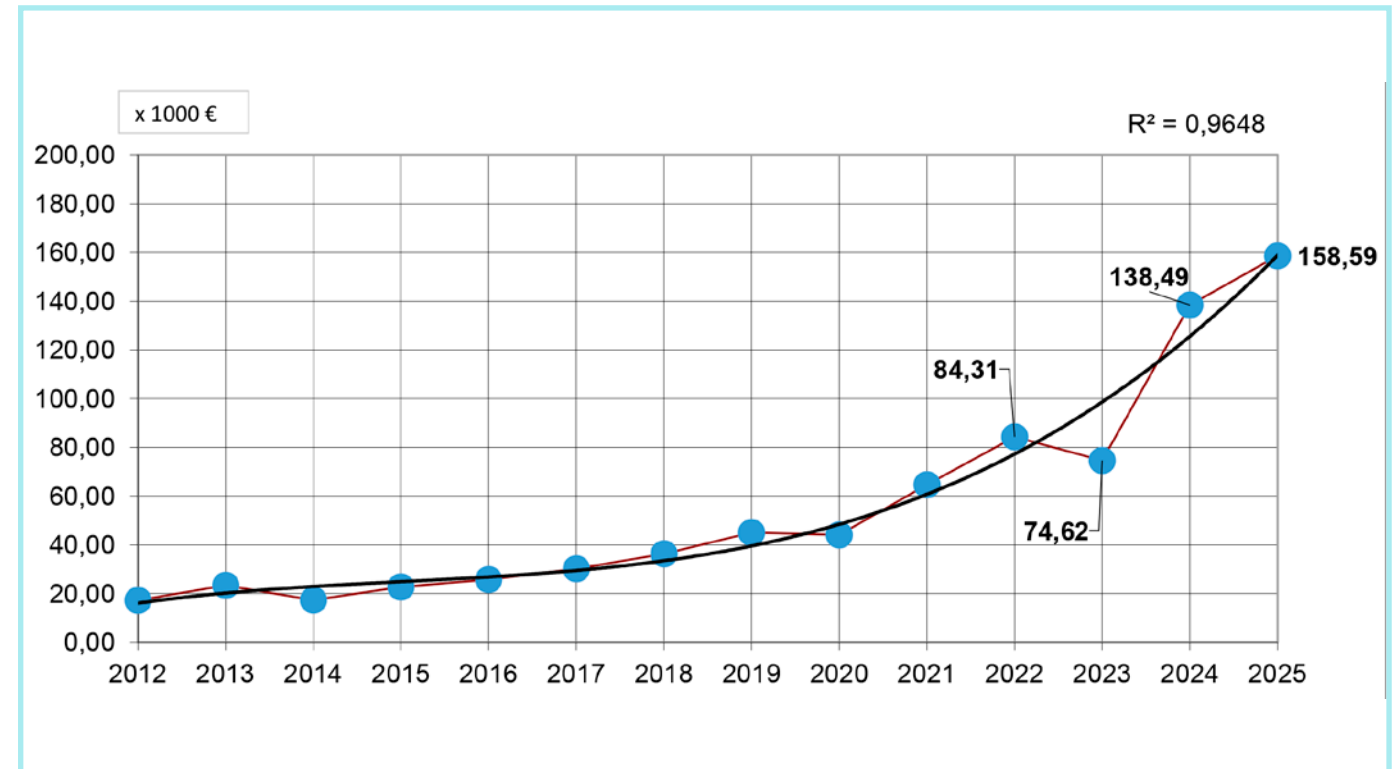


En la **Gráfica 15** se representa, por comunidades autónomas, el gasto en seguridad de los sistemas de información, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para e 2025 es 158,59 (columna 0).

Gráfica 15: Gasto en seguridad de los sistemas de información por 100.000 personas de población protegida



Gráfica 16: Evolución del gasto medio en seguridad de los sistemas de información por 100.000 personas de población protegida



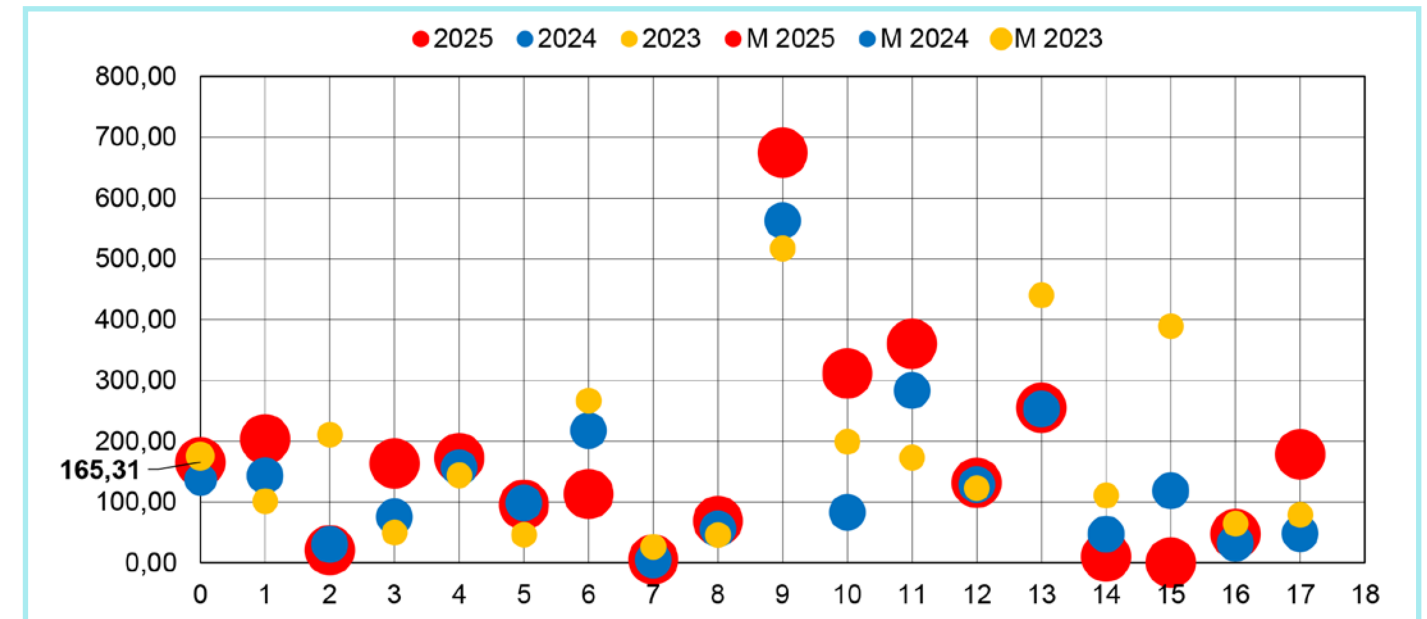
En la **Tabla 6** se muestra el desglose del gasto global acumulado a escala nacional en plataforma tecnológica en los años 2022, 2023, 2024 y 2025. Para el 2025 se proporciona, además del importe, el porcentaje respecto al presupuesto global TIC de las CCAA.

Tabla 6: Desglose del gasto global en plataforma tecnológica

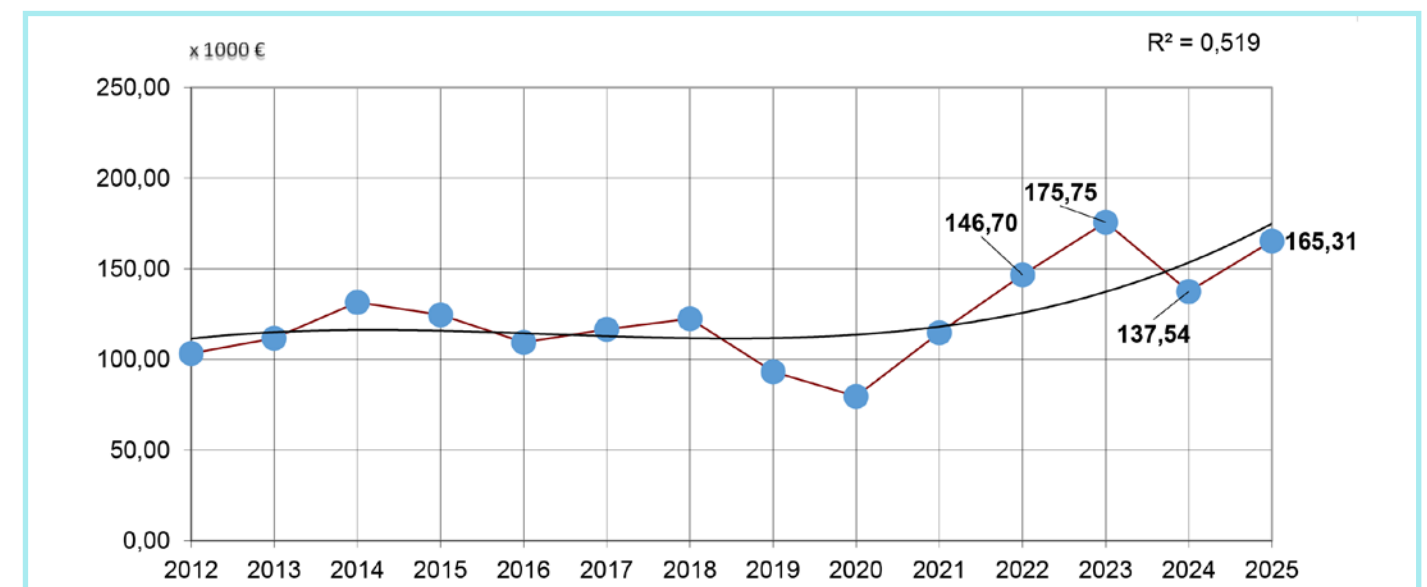
Desglose del gasto global en plataforma tecnológica (PT)	2022	2023	2024	2025		% variación 2025/2024
	En miles €	En miles €	En miles €	En miles €	% sobre el Presupuesto TIC	
En CPD	57.412	75.604	61.792	73.772	7,18%	19,39%
En puestos de trabajo	85.043	114.668	77.917	103.721	10,09%	33,12%
En comunicaciones de datos	63.044	70.514	75.544	76.704	7,46%	1,54%
En software base de sistemas y comunicaciones	46.243	53.371	53.173	78.421	7,63%	47,48%
En sistemas gestores de BD	23.122	24.722	18.566	19.976	1,94%	7,59%
En contratación de servicios externos	148.048	157.119	182.582	291.462	28,36%	59,63%
En personal propio dedicado exclusivamente a PT	24.763	26.300	31.216	30.131	2,93%	-3,48%
Otros gastos	19.835	16.597	31.407	22.021	2,14%	-29,88%
Gasto total en PT	467.510	538.896	532.198	696.209	67,75%	30,82%

En la **Gráfica 17** se representa, por comunidades autónomas, el gasto en CPD, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 165,31 (columna 0).

Gráfica 17: Gasto en CPD por 100.000 personas de población protegida

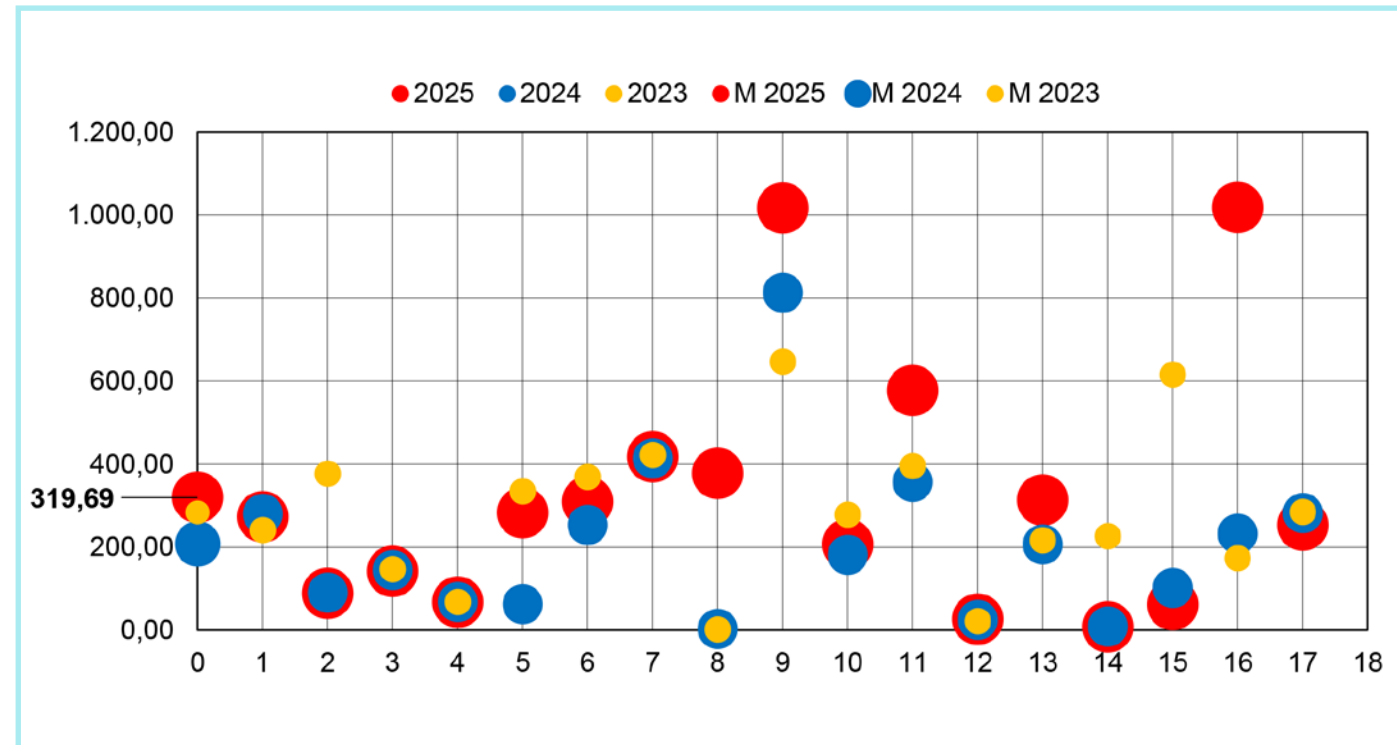


Gráfica 18: Evolución del gasto medio en CPD por 100.000 personas de población protegida

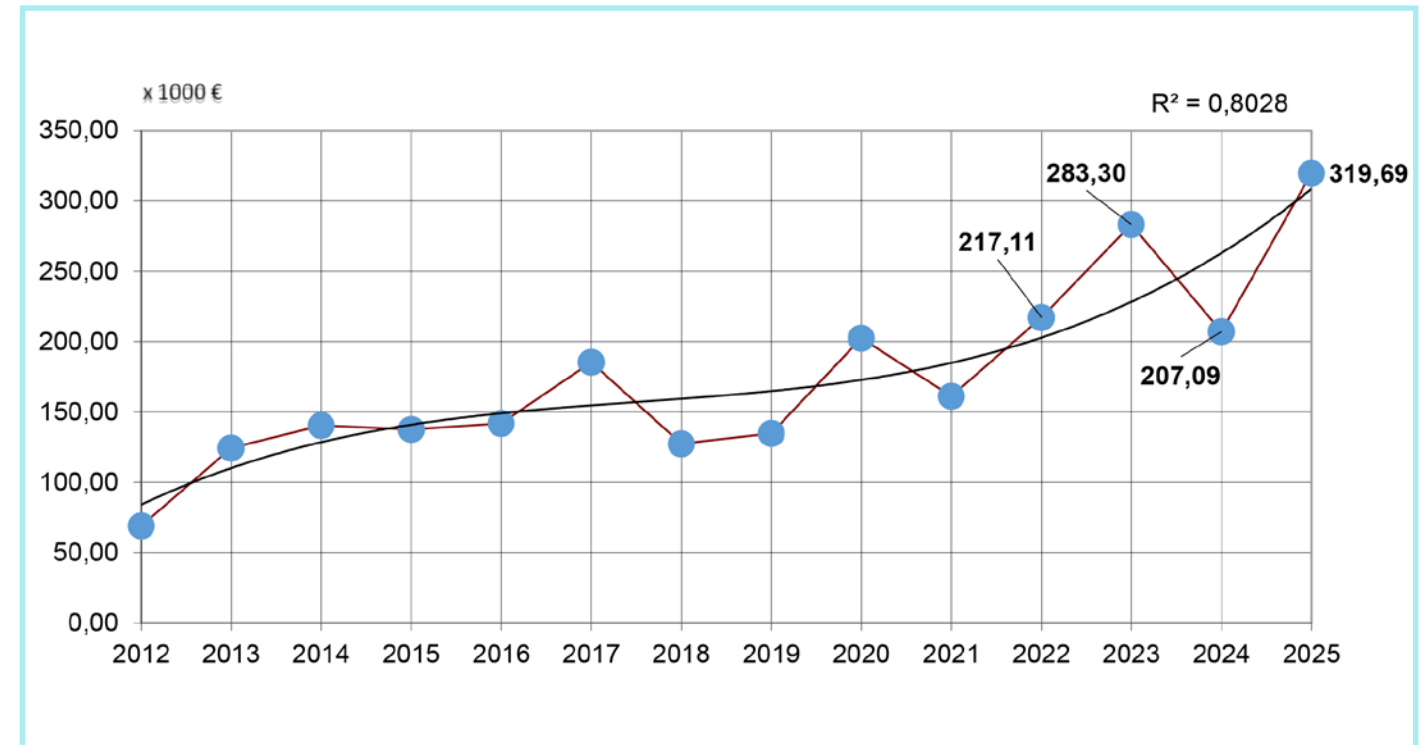


En la **Gráfica 19** se representa, por comunidades autónomas, el gasto en puestos de trabajo, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 319,69 (columna 0).

Gráfica 19: Gasto en puestos de trabajo por 100.000 personas de población protegida

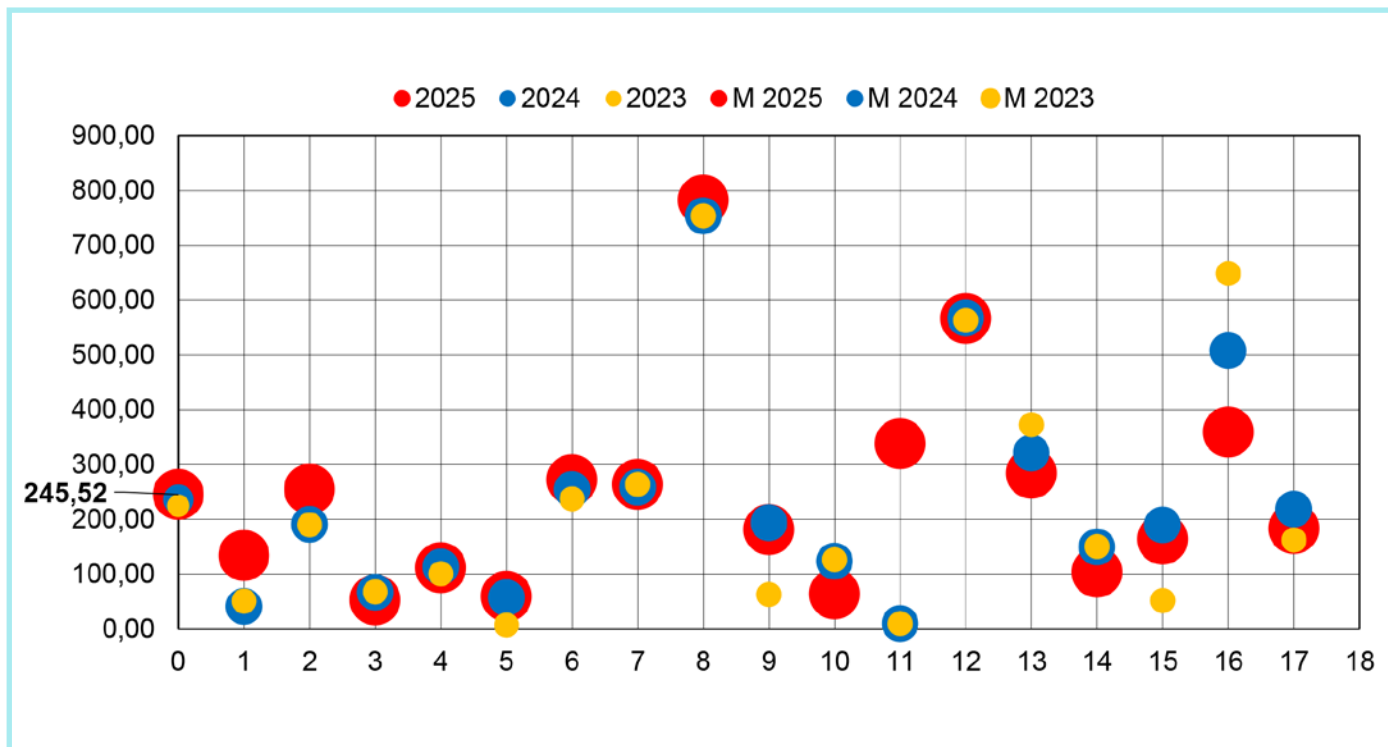


Gráfica 20: Evolución de la media del gasto en puestos de trabajo por 100.000 personas de población protegida

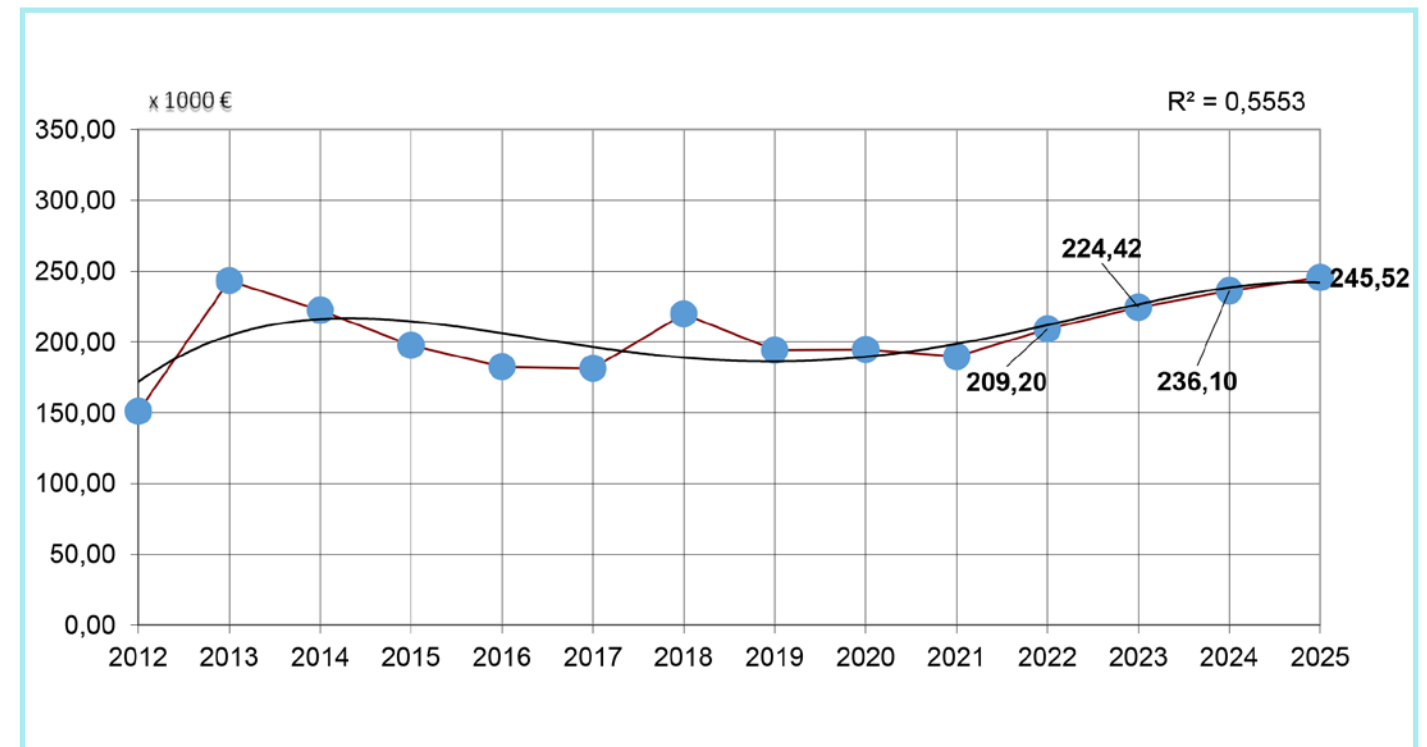


En la **Gráfica 21** se representa, por comunidades autónomas, el gasto en comunicaciones de datos, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para 2025 es 245,52 (columna 0).

Gráfica 21: Gasto en comunicaciones de datos por 100.000 personas de población protegida

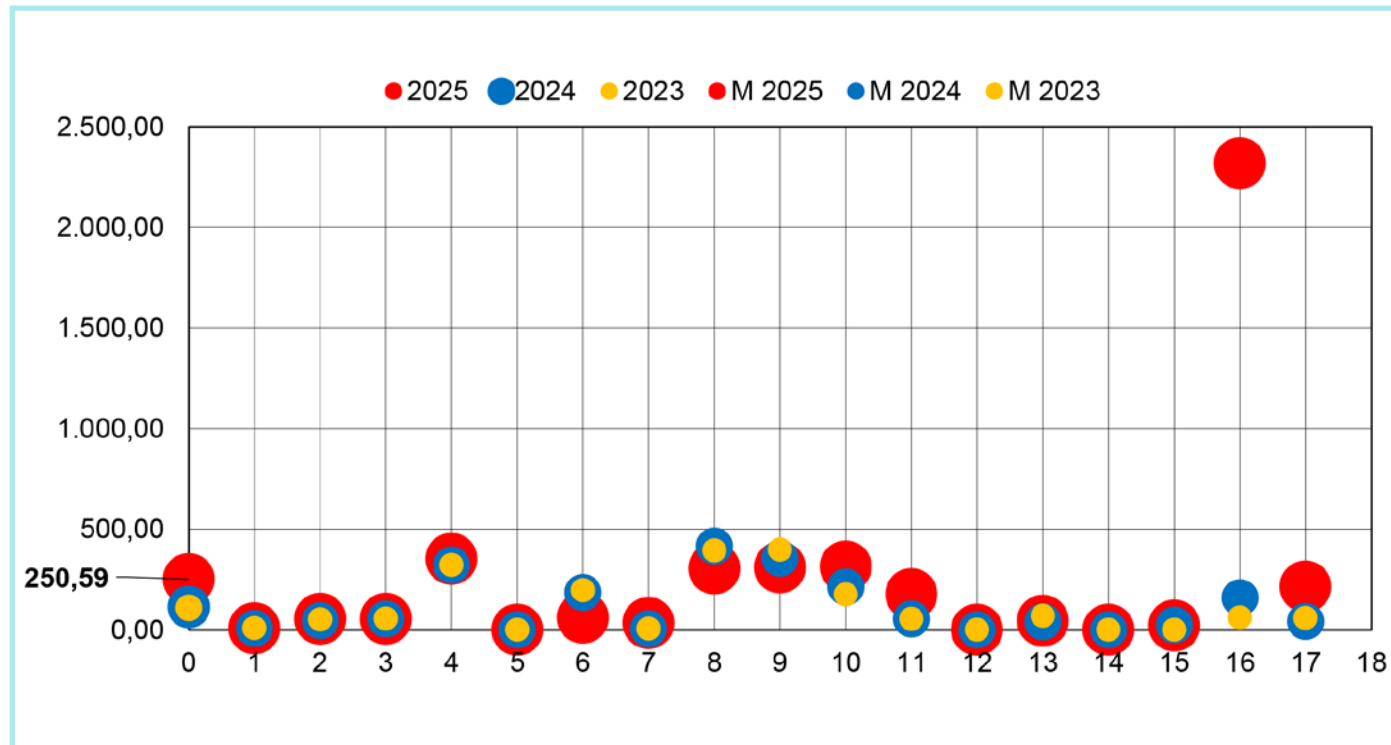


Gráfica 22: Evolución de la media del gasto en comunicaciones de datos por 100.000 personas de población protegida

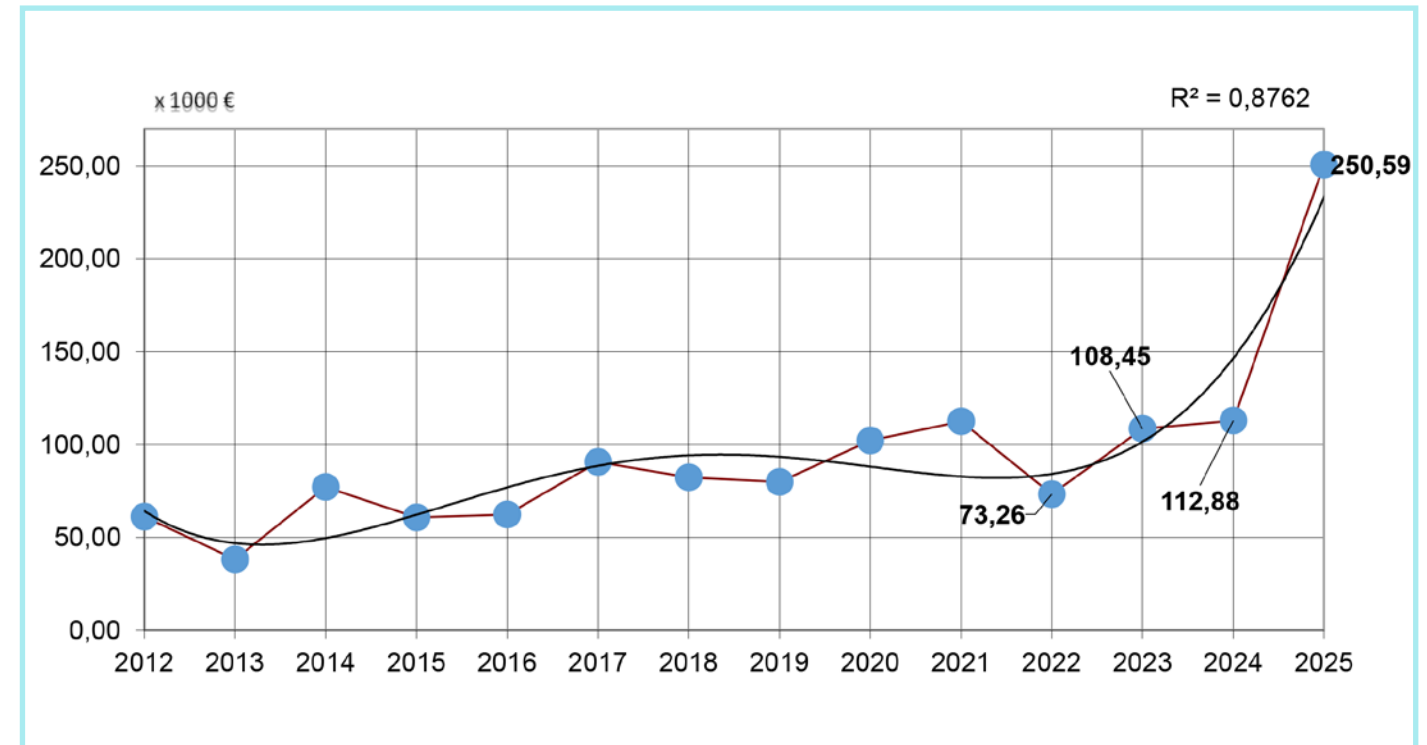


En la **Gráfica 23** se representa, por comunidades autónomas, el gasto en software base de sistemas y comunicaciones, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 250,59 (columna 0).

Gráfica 23: Gasto en software base de sistemas y comunicaciones por 100.000 personas de población protegida

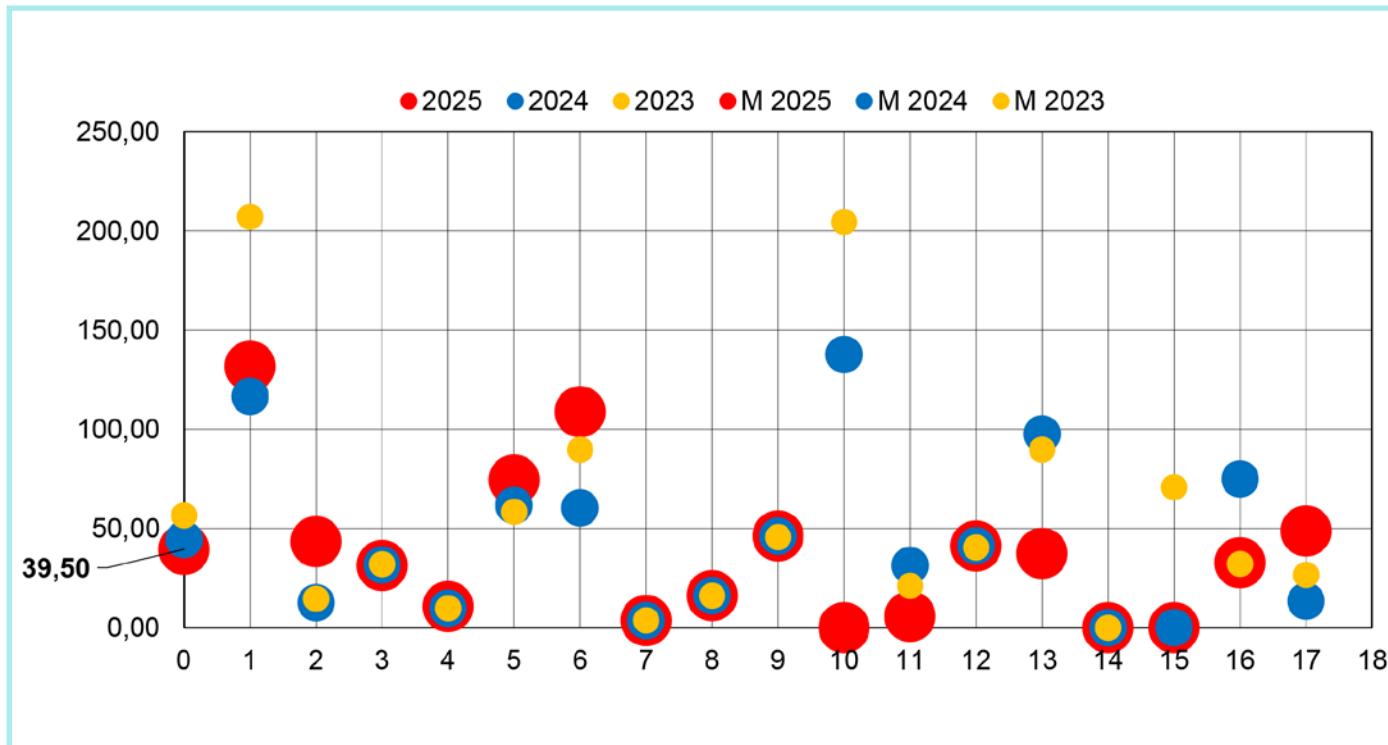


Gráfica 24: Evolución de la media del gasto en software base de sistemas y comunicaciones por 100.000 personas de población protegida

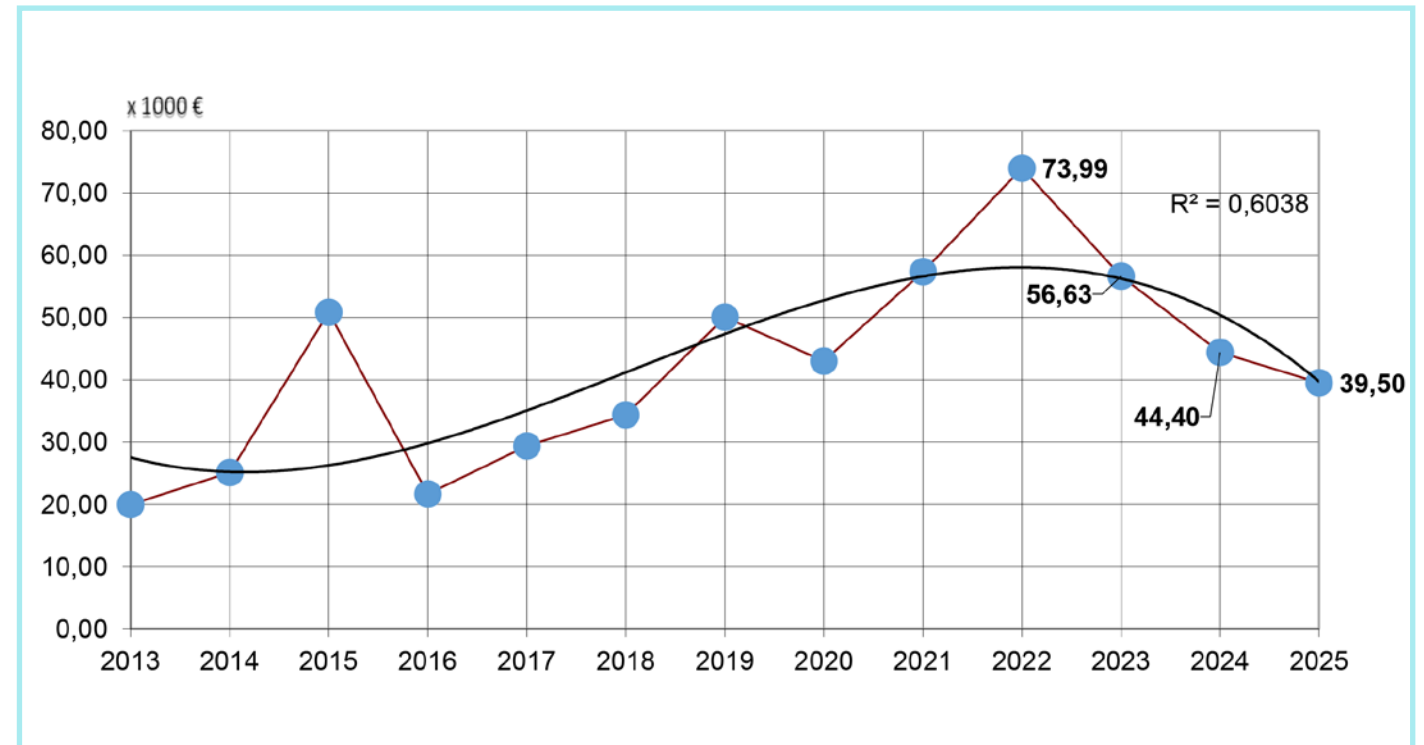


En la **Gráfica 25** se representa, por comunidades autónomas, el gasto en contratación de sistemas gestores de bases de datos, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 39,50 (columna 0).

Gráfica 25: Gasto en sistemas gestores de bases de datos por 100.000 personas de población protegida

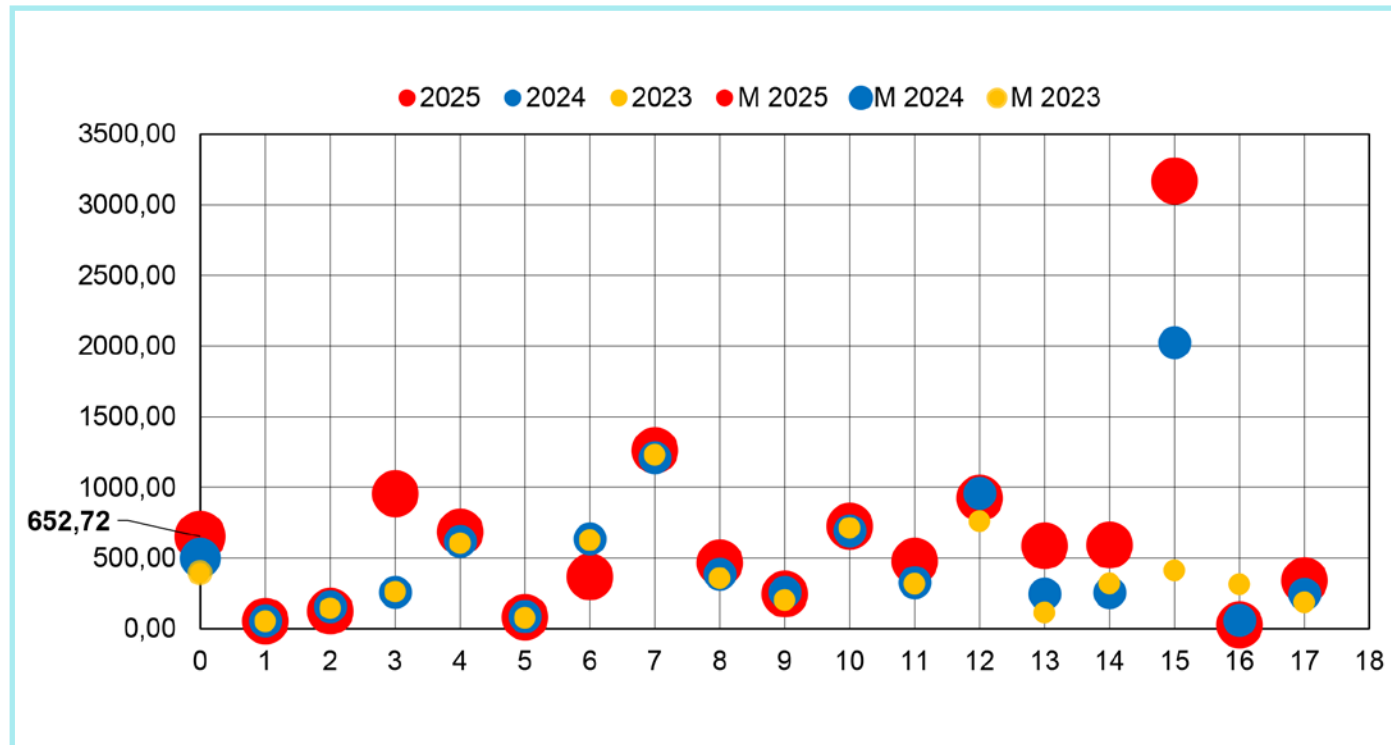


Gráfica 26: Evolución del gasto medio en sistemas gestores de bases de datos por 100.000 personas de población protegida

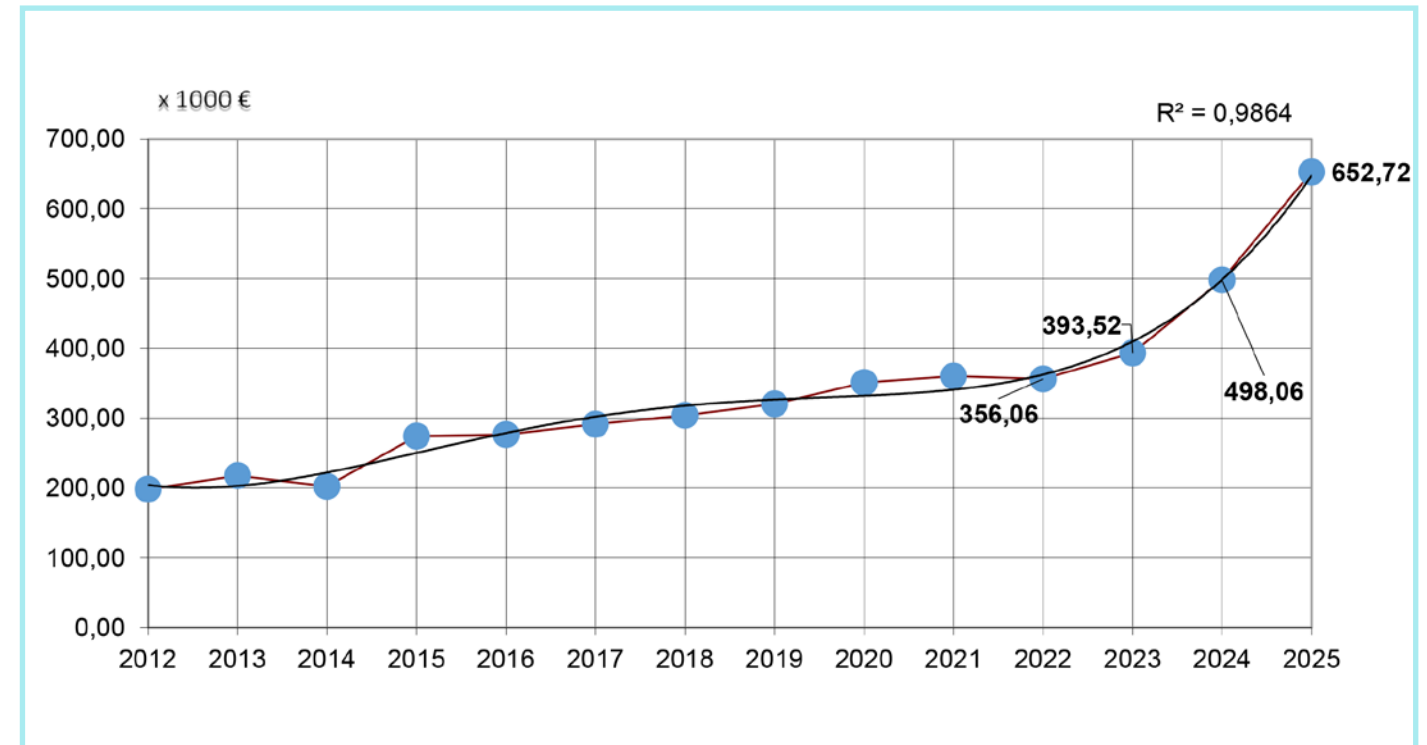


En la **Gráfica 27** se representa, por comunidades autónomas, el gasto, en miles de euros, en contratación de servicios externos para el soporte, mantenimiento y explotación de la plataforma tecnológica, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 652,72 (columna 0).

Gráfica 27: Gasto en contratación de servicios externos para la plataforma tecnológica por 100.000 personas de población protegida

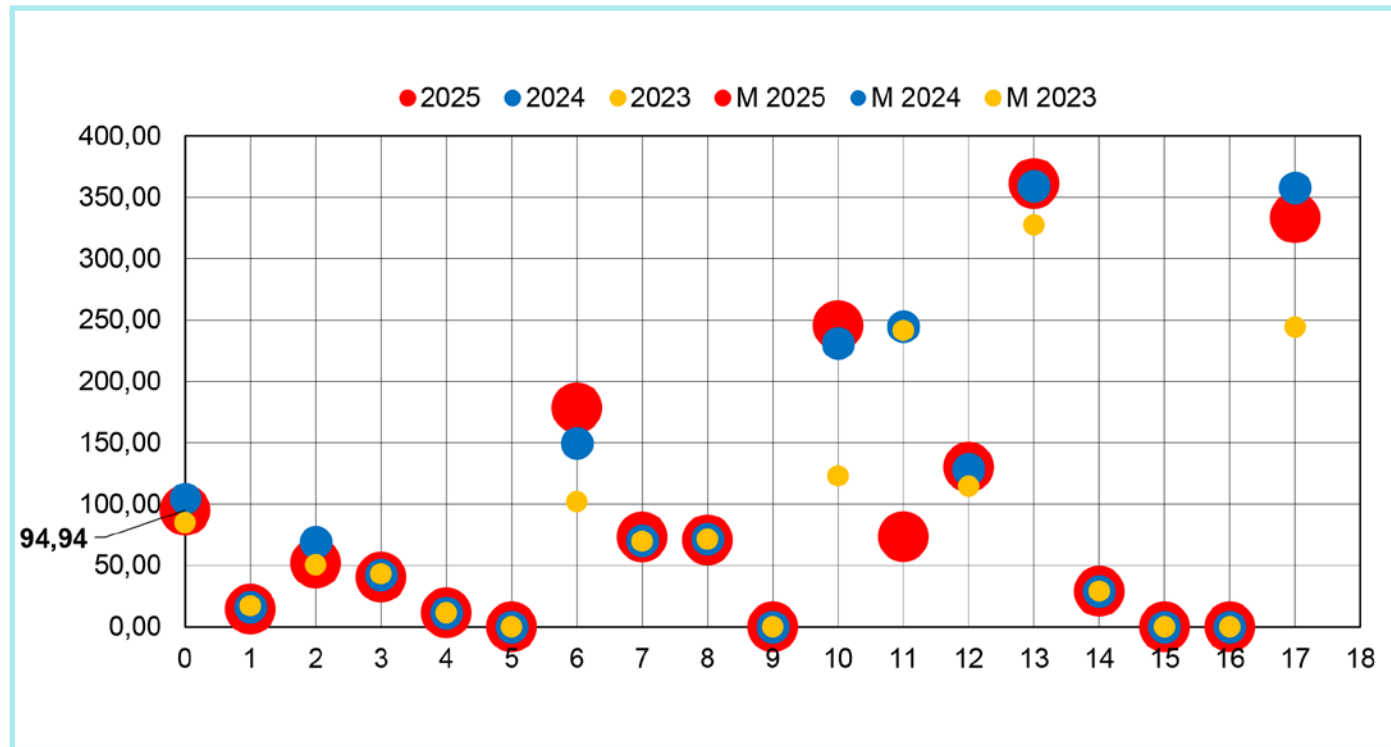


Gráfica 28: Evolución del gasto medio en contratación de servicios externos para la plataforma tecnológica por 100.000 personas de población protegida

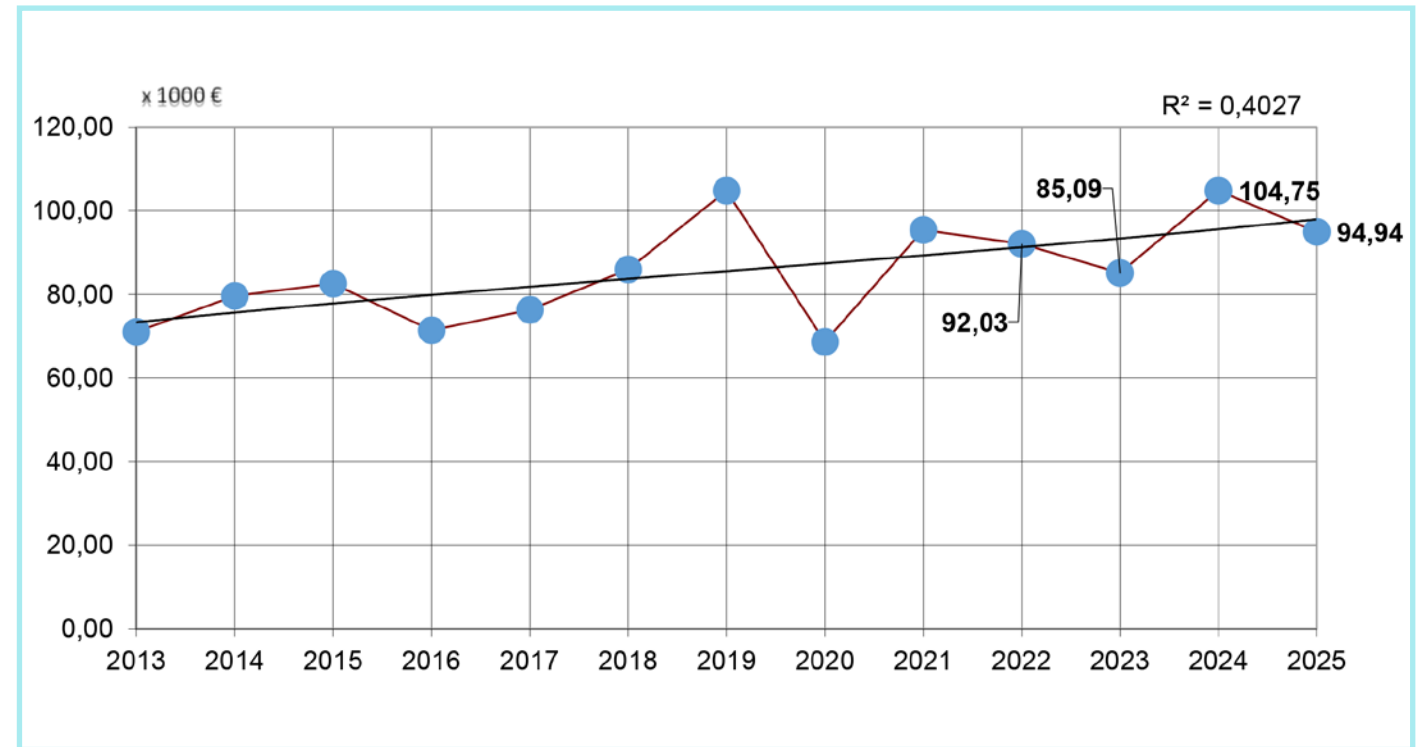


En la **Gráfica 29** se representa, por comunidades autónomas, el gasto en personal propio en plataforma tecnológica, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para 2025 es 94,94 (columna 0).

Gráfica 29: Gasto en personal propio en plataforma tecnológica por 100.000 personas de población protegida



Gráfica 30: Evolución del gasto medio en personal propio en plataforma tecnológica por 100.000 personas de población protegida



En la **Tabla 7** se muestra el desglose, por conceptos y tipo de contrato, del gasto global a escala nacional en plataforma tecnológica en el 2025.

Tabla 7: Desglose del gasto en plataforma tecnológica, por concepto y tipo de contrato

Desglose del gasto en plataforma tecnológica (PT) en 2024 en miles de €	Adquisiciones	Arrendamientos	Mantenimientos	Total
En CPD	35.089	16.117	22.567	73.772
En puestos de trabajo	47.769	26.932	29.020	103.721
En comunicaciones de datos	21.843	16.357	38.504	76.704
En software base de sistemas y comunicaciones	22.730	13.098	42.594	78.421
En sistemas gestores de BD	4.017	1.344	14.615	19.976
En contratación de servicios externos				291.462
En personal propio exclusivamente dedicado a PT				30.131
Otros gastos	4.004	2.991	15.025	22.021
Total	135.452	76.839	162.324	696.209

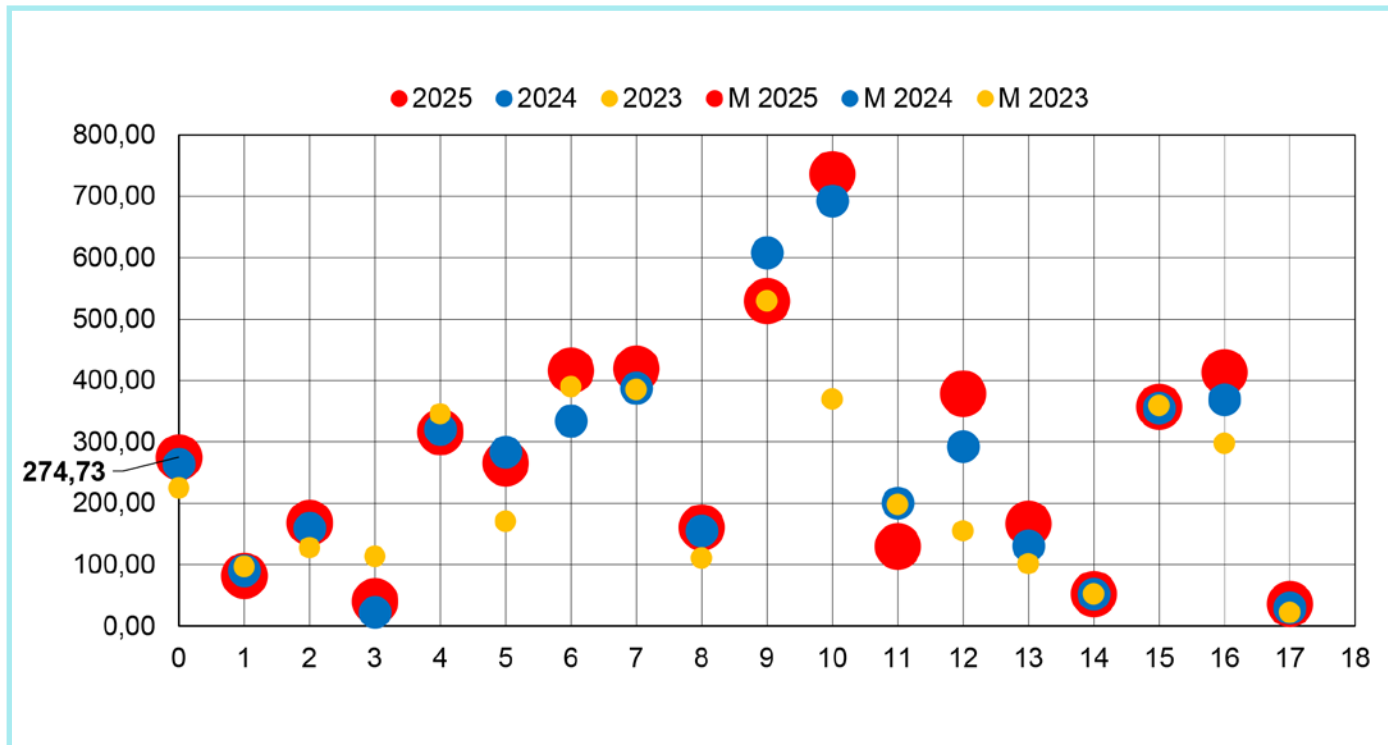
En la **Tabla 8** se indica el desglose del gasto global a nivel nacional, en sistemas de información de los años 2022, 2023, 2024 y 2025. Para el 2025, además del importe, se indica el porcentaje con respecto al presupuesto global TIC de las CCAA.

Tabla 8: Desglose del gasto global en sistemas de información

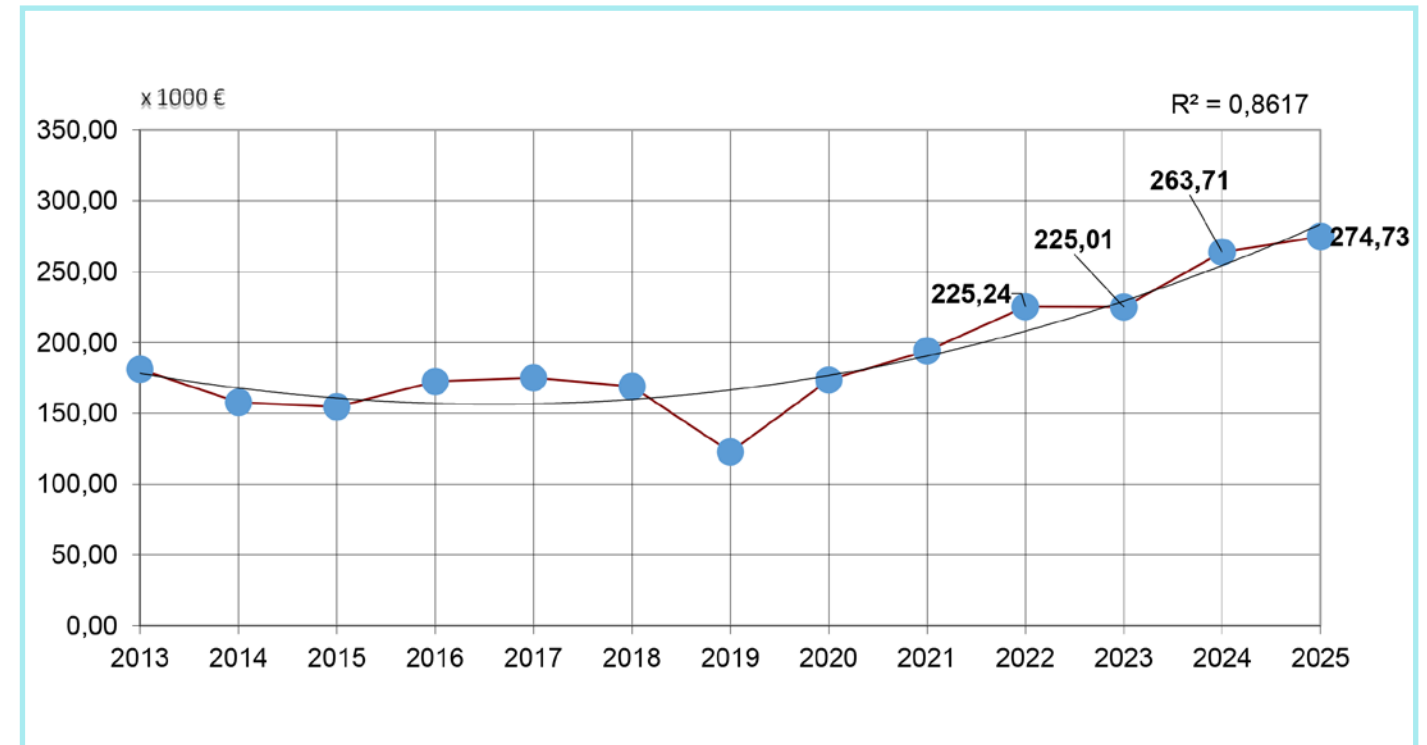
Desglose del gasto global en Sistemas de Información (SI)	2022	2023	2024	2025		% variación 2025/2024
	En miles €	En miles €	En miles €	En miles €	% sobre el Presupuesto TIC	
Gasto en personal propio en SI	91.315	92.080	94.082	97.666	9,50%	3,81%
Gasto en SI horizontales	99.814	99.621	97.788	139.185	13,55%	42,33%
Gasto en SI verticales	186.111	201.801	239.070	273.839	26,65%	14,54%
Otros gastos en SI	41.160	15.016	22.818	17.501	1,70%	-23,30%
Total gastos en SI	418.400	408.518	453.758	528.191	51,40%	16,40%

En la **Gráfica 31** se representa, por comunidades autónomas, el gasto en personal propio en sistemas de información, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para 2025 es 274,73 (columna 0).

Gráfica 31: Gasto en personal propio en sistemas de información por 100.000 personas de población protegida

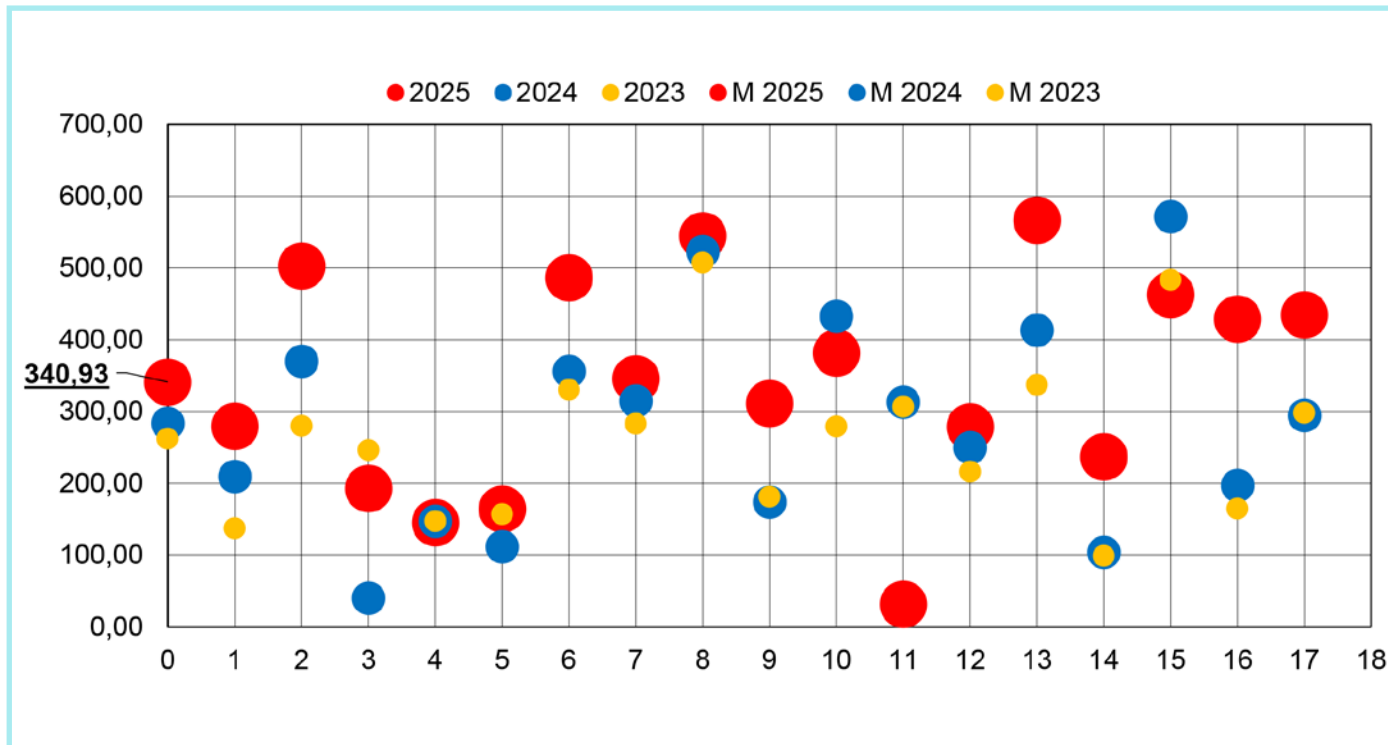


Gráfica 32: Evolución del gasto en personal propio en sistemas de información por 100.000 personas de población protegida

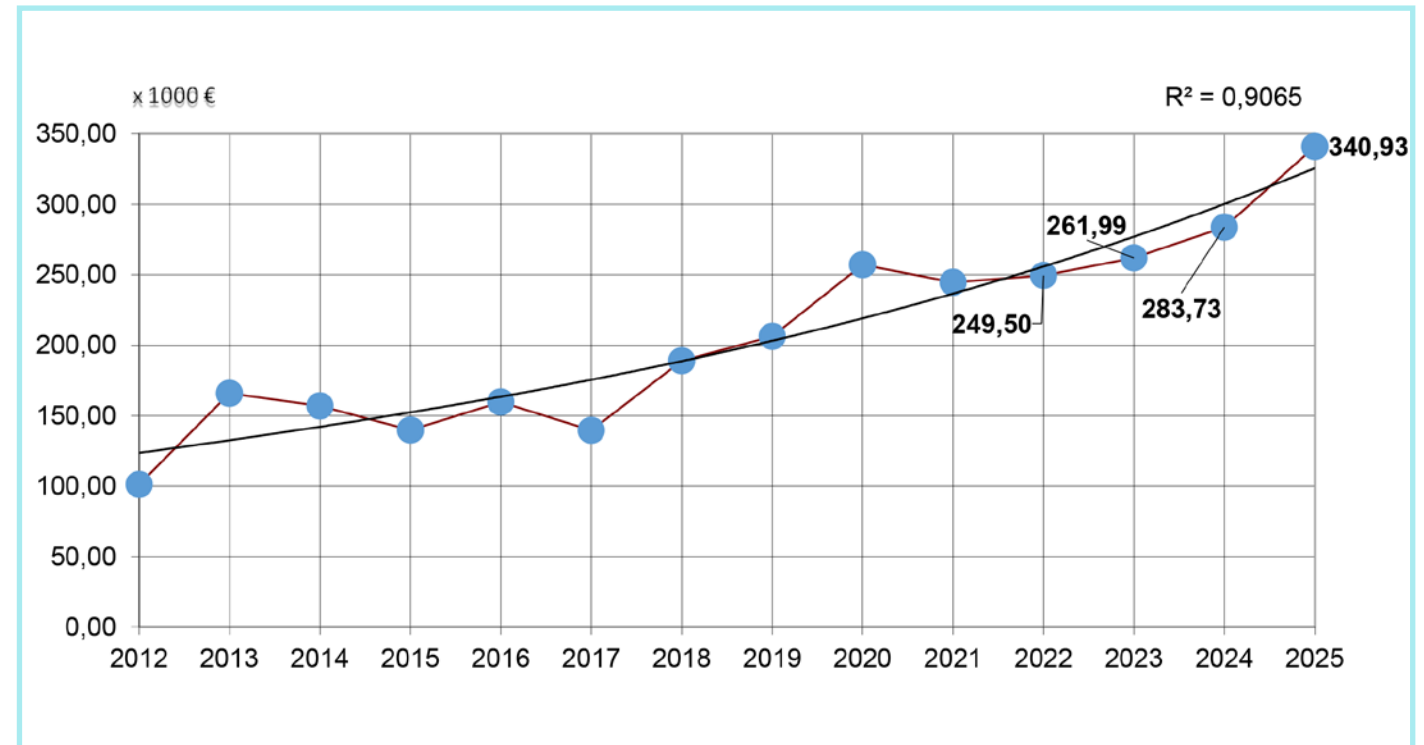


En la **Gráfica 33** se representa, por comunidades autónomas, el gasto en sistemas de información horizontales, en miles de euros, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para 2025 es 340,93 (columna 0)

Gráfica 33: Gasto en sistemas de información horizontales por 100.000 personas de población protegida

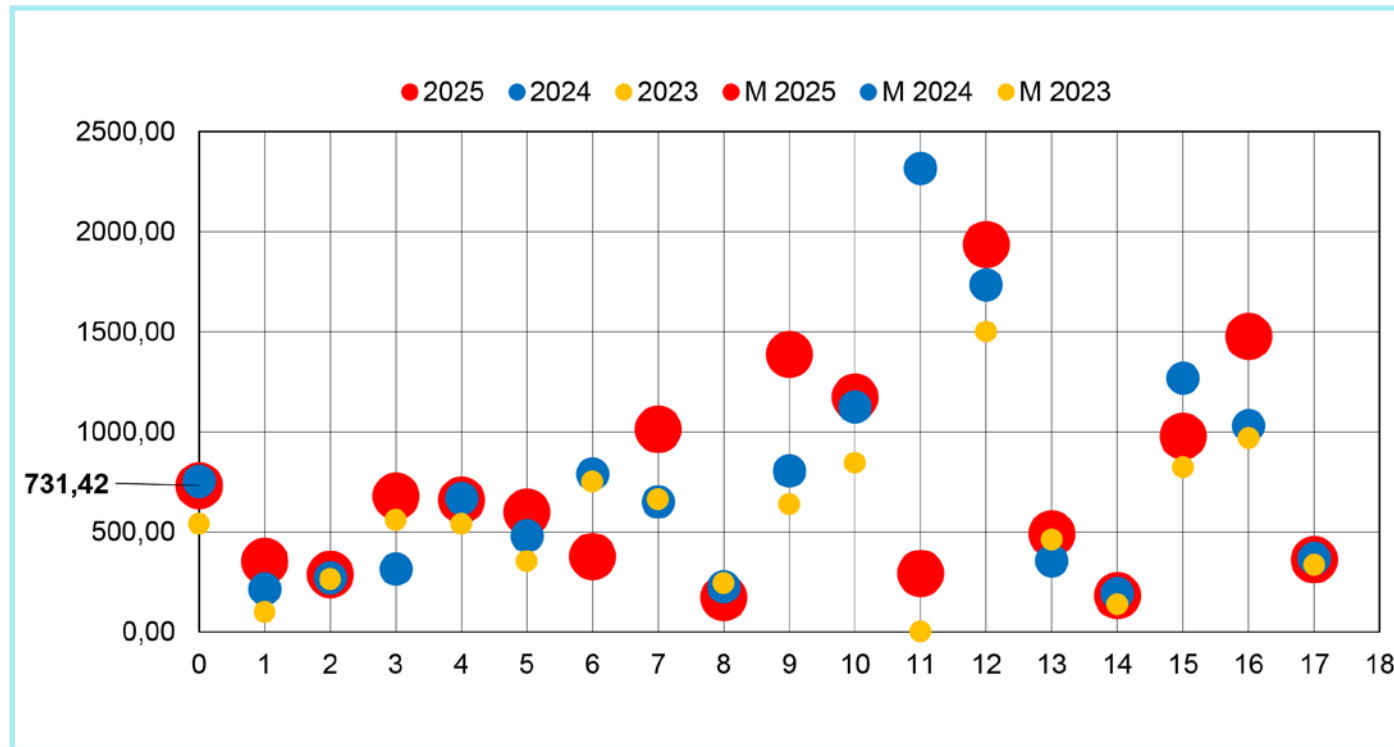


Gráfica 34: Evolución del gasto medio en sistemas de información horizontales por 100.000 personas de población protegida

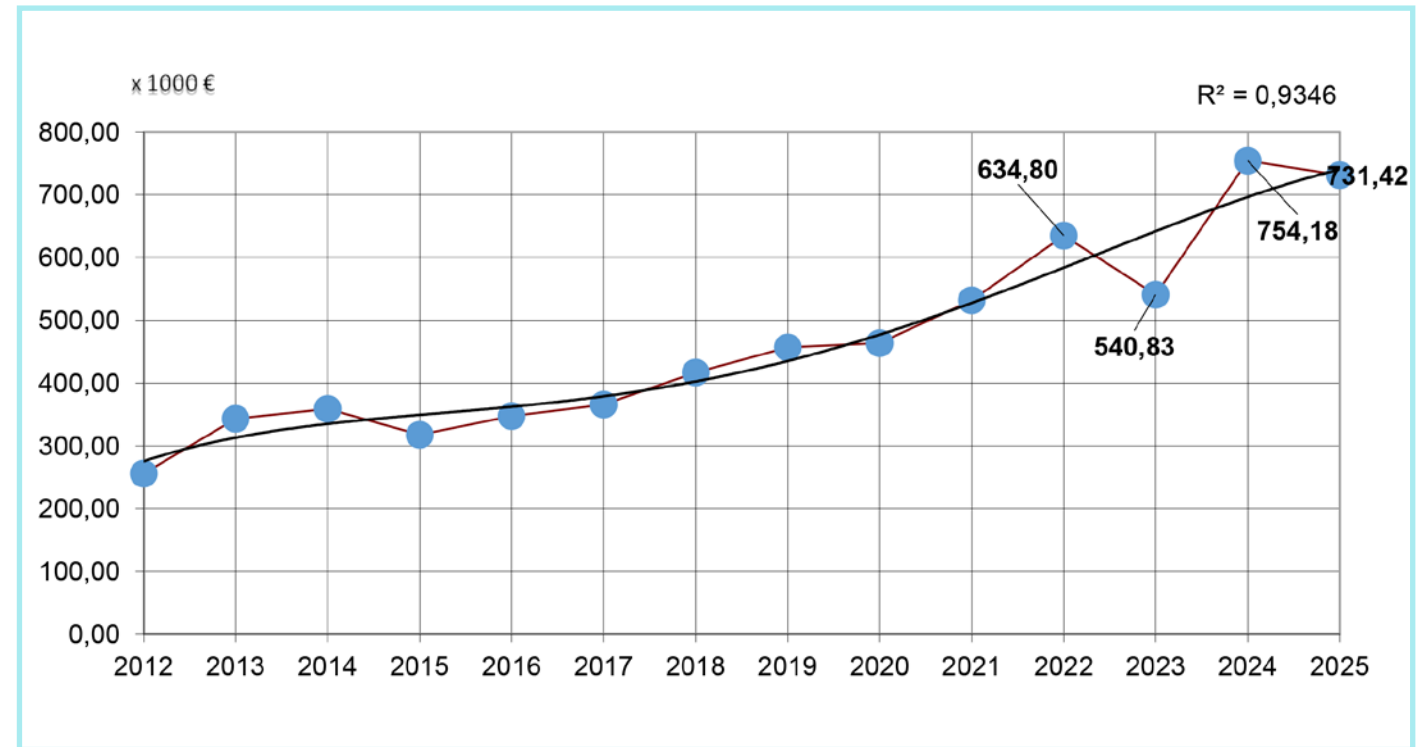


En la **Gráfica 35** se representa, por comunidades autónomas, el gasto, en miles de euros, en sistemas de información verticales, ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para el 2025 es 731,42 (columna 0)

Gráfica 35: Gasto en sistemas de información verticales por 100.000 personas de población protegida



Gráfica 36: Evolución del gasto medio en sistemas de información verticales por 100.000 personas de población protegida



Historia Electrónica de Salud (HES)

Se considera que una comunidad autónoma dispone de una Historia Electrónica de Salud (HES) de sus ciudadanos cuando en el Servicio de Salud existe un sistema que permite acceder a los procesos de los pacientes de forma agregada y longitudinal con independencia del centro sanitario o ámbito asistencial dentro de la red sanitaria de utilización pública de la Comunidad Autónoma. Desde el 2018 las 17 CCAA disponen de sistemas que soportan una HES única para cada ciudadano y desde el 2022 todas las CCAA soportan el acceso de los ciudadanos a su HES a través de Internet.

En la **Tabla 9** se indican el número de CCAA, y el porcentaje que representan respecto a las 17, en las que sus ciudadanos pueden acceder a su HES a través de una app específica para dispositivos móviles, en las que sus ciudadanos pueden incorporar datos a su HES a través de Internet. así como el número de ciudadanos que han actualizado datos en sus HES a través de Internet y el porcentaje que representan con respecto a la población protegida de las CCAA que tienen esa posibilidad.

Tabla 9: Historia Electrónica de Salud (HES)

Historia Electrónica de Salud (HES)	2022	2023	2024	2025		% vari. 2025-2024
				Valor	% sobre el total	
CC.AA. en las que los ciudadanos pueden acceder a sus HES a través de una app específica para dispositivos móviles	15	16	16	17	100,00%	6,25%
CC.AA. en las que los ciudadanos pueden incorporar datos a sus HES a través de Internet	7	7	7	6	35,29%	-14,29%
Nº de ciudadanos que han actualizado datos de sus HES a través de Internet (*)	1.198.313	980.421	2.438.929	1.324.466	5,81%	-45,69%

(*) El 5,81% se refiere al nº de ciudadanos que actualizaron datos con respecto a la PP de las 6 CCAA que tienen esa posibilidad.

Servicios sanitarios para el ciudadano basados en TIC

Para conocer los servicios que basados en TIC dan las CCAA a los ciudadanos, en el cuestionario de captura de datos para el ÍNDICE 2025 se incluyeron los indicadores que se indican en la **Tabla 10** con el resumen de las contestaciones.

Tabla 10: Servicios sanitarios para el ciudadano basados en TIC

Servicios sanitarios para el ciudadano basados en TIC	2025
CCAA en las que los ciudadanos pueden consultar, a través de Internet, su carpeta de salud	17
CCAA en las que los ciudadanos pueden consultar, a través de Internet, las citas de AP y AE (AH)	17
CCAA en las que los ciudadanos pueden gestionar, a través de Internet, las citas de AP	17
CCAA en las que los ciudadanos pueden gestionar, a través de Internet, las citas de AE (AH)	8
CCAA en las que los ciudadanos pueden gestionar, a través de Internet, algunos datos de su TSI	12

Además, en el cuestionario de captura de datos se pedía que indicasen, de forma abierta, que otros servicios basados en TIC ofrecía la CA a sus ciudadanos, para incluirlos en el cuestionario de la próxima edición, recibándose las siguientes contestaciones:

- 3 CCAA en las que existe acceso a la videoconsulta de AP
- 3 CCAA en las que existe acceso al tratamiento anticoagulación
- 2 CCAA en las que existe la TSI Virtual
- 2 CCAA en las que existe acceso a las donaciones de sangre
- 2 CCAA en las que se puede solicitar el justificante de asistencia a consulta de AP
- 1 CCAA en la que existe acceso a la lista de espera quirúrgica
- 1 CCAA en la que se pueden consultar las subvenciones tratamientos farmacológicos
- 1 CCAA en la que existe acceso a las donaciones de órganos
- 1 CCAA en la que se pueden consultar las campañas de vacunación
- 1 CCAA en la que se puede consultar el registro de instrucciones previas
- 1 CCAA en la que se puede solicitar la renovación de recetas
- 1 CCAA en la que el paciente puede enviar documentación al profesional de AP y AE (AH)
- 1 CCAA en la que se puede consultar la aportación farmacéutica
- 1 CCAA en la que se permite la representación digital

Hay que señalar que, al ser preguntas abiertas, las CCAA que han indicado que tienen esos servicios sean las únicas que los tienen.

Sistemas para citaciones a consultas

En la **Tabla 11** se indican el número de citaciones, en miles, para consultas de Atención Primaria y el número de comunicaciones o confirmaciones de citas para Atención Especializada, efectuadas en 2025, desglosadas según el canal utilizado para su solicitud.

En la **Tabla 12** se indica la variación de estos datos con respecto a los de 2024 en porcentajes.

Tabla 11: Citaciones/comunicaciones para consulta según canal

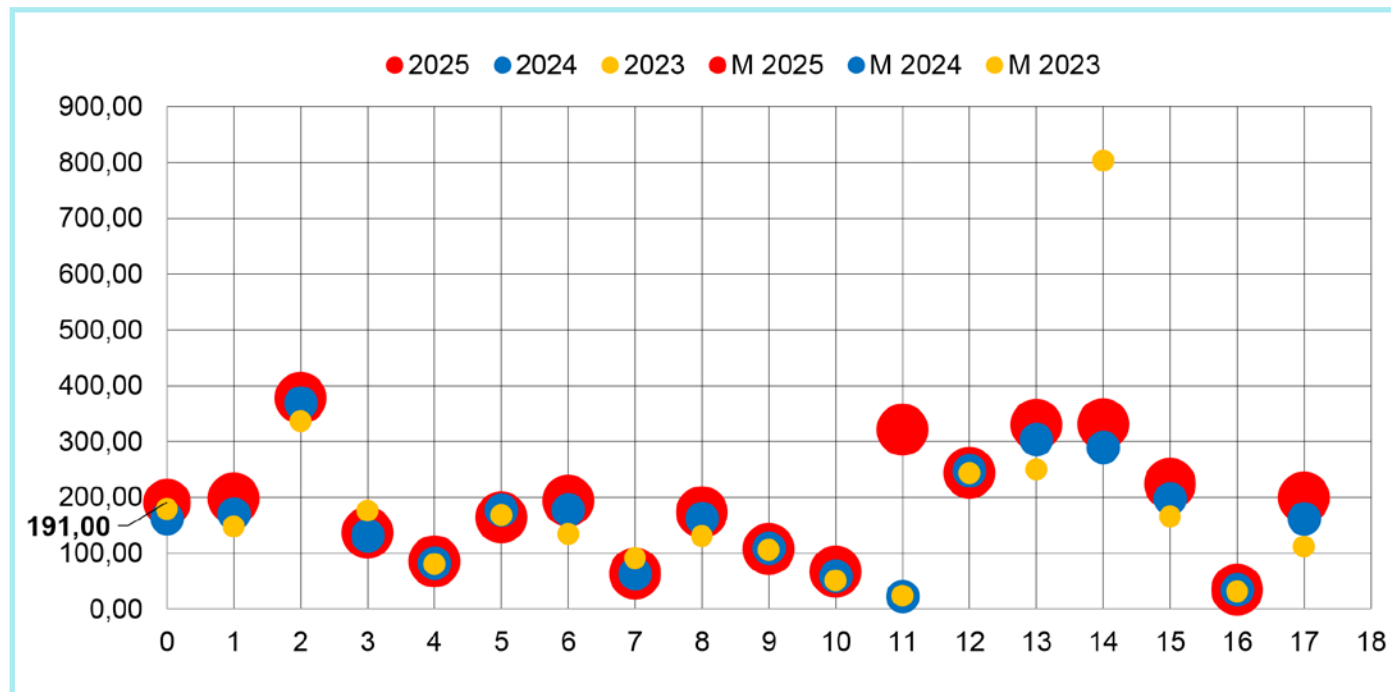
Citaciones y comunicaciones en 2024, en miles	Por Internet	Por teléfono	Por otros medios	Total
Citaciones para AP	95.917	113.528	210.289	419.734
Comunicaciones y confirmación de citaciones para AE (o AH)	15.643	18.166	65.369	99.179
Total	111.560	131.694	275.659	518.913

Tabla 12: Citaciones/comunicaciones para consulta según canal. % de variación con respecto al año anterior

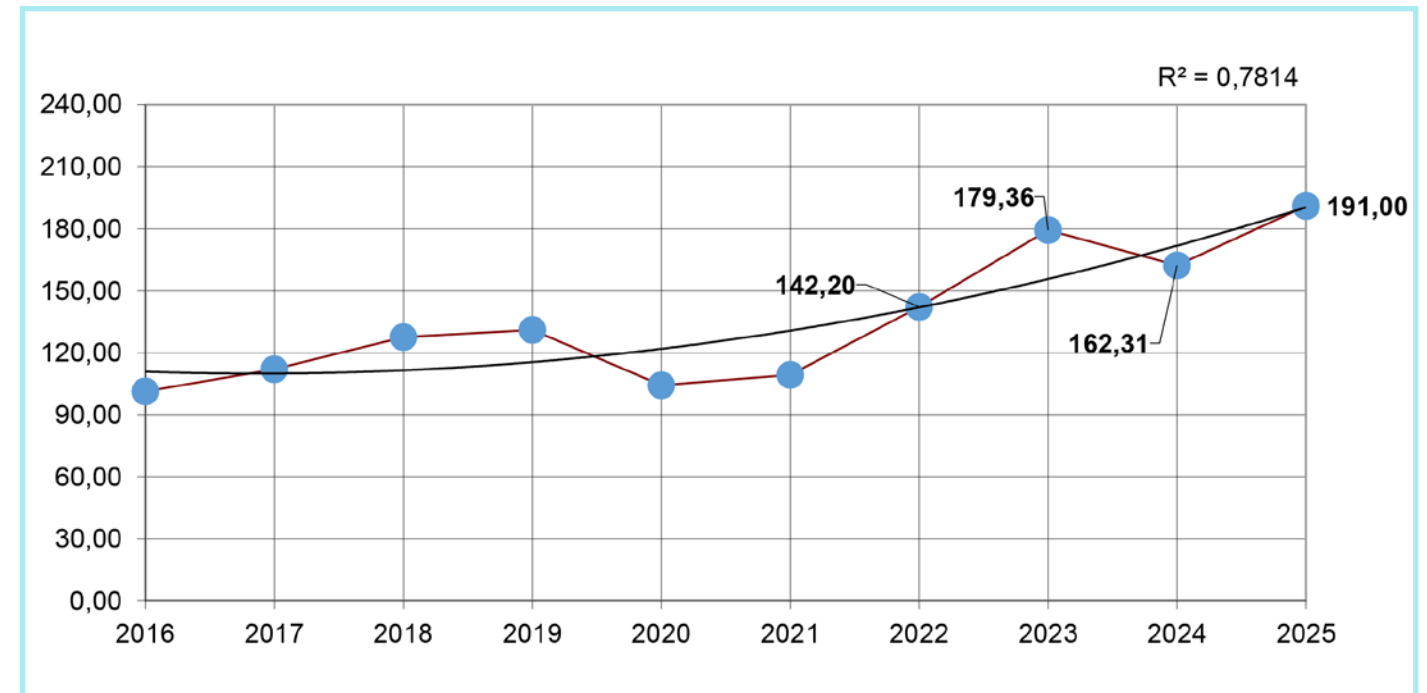
Citaciones y comunicaciones. % variación 2025/2024	Por Internet	Por teléfono	Por otros medios	Total
Citaciones para AP	11,86%	0,47%	9,21%	7,27%
Comunicaciones y confirmación de citaciones para AE (o AH)	372,95%	-2,75%	9,19%	21,16%
Total	25,27%	0,01%	9,21%	9,67%

En las **gráficas 37, 39 y 41** se representan, por comunidades autónomas, el número, en miles, ponderado por cada 100.000 personas de población protegida, de citaciones en Atención Primaria: por internet, por teléfono y por otros medios, en 2023, 2024 y 2025. En cada gráfica también se indica la media de los valores representados en el 2025. En las **gráficas 38, 40 y 42** se representan la evolución de esos valores medios desde el 2016.

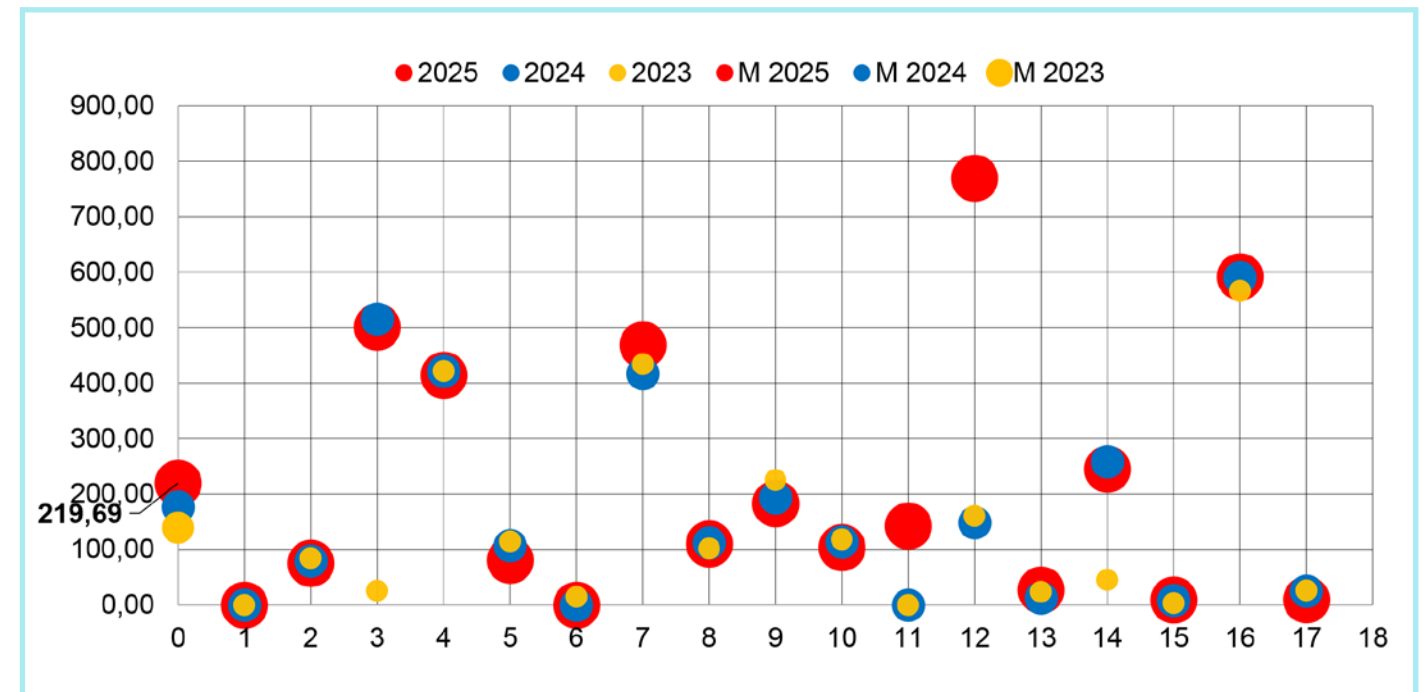
Gráfica 37: Número de citaciones en AP por internet por cada 100.000 personas de población protegida



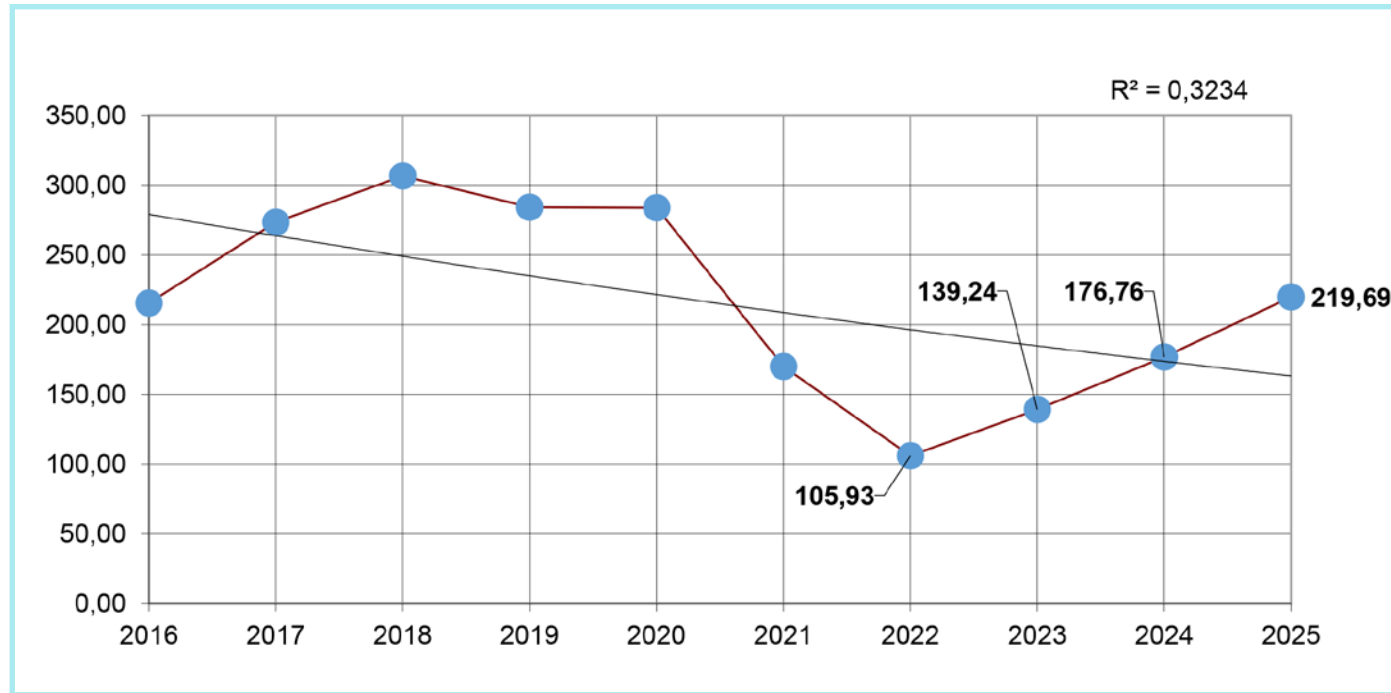
Gráfica 38: Evolución de los valores medios del número de citaciones en AP por internet por cada 100.000 personas de población protegida



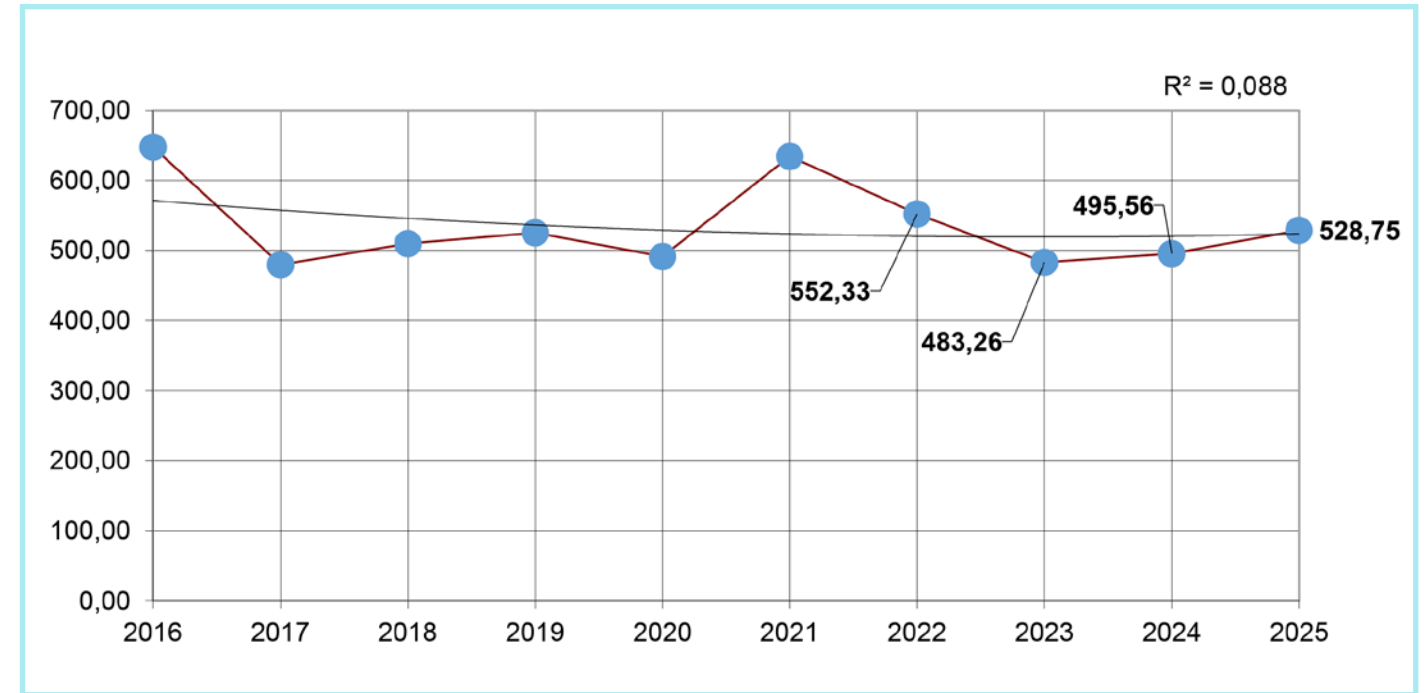
Gráfica 39: Número de citaciones en AP por teléfono por cada 100.000 personas de población protegida



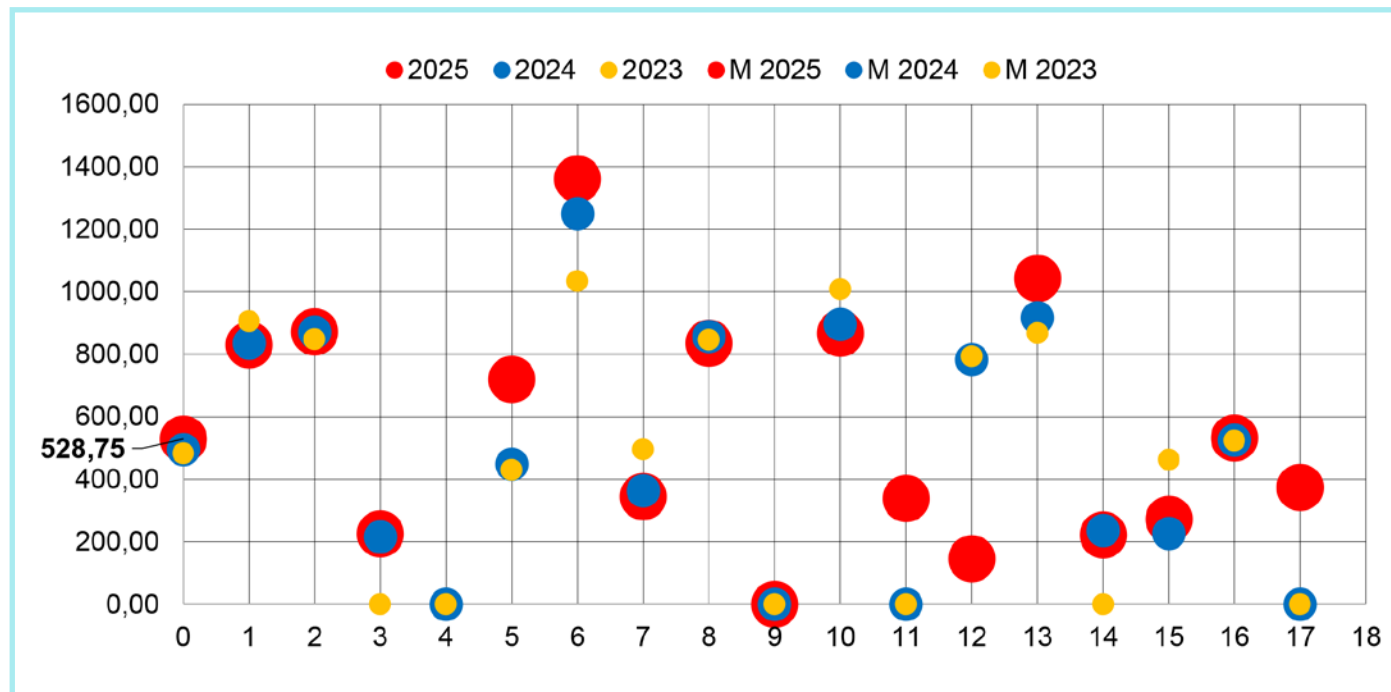
Gráfica 40: Evolución de los valores medios del número de citaciones en AP por teléfono por cada 100.000 personas de población protegida



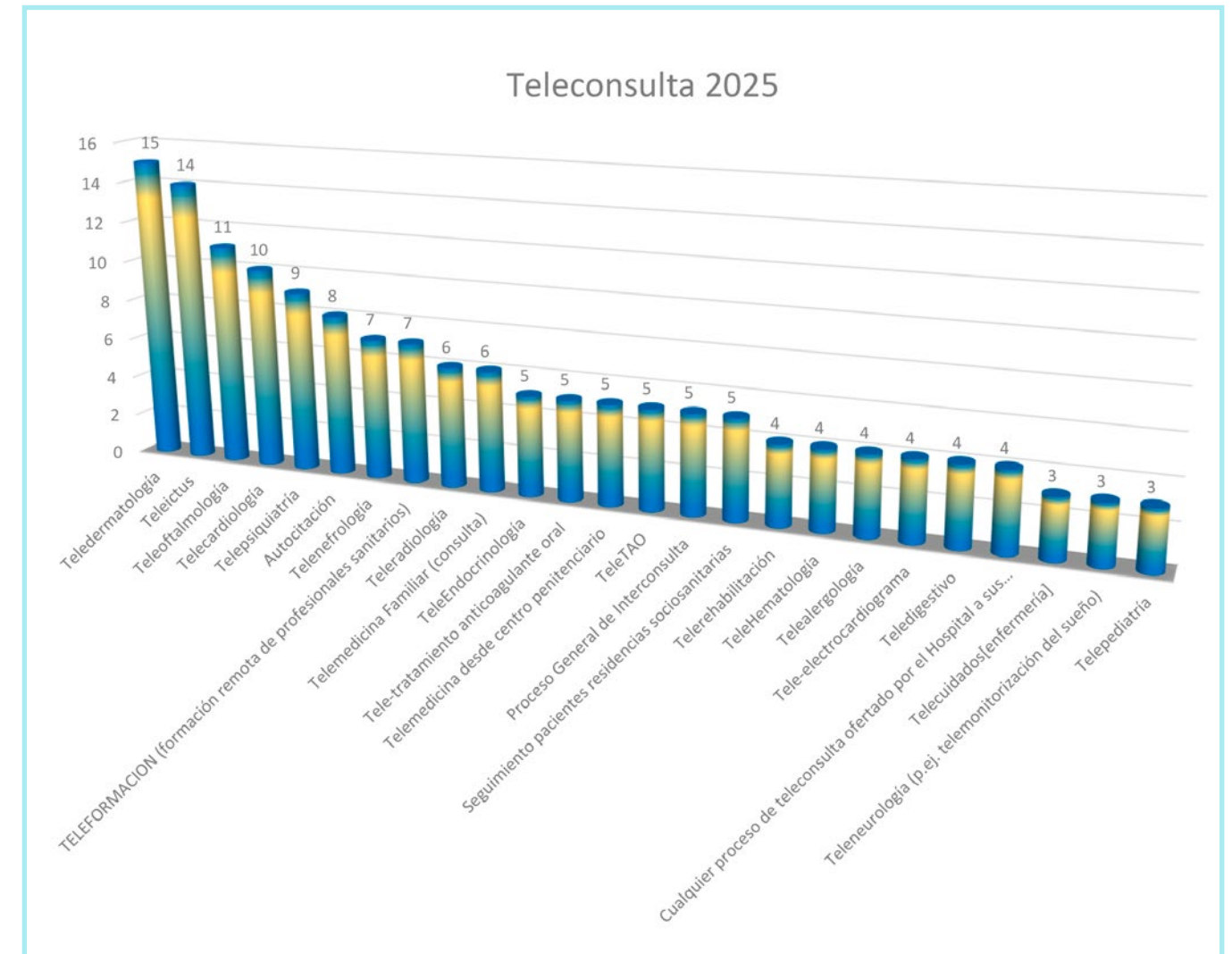
Gráfica 42: Evolución de los valores medios del número de citaciones en AP por otros medios, por cada 100.000 personas de población protegida



Gráfica 41: Número de citaciones en AP por otros medios, por cada 100.000 personas de población protegida



Gráfica 43: Especialidades de Telemedicina



Telemedicina

En la Gráfica 43 se muestran las especialidades de telemedicina con el número de CCAA (frecuencias) que, en el 2025, tienen iniciativas en cada especialidad, sólo se indican las especialidades que tienen más de 3 frecuencias.

Se puede observar que las especialidades que más frecuencias tienen son: Tele dermatología en 15 CCAA, Teleictus en 14 y Teleoftalmología en 11.

En la Tabla 13 se indica el número de teleconsultas realizadas en Atención Primaria y Atención Especializada de las CCAA que contestaron a estas preguntas.

Tabla 13: Teleconsultas realizadas

Teleconsultas	2022		2023		2024		2025	
	Nº de CCAA que contestaron	Número total de teleconsultas	Nº de CCAA que contestaron	Número total de teleconsultas	Nº de CCAA que contestaron	Número total de teleconsultas	Nº de CCAA que contestaron	Número total de teleconsultas
En Atención Primaria	12	15.684.791	15	33.537.910	14	42.812.767	15	46.640.762
En Atención Especializada	12	3.277.273	16	5.728.068	15	9.461.419	16	10.063.300

Unidades TIC y de seguridad de los sistemas de información

Con el objetivo de conocer la situación en que se encuentran las unidades TIC dentro de la estructura organizativa de cada Servicio de Salud, el cuestionario de captura de datos incluye varios indicadores (preguntas) relacionados con la organización y recursos disponibles de las unidades TIC y de las unidades de seguridad de los sistemas de información.

En la **Tabla 14** se muestra el número de recursos humanos, a escala nacional, dedicados en exclusiva a las TIC en los años 2022, 2023, 2024 y 2025.

En la **Tabla 15** se muestran, a nivel nacional, el número de recursos humanos propios (funcionarios/estatutarios y laborales), dedicados en exclusiva a las TIC en el 2025, distribuidos según la categoría (nivel) que corresponda al puesto de trabajo que desempeñan.

En la **Tabla 16** se muestra la variación, en porcentajes, de los recursos humanos propios (funcionarios/estatutarios y laborales) dedicados en exclusiva a las TIC del 2025 con respecto al 2024.

Tabla 14: Recursos humanos dedicados en exclusiva a las TIC

Recursos humanos dedicados en exclusiva a las TIC	2022	2023	2024	2025	% varia. 2025-2024
Personal propio	3.308	3.261	3.724	3.821	2,61%
Personal externo	2.798	3.370	4.073	4.373	7,37%
Personal total	6.106	6.631	7.797	8.194	5,10%

Tabla 15: Distribución de los RRHH propios dedicados en exclusiva a las TIC

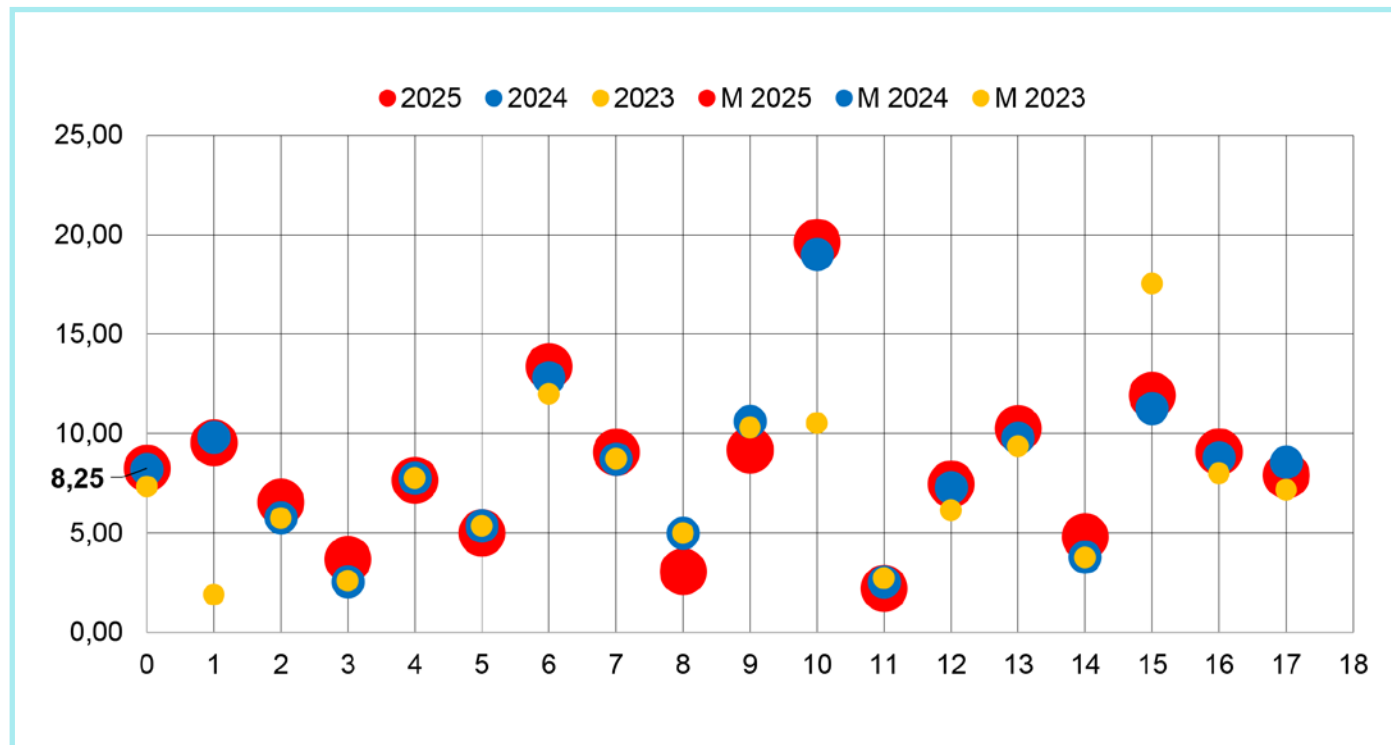
Recursos humanos propios según nivel del puesto de trabajo	Nivel A1	Nivel A2	Nivel B	Nivel C1	Nivel C2	Total
Funcionarios o estatutarios	1.040	931	156	1267	168	3.562
Personal laboral	88	50	40	76	5	259
Total	1.128	981	196	1.343	173	3.821

Tabla 16: Variación con respecto al año anterior, en porcentajes, de los RRHH propios dedicados en exclusiva a las TIC

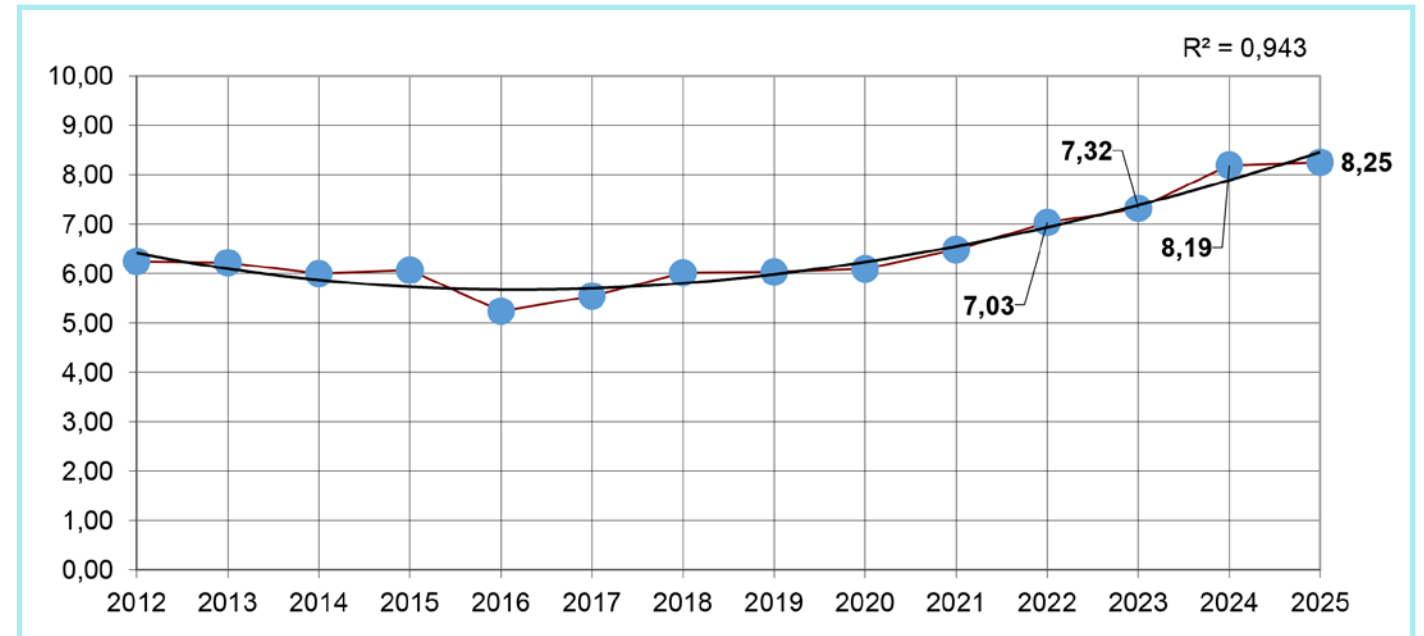
Recursos humanos propios según nivel del puesto de trabajo	Nivel A1	Nivel A2	Nivel B	Nivel C1	Nivel C2	Total
% de variación 2025-2024 funcionarios o estatutarios	14,02%	3,70%	-4,88%	3,01%	-8,10%	5,18%
% de variación 2025-2024 Personal laboral	-38,03%	-16,67%	-20,00%	-1,30%	-37,50%	-23,15%
% de variación 2025-2024 del total de personal propio	7,01%	2,42%	-8,41%	2,75%	-9,33%	2,61%

En las **Gráficas 44, 46 y 48** se representan, por comunidades autónomas, los recursos humanos dedicados exclusivamente a las TIC, ponderados por 100.000 personas de población protegida, así como las medias de los valores representados y su valor para el 2025, correspondientes a: funcionarios y/o estatutarios, laborales y personal externo; y en las **Gráficas 45, 47 y 49** se representan la evolución de los respectivos valores de las medias.

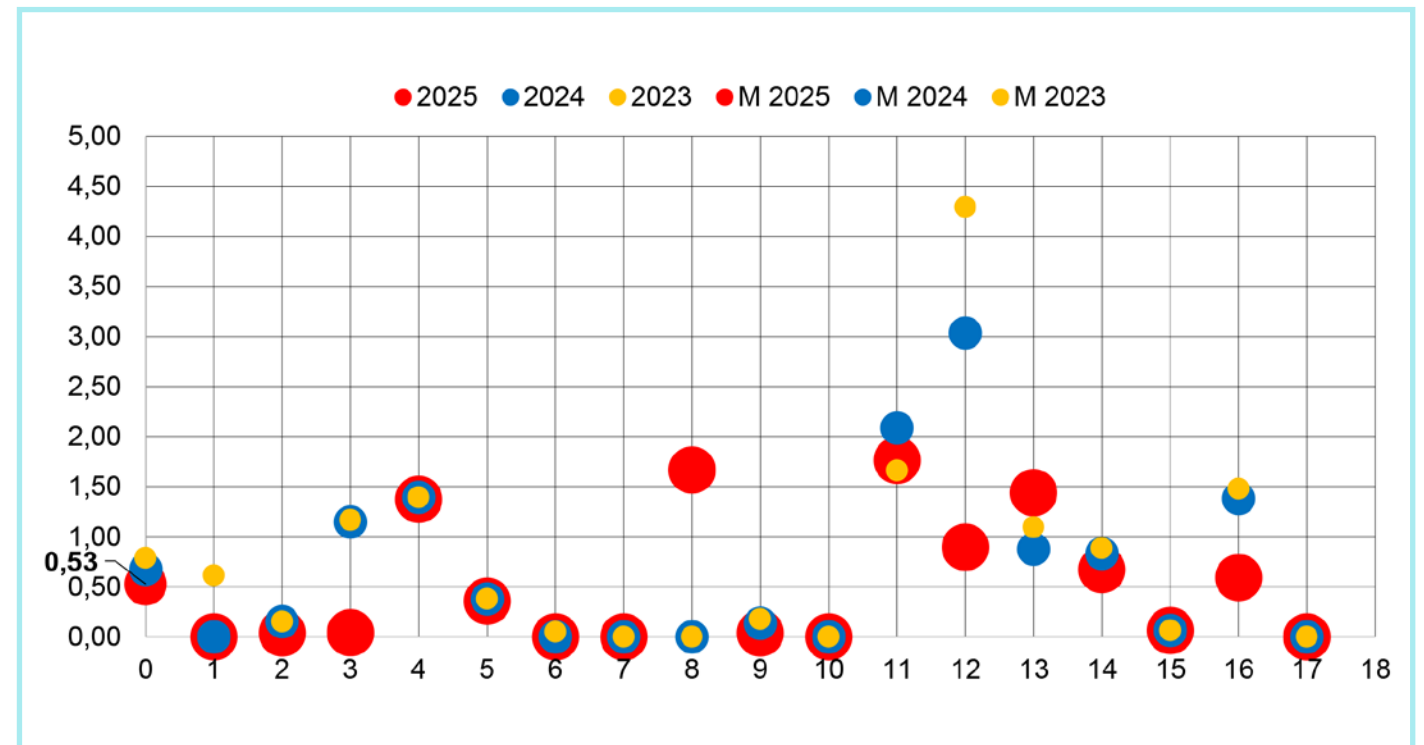
Gráfica 44: Número de funcionarios y/o estatutarios por 100.000 personas de población protegida



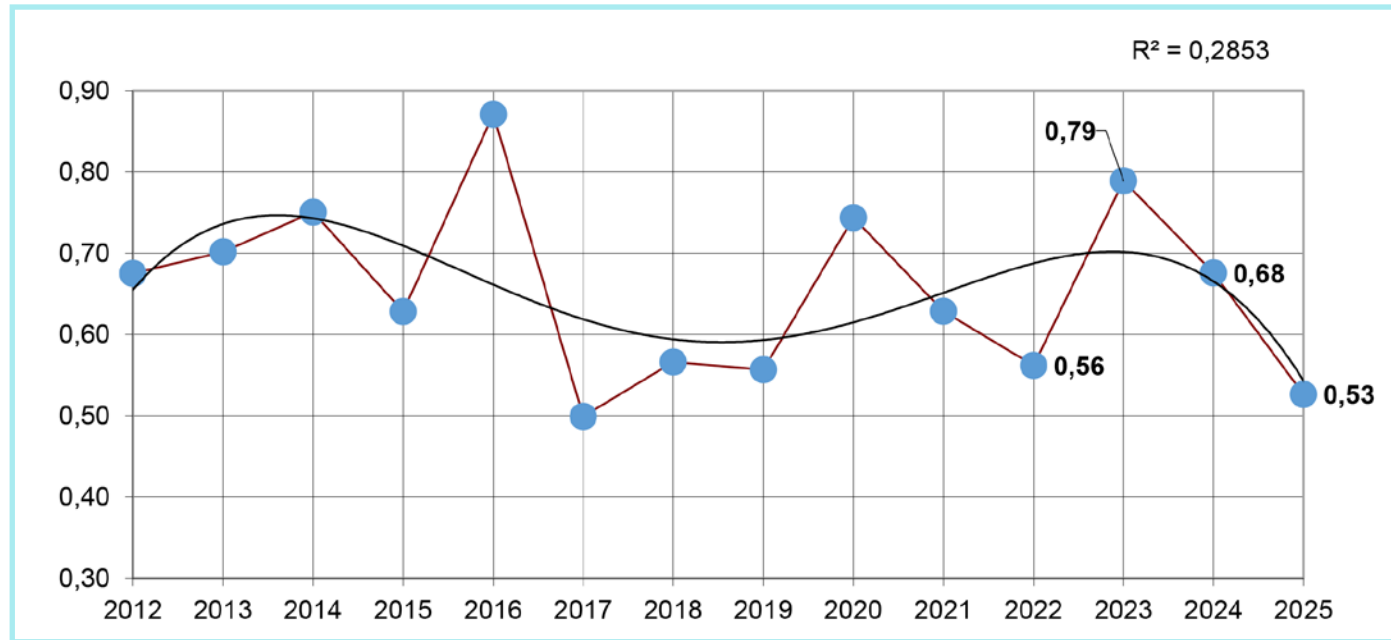
Gráfica 45: Evolución de los valores medios del número de funcionarios y/o estatutarios por 100.000 personas de población protegida



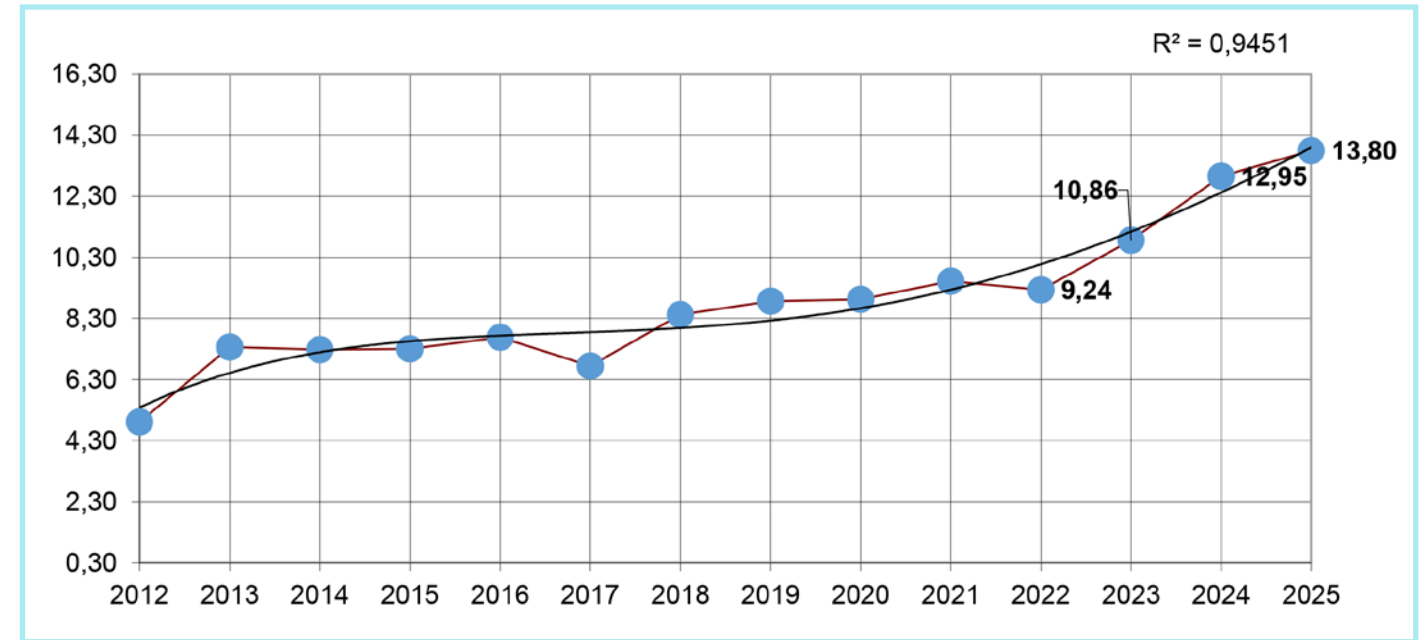
Gráfica 46: Número de personal laboral por 100.000 personas de población protegida



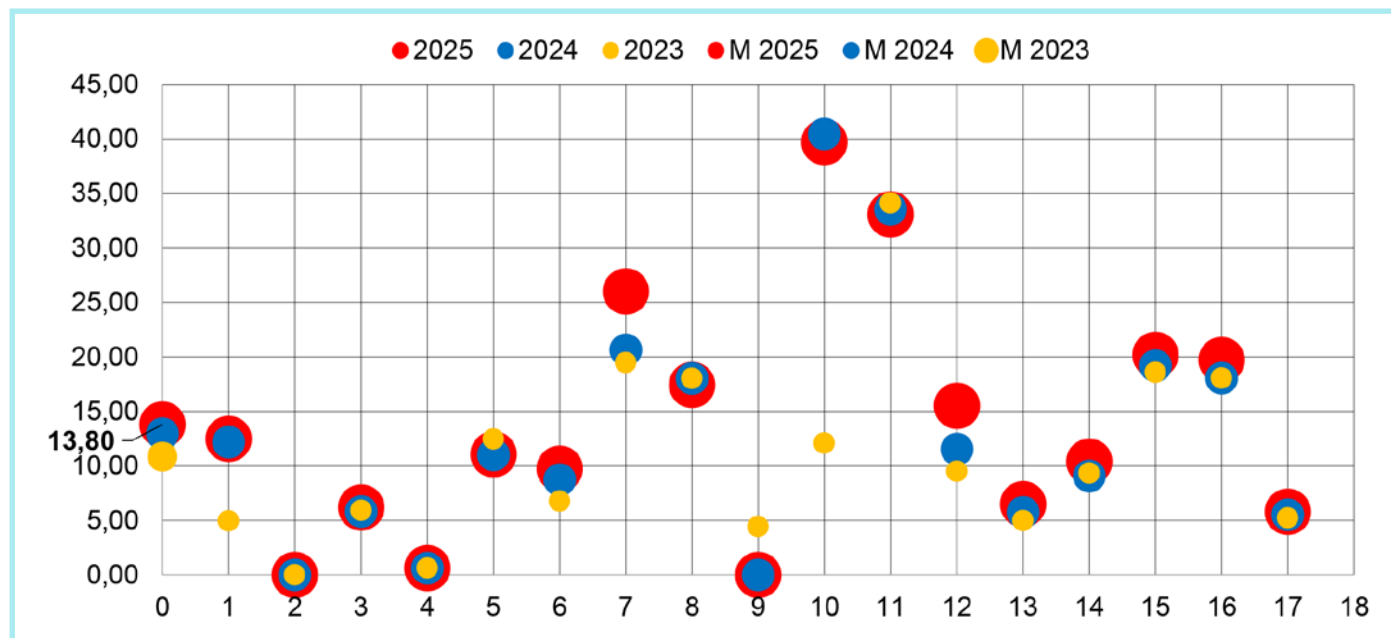
Gráfica 47: Evolución de los valores medios del número de personal laboral por 100.000 personas de población protegida



Gráfica 49: Evolución de los valores medios del número de personal externo por 100.000 personas de población protegida

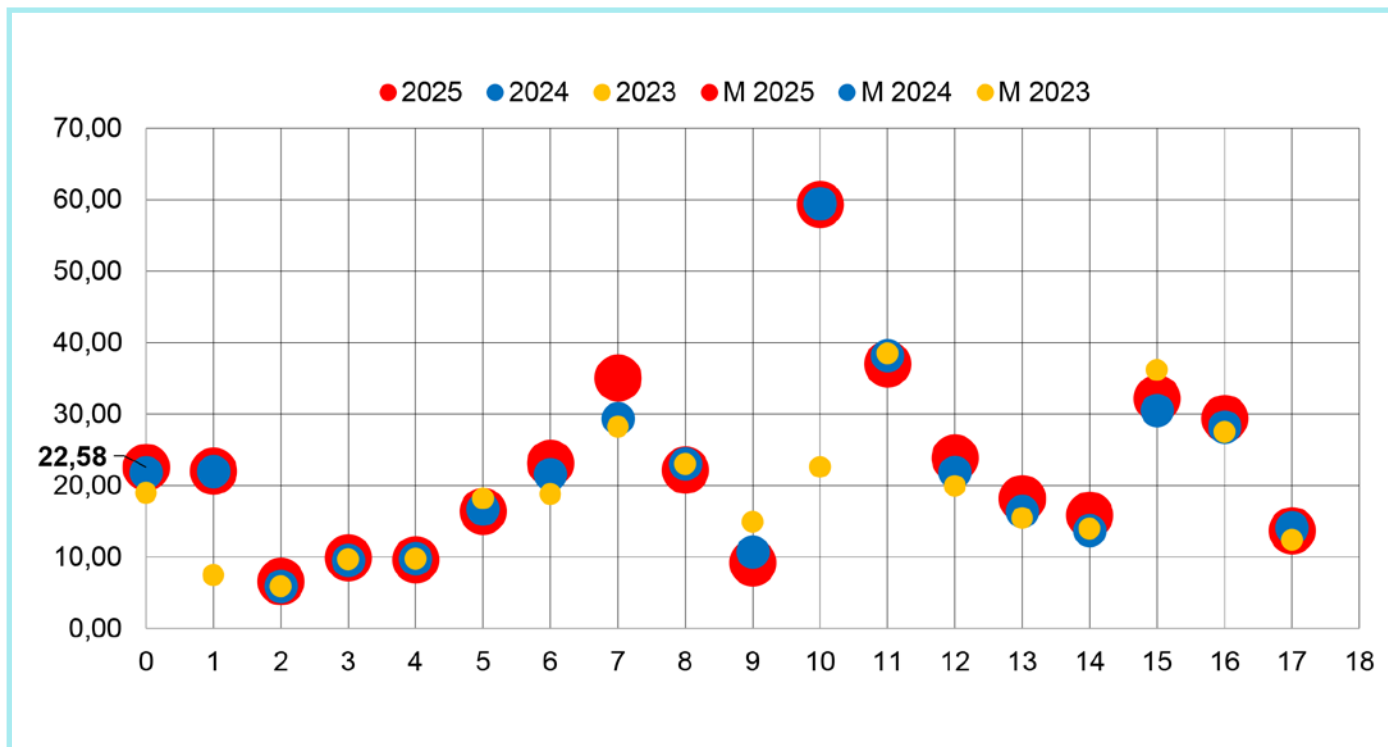


Gráfica 48: Número de personal externo por 100.000 personas de población protegida

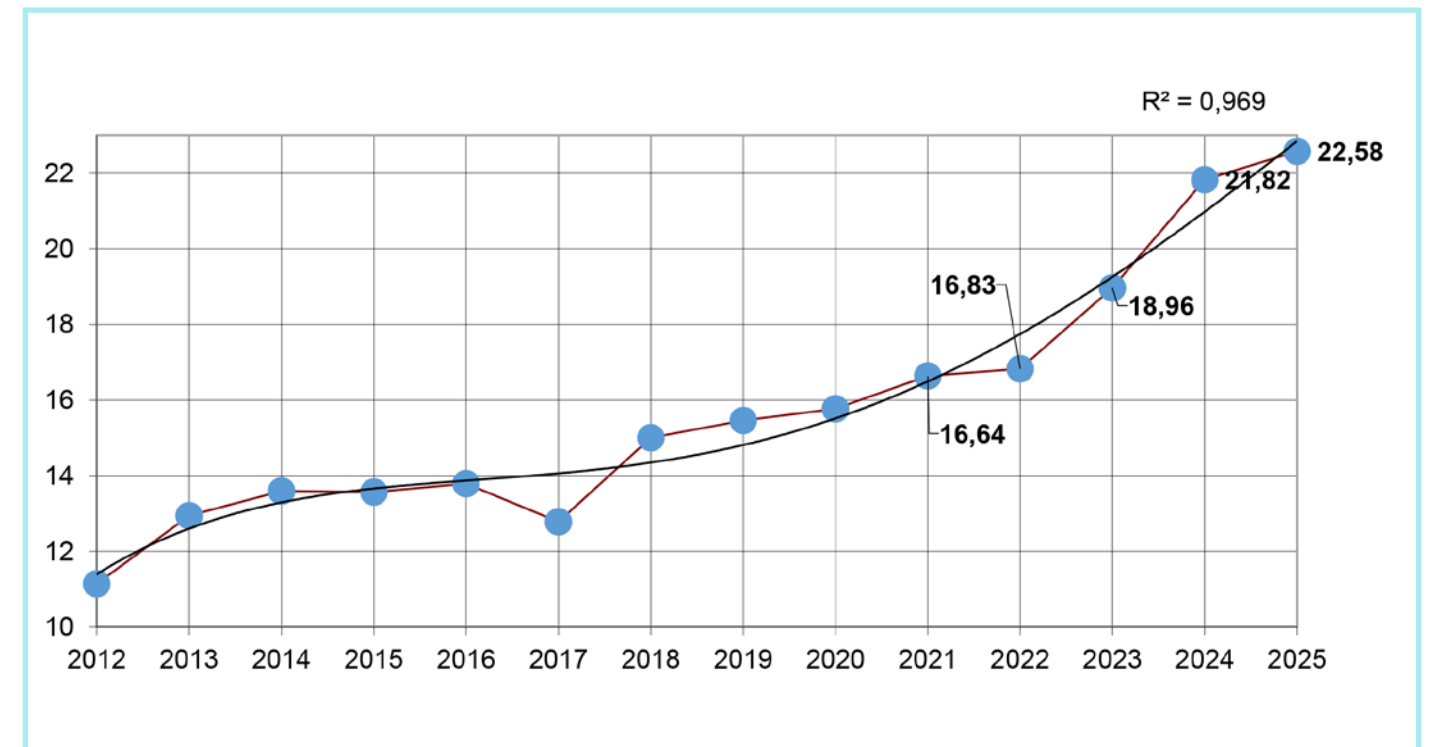


En la **Gráfica 50** se representa por comunidades autónomas, el número total de recursos humanos dedicados exclusivamente a las TIC ponderado por 100.000 personas de población protegida. La media de los valores representados en la gráfica para 2025 es 22,58 (columna 0).

Gráfica 50: Número total de recursos humanos TIC por 100.000 personas de población protegida



Gráfica 51: Evolución de los valores medios del número total de recursos humanos TIC por 100.000 personas de población protegida



En la **Tabla 17** se indican para los años 2022, 2023, 2024 y 2025, el número de CCAA en las que la unidad superior de la que depende la unidad responsable de las TIC de la Consejería de Sanidad o del Servicio de Salud tienen un determinado nivel orgánico o administrativo. El indicador correspondiente no se pidió en el cuestionario del ÍNDICE 2023 pero se ha vuelto a incorporar a partir del ÍNDICE 2024 por considerar útil la información que aportaba.

Tabla 17: Unidad superior de la que depende la unidad TIC de la Consejería de Sanidad o del Servicio de Salud (SS)

Nivel orgánico/pertenencia de la unidad superior de la que depende la unidad TIC	2022	2023(*)	2024	2025
Consejería de Sanidad	1	-	-	-
Viceconsejería de Sanidad	1	-	-	-
Gerencia del SS, Secretaría General o Autónoma de la Consejería o del SS	8	-	9	11
Dirección General de la Consejería de Sanidad o del SS	7	-	3	2
Dirección General de otra Consejería distinta a la de Sanidad	-	-	3	3
Consejería distinta a la de Sanidad	-	-	2	-
Subdirección. General de la Consejería de Sanidad o del SS	-	-	-	1

(*) para el ÍNDICE 2023 no se solicitó este dato

En la **Tabla 18** se indican, para los años 2022, 2023, 2024 y 2025, el número de CCAA en las que la unidad responsable de las TIC de la Consejería de Sanidad o del Servicio de Salud tienen un determinado nivel orgánico o administrativo.

A la pregunta: “¿El responsable (o los responsables) de la unidad TIC forman parte del Comité de Dirección del Servicio de Salud?”, contestaron afirmativamente: 12 CCAA en 2022, 12 en 2023, 10 en 2024 y 14 en 2025.

Tabla 18: Unidad TIC de la Consejería de Sanidad o del Servicio de Salud (SS)

Nivel orgánico/pertenencia de la unidad TIC	2022	2023	2024	2025
Dirección General de la Consejería de Sanidad o del SS	3	6	3	3
Dirección General de otra Consejería distinta a la de Sanidad	-	-	2	2
Subdirección General de la Consejería de Sanidad o del SS	9	9	9	9
Dirección Técnica de SI de la Consejería de Sanidad o del SS	2	1	2	2
Jefatura de Área de la Consejería de Sanidad o del SS	2	1	1	1
No especifica el nivel orgánico de la unidad TIC	1	-	-	-

Seguridad de los SI y protección de datos

En la **Tabla 19** se indican, para los años 2022, 2023, 2024 y 2025, el número de CCAA en las que la unidad superior de la que depende la unidad responsable de seguridad de los Sistemas de Información de la Consejería de Sanidad o del Servicio de Salud tienen un determinado nivel orgánico o administrativo. El indicador correspondiente dejó de pedirse en el cuestionario de captura de datos del ÍNDICE 2023 pero se ha vuelto a incorporar a partir del ÍNDICE 2024 por considerar útil la información que aportaba.

Tabla 19: Unidad superior de la que depende la unidad de seguridad de los SI de la Consejería de Sanidad o del Servicio de Salud (SS)

Nivel orgánico/pertenencia de la unidad superior de la que depende la unidad de seguridad de los SI	2022	2023 (*)	2024	2025
Gerencia del SS o Secretaría General de la Consejería de Sanidad o del SS	3	-		2
Dirección General de la Consejería de Sanidad o del SS	4	-	3	1
Dirección General de otra Consejería distinta a la de Sanidad	-	-	2	3
Subdirección General de la Consejería de Sanidad o del SS	6	-	7	8
Jefatura de Área de la Consejería de Sanidad o del SS	1	-	1	1
Jefatura de Servicio de la Consejería de Sanidad o del SS	-	-	1	-
Dirección Técnica de Sistemas de Información	1	-	1	-
Unidad de proyectos de seguridad de la Consejería de Sanidad o del SS	-	-	1	-
Agencia de Ciberseguridad de la Comunidad Autónoma	-	-	1	1
Subdirección de Ciberseguridad	-	-	-	1
No existe en la Consejería de Sanidad o en el SS una unidad específica de seguridad de los SI, o no se indica	2	-	-	-

(*) para el ÍNDICE 2023 no se solicitó este dato

En la **Tabla 20** se indican, para los años 2022, 2023, 2024 y 2025, el número de CCAA en las que la unidad de Seguridad de los Sistemas de Información (SI) de la Consejería de Sanidad o del Servicio de Salud tienen un determinado nivel orgánico o administrativo.

Tabla 20: Unidad de seguridad de los SI de la Consejería de Sanidad o del Servicio de Salud (SS)

Nivel orgánico/pertenencia de la unidad de seguridad de los SI	2022	2023	2024	2025
Dirección General de la Consejería de Sanidad o del SS	-	-	-	1
Dirección General de otra Consejería distinta a la de Sanidad				2
Jefatura de Área de la Consejería de Sanidad o del SS	1	1	1	1
Jefatura de Servicio de la Consejería de Sanidad o del SS	6	4	5	4
Jefatura de Servicio de otra Consejería distinta a la de Sanidad	-	-	-	2
Oficina de seguridad de la Consejería de Sanidad o del SS	3	3	3	2
Unidad de proyectos de seguridad de la Consejería de Sanidad o del SS	1	1	2	2
Agencia de Ciberseguridad de la Comunidad Autónoma	-	-	2	-
Dirección Técnica de S., Jefatura de Sección o Informático Corporativo	3	5	-	
Subdirección de Ciberseguridad				1
Responsable de Ciberseguridad de la CA				1
No existe en la Consejería de Sanidad o en el SS una unidad específica de seguridad de los SI, o no se indica su nivel orgánico	3	3	4	1

En la **Tabla 21** se indican para los años 2022, 2023, 2024 y 2025, el número de técnicos que trabajan en Seguridad de los Sistemas de Información y número de derechos ejercidos por los ciudadanos de los contemplados en el RGPD (derechos de: acceso, rectificación, oposición, supresión, limitación y portabilidad).

Tabla 21: Aspectos relacionados con la Seguridad de los Sistemas de Información

Número de técnicos/ derechos de acceso	2022	2023	2024	2025	% vari. 2025-2024
Número de técnicos (propios y externos) que trabajan exclusivamente en la seguridad de los SI	111	142	198	207	4,56%
Derechos de acceso, de los contemplados en el RGPD, ejercidos por los ciudadanos (*)	224.448	175.521	286.716	184.183	-35,76%

(*) De las 17 CCAA NO han contestado a esta pregunta: 5 en 2022, 2 en 2023, 1 en 2024 y 1 en 2025. Para valorar los datos indicados hay que tener en cuenta estas circunstancias

Profesionales asistenciales (médicos, enfermeras y otro personal asistencial) con certificado electrónico reconocido o cualificado

Resumen de las contestaciones al cuestionario del 2024:

- 10 CCAA contestaron a todas las preguntas
- 3 CCAA contestaron únicamente a las preguntas referidas al personal médico y de enfermería
- 4 CCAA contestaron de forma parcial o no contestaron

De acuerdo con este resumen, a continuación, se indican dos tablas :

La **Tabla 22** referida a las 10 CCAA que respondieron a todos los datos solicitados

La **Tabla 23** referida a 11 CCAA, las 10 CCAA de la tabla anterior mas 1 que únicamente respondió a los datos de personal médico y de enfermería.

Tabla 22: Profesionales asistenciales con certificado digital en 2025

Referido a 10 CC. AA.	Personal médico	Personal de enfermería	Otro personal asistencial
Número de profesionales asistenciales con certificado electrónico reconocido o cualificado	87.559	74.949	23.763
Número total de profesionales asistenciales	99.479	132.859	75.375
Porcentaje de profesionales con certificado	88,02%	56,41%	31,53%

Tabla 23: Profesionales asistenciales con certificado digital en 2025 (solo personal médico y de enfermería)

Referido a 11 CCAA	Personal médico	Personal de enfermería
Número de profesionales asistenciales con certificado electrónico reconocido o cualificado	92.659	78.349
Número total de profesionales asistenciales	104.579	140.359
Porcentaje de profesionales con certificado	88,60%	55,82%



SOC/CERT (Centro de Operaciones de Ciberseguridad/Computer Emergency Response Team)

En la **Tabla 24** se indican el número de CCAA que han respondido afirmativamente a cada una de las preguntas relacionadas con el SOC/CERT a los mismos en 2022, 2023, 2024 y 2025.

Tabla 24: Características de los SOC/CERT

SOC/CERT	2022	2023	2024	2025
Nº de CCAA, en las que existe un SOC/CERT en su Servicio de Salud (SS) o en la Consejería de Sanidad (CS)	8	8	13	12
Nº de CCAA en las que el SOC/CERT es un servicio propio del SS o de la CS	5	5	7	7
Nº de CCAA en las que el SS o la CS están certificados en el Esquema Nacional de Seguridad (ENS) (*)	1	1	2	2

(*) Las 2 CCAA que en 2025 están certificadas en el ENS tienen un nivel alto de certificación (nivel 3)

ELECTROMEDICINA

Al considerar que los dispositivos de electromedicina son muy vulnerables en sí mismos y además, al estar conectados con el exterior y con las redes de los centros asistenciales, son puertas de acceso que requieren un control y unas medidas de protección especiales por parte de los responsables de la seguridad de los SI corporativos. Para conocer la magnitud del problema a nivel global, en el cuestionario del 2023 se incluyeron dos nuevos indicadores. En la **Tabla 25** se resumen las contestaciones recibidas en 2023, 2024 y en 2025.

Tabla 25: Dispositivos de Electromedicina

ELECTROMEDICINA	2023	2024	2025
Nº de CCAA que han contestado a los dos indicadores siguientes	11	12	12
Nº de equipos de electromedicina implantados e integrados con la historia digital de Salud (HES).	16.882	20.689	22.355
Nº de proyectos operativos vinculados a electromedicina	189	450	456

Tendencias y proyectos prioritarios

Uno de los objetivos del ÍNDICE es conocer los futuros desarrollos y proyectos TIC que tienen previsto abordar próximamente las CCAA. Para ello en el apartado Tendencias y proyectos prioritarios del cuestionario de captura de datos se efectúan dos tipos de preguntas:

Tabla 26: Proyectos tecnológicos implantados

Tendencias tecnológicas	Contestaron Sí			En 2025		
	En 2022	En 2023	En 2024	Contestan Sí	Contestan NO	No contestan
CCAA que tienen implantados proyectos de <i>cloud computing</i>	12	12	13	13	4	0
CCAA que tienen implantados proyectos de <i>big data</i>	10	14	13	15	2	0
CCAA que tienen implantados proyectos que integran datos de IOT en las HES (*)	3	8	8	13	3	1
CCAA que tienen implantados proyectos de inteligencia artificial (*)	8	11	12	16	1	0
CCAA que tienen implantados proyectos de medicina de precisión (*)	6	9	11	14	2	1
CCAA que tienen implantados proyectos que integran datos genómicos de los ciudadanos en las HES (*)	4	7	10	10	6	1

Tendencias tecnológicas

En las **Tablas 26 y 27** se resumen las contestaciones a la situación sobre la implantación de proyectos de tecnológicos avanzados y las previsiones para el próximo año.

Tabla 27: Proyectos tecnológicos previstos implantar en el año siguiente

Tendencias tecnológicas	Contestaron Sí			En 2025		
	En 2022	En 2023	En 2024	Contestan Sí	Contestan NO	No contestan
CCAA que tienen previsto implantar proyectos de <i>cloud computing</i> en el año siguiente	13	10	11	14	2	1
CCAA que tienen previsto implantar proyectos de <i>big data</i> en el año siguiente	15	13	11	16	1	0
CCAA que tienen previsto abordar, el próximo año, proyectos que integren datos de IOT en las HES	8	11	10	17	0	0
CCAA que tienen previsto abordar, el próximo año, proyectos de inteligencia artificial	13	13	12	17	0	0
CCAA que tienen previsto abordar, el próximo año, proyectos de medicina de precisión	10	10	9	15	1	1
CCAA que tienen previsto abordar, el próximo año, proyectos que integren datos genómicos de los ciudadanos en las HES	7	11	10	16	1	0

(*) A partir del 2025, las CCAA que tienen implantados proyectos de un determinado tipo, se contabilizan como que tienen previsto abordar el próximo año, proyectos de ese tipo

Inteligencia Artificial (IA)

En el cuestionario de captura de datos para el ÍNDICE 2025, se introdujeron varios indicadores para conocer algunas características relacionadas con la implantación de la Inteligencia Artificial en el SNS.

Tabla 28: Inteligencia artificial

Inteligencia artificial	2025		
	Contestan SÍ	Contestan NO	NO Contestan
¿Existe una unidad específica responsable de la IA en la Consejería de Sanidad o en el SS?	8	9	-
¿Existe algún sistema / modelo de Gobernanza de la IA en la Consejería de Sanidad o en el SS?	6	10	1
¿Existe en la Consejería de Sanidad o en el SS un plan o programa de formación en IA para profesionales de salud?	5	11	1

En la **Tabla 28** se indican el número de CCAA que han respondido a las correspondientes preguntas.

En la **Tabla 29** se indica el número de CCAA, en las que la unidad superior de la que depende la unidad responsable de IA tiene un determinado nivel orgánico o administrativo.

Tabla 29: Nivel orgánico de la Unidad superior de la que depende la unidad de IA

Nivel orgánico/pertenencia de la unidad superior de la que depende la unidad responsable de la IA	2025
Consejería distinta a la de Sanidad	2
Gerencia del SS, Secretaria General o Autónoma de la Consejería o del SS	4
Subdirección General de la Consejería de Sanidad o del SS	2
Dirección General de otra Consejería distinta a la de Sanidad	2
Dirección Técnica de SI de la Consejería de Sanidad o del SS	1
Jefatura de Servicio de la Consejería de Sanidad o del SS	2
No se indica la unidad superior de la que depende la unidad de IA	4

En la **Tabla 30** se indica el número de CCAA en las que la unidad responsable de la IA tiene un determinado nivel orgánico o administrativo.

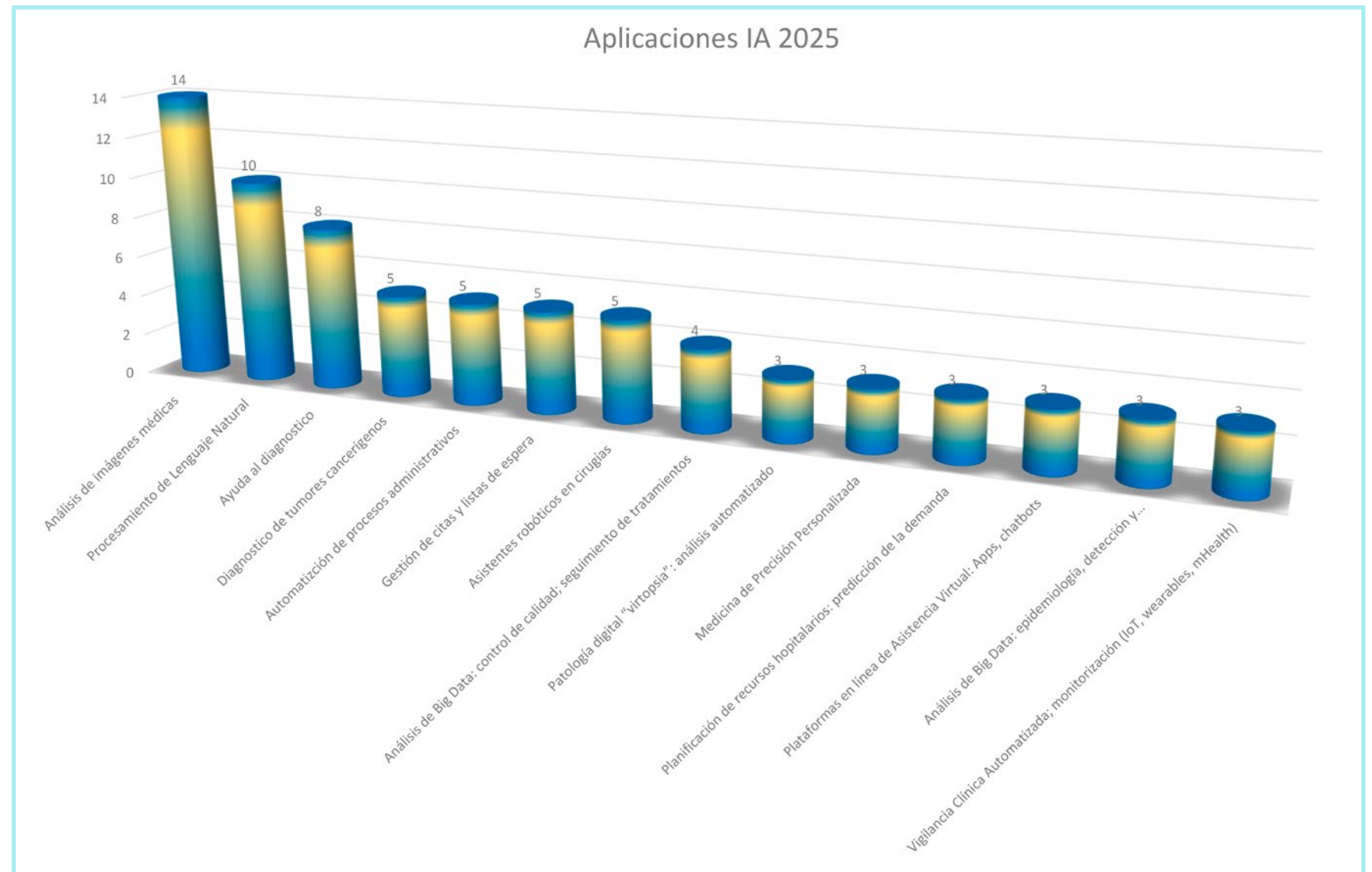
En la **Gráfica 52** se muestran las aplicaciones de Inteligencia Artificial con el número de CCAA (frecuencias) que en el 2025 tienen implantada una determinada aplicación, solo se indican las aplicaciones que tienen más de 3 frecuencias, o sea las que están implantadas en 3 o más CCAA.

Se puede observar que las aplicaciones de IA más implantadas son: análisis de imágenes médicas en 14 CCAA, procesamiento de lenguaje natural en 10 y ayuda al diagnóstico en 8 CCAA.

Tabla 30: Nivel orgánico de la Unidad de Inteligencia Artificial

Nivel orgánico de la unidad responsable de la IA	2025
Dirección General de la Consejería de Sanidad o del SS	2
Dirección General de otra Consejería distinta a la de Sanidad	1
Jefatura de Servicio de la Consejería de Sanidad o del SS	1
Jefatura de Sección de la Consejería de Sanidad o del SS	1
Informático Corporativo	1
Unidad de Innovación de otra Consejería distinta a la de Sanidad	1
Oficina Autónoma para la Aplicación de la IA en la Salud	1
Subdirección de la Consejería de Sanidad o del SS	1
Oficina Técnica del Impulso de la Inteligencia Artificial	1
No se indica o no existe, en la Consejería de Sanidad o en el SS, una unidad específica de IA	7

Gráfica 52: Aplicaciones de inteligencia artificial



Proyectos prioritarios

En el cuestionario de captura de datos se pide que indiquen los proyectos TIC previstos abordar en los próximos años y que se clasifiquen de 1, más prioritario, a 5, menos prioritario.

La **Gráfica 53** muestra el resultado de esa pregunta, ciñéndose únicamente a indicar para cada proyecto cuantas CCAA (cada una es un impacto) lo han considerado de prioridad 1 (la más alta), de prioridad 2, de prioridad 3, de prioridad 4 o de prioridad 5 (la más baja).

Se ha hecho una ponderación de las 5 prioridades, multiplicando:

- Por 5 los impactos de prioridad 1
- Por 4 los impactos de prioridad 2
- Por 3 los impactos de prioridad 3
- Por 2 los impactos de prioridad 4
- Por 1 los impactos de prioridad 5

A continuación se realiza la suma de los resultados parciales

$$P = P1*5 + P2*4 + P3*3 + P4*2 + P5$$

Gráfica 53: Proyectos prioritarios

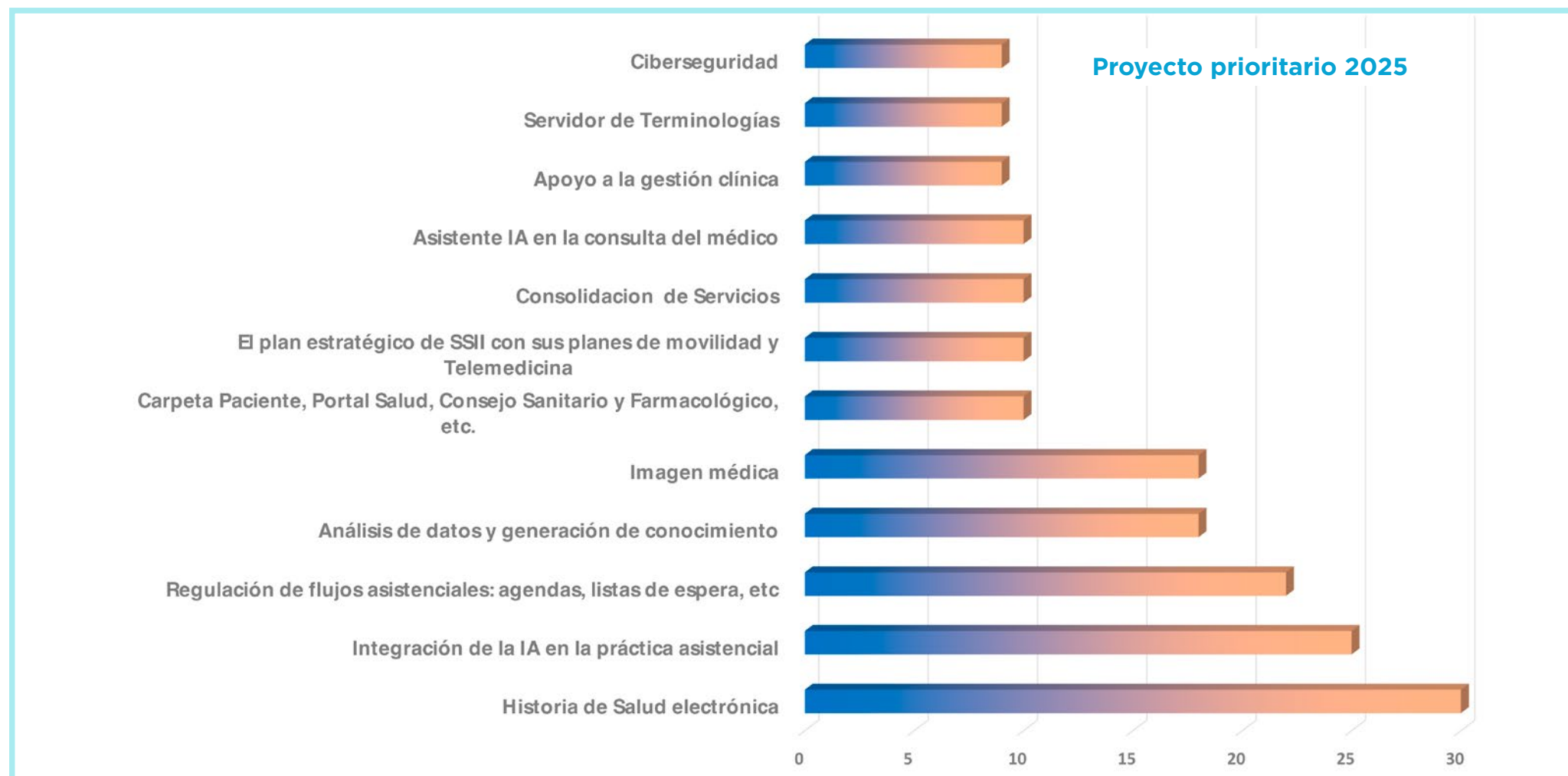


Tabla 31: Relación de proyectos prioritarios

Tendencias 2025 (Proyectos Prioritarios)	COD	P1	P2	P3	P4	P5	Puntuación ponderada
Historia de Salud electrónica	12	30	0	0	0	0	30
Integración de la IA en la práctica asistencial	69	10	12	3	0	0	25
Regulación de flujos asistenciales: agendas, listas de espera, etc.	3	5	12	3	2	0	22
Análisis de datos y generación de conocimiento	1	15	0	3	0	0	18
Imagen médica	7	0	12	6	0	0	18
Carpeta Paciente, Portal Salud, Consejo Sanitario y Farmacológico, etc.	22	0	8	0	2	0	10
El plan estratégico de SSII con sus planes de movilidad y Telemedicina	25	10	0	0	0	0	10
Consolidación de Servicios	34	10	0	0	0	0	10
Asistente IA en la consulta del médico	72	10	0	0	0	0	10
Apoyo a la gestión clínica	11	5	4	0	0	0	9
Servidor de Terminologías	29	5	0	3	0	1	9
Ciberseguridad	61	5	4	0	0	0	9
Medicina personalizada	58	5	0	0	2	0	7
Receta electrónica y/o Interoperabilidad	5	5	0	0	0	1	6
Producir información con base poblacional como soporte para la toma de decisiones clínicas y de gestión	2	5	0	0	0	0	5
Integración primaria, especializada y procesos comunes	27	5	0	0	0	0	5
Interoperabilidad	38	5	0	0	0	0	5
SIL Corporativo	54	5	0	0	0	0	5
Plataforma Unificada de datos	63	5	0	0	0	0	5
Gestión integral de la protección de datos y ciberseguridad	70	5	0	0	0	0	5
Gestión del Bloque Quirúrgico	73	5	0	0	0	0	5
Programa Marco para trasladar la Estrategia de Salud Digital	74	5	0	0	0	0	5
Integración sistema asistencial y sistema de facturación	78	5	0	0	0	0	5
Anillo de Anatomía Patológica, compartido entre todos los laboratorios	80	5	0	0	0	0	5
Command Center Regional (Centro de Mando Regional)	82	5	0	0	0	0	5
Orquestador Vías Clínicas	83	5	0	0	0	0	5
Atención a enfermos crónicos con enfoque sociosanitario	8	0	4	0	0	0	4
Carpeta/Canal Personal de Salud	18	0	4	0	0	0	4
Estación Clínica	19	0	4	0	0	0	4
Consolidación de aplicaciones departamentales	35	0	4	0	0	0	4
Llamada Anónima a Consultas e información a familiares y acompañantes	43	0	4	0	0	0	4
Ayuda a la prescripción	77	0	4	0	0	0	4
Proyecto de Dietética y Cocina	79	0	4	0	0	0	4

Donde P es la puntuación ponderada para ese proyecto.

Con esto visualizamos la participación no lineal de las prioridades destacando aquellos proyectos que alcanzan más puntuación acumulada, lo que permite tener una aproximación más real al resultado buscado y elimina la gran dispersión que presentarían los resultados si se hubiera tenido en cuenta todos los impactos y su prioridad correspondiente.

En el eje horizontal aparece la escala del número de impactos ponderado (P).

En la **Tabla 31** se relacionan los proyectos prioritarios ordenados por la ponderación obtenida de acuerdo con el cálculo anteriormente indicado.

Oficina del Dato de Salud

En el cuestionario de captura de datos para el ÍNDICE 2025 se introdujeron varios indicadores para conocer la existencia y características de las Oficinas del Dato de Salud en el SNS.

A la pregunta: “¿Existe una Oficina del Dato de Salud, en su Servicio de Salud o en su Consejería de Sanidad?”;

- 11 CCAA contestaron SÍ
- 6 CCAA contestaron NO

En la **Tabla 32** se indican, para el 2025, el número de CCAA, en las que la unidad superior de la que depende la Oficina del Dato de Salud tiene un determinado nivel orgánico o administrativo. Cabe señalar que hay CCAA en las que no está creada formalmente la Oficina del Dato de Salud, si indican la Unidad de la que dependerá cuando se cree.

Tabla 31: Relación de proyectos prioritarios (continuación)

Tendencias 2025 (Proyectos Prioritarios)	COD	P1	P2	P3	P4	P5	Puntuación ponderada
Programa piloto para implantar la telesalud mental en el SS	81	0	4	0	0	0	4
VNA (Vendor Neutral Archive) Hospitalaria y AP	84	0	4	0	0	0	4
Consolidación de CPD	16	0	0	3	0	0	3
Gestión de Crónicos	32	0	0	3	0	0	3
Centralización de la solución de HCE en Atención Primaria	41	0	0	3	0	0	3
Accesibilidad del paciente al sistema de salud	55	0	0	3	0	0	3
Sistemas de ayuda a la decisión	39	0	0	0	0	2	2
Digitalización con firma biométrica de consentimientos informados y similares	44	0	0	0	2	0	2
Plataforma sociosanitaria	49	0	0	0	2	0	2
Captura de datos dispositivos médicos y monitorización de pacientes crónicos	67	0	0	0	2	0	2

Tabla 32 : Dependencia de la Oficina del Dato de Salud

Nivel orgánico/pertenencia de la unidad superior de la que depende la Oficina del Dato de Salud de la Consejería de Sanidad o del SS	2025
Consejería distinta a la de Sanidad	1
Gerencia del SS o de la Consejería de Sanidad, Secretaría General	5
Dirección General de la Consejería de Sanidad o del SS	2
Subdirección General de la Consejería de Sanidad o del SS	3
Subdirección General de otra Consejería distinta a la de Sanidad	1
Jefatura de Servicio de la Consejería de Sanidad o del SS	1
No se indica la unidad superior de la que depende la Oficina del Dato de Salud	4
No se indica o no existe, en la Consejería de Sanidad o en el SS, una unidad específica de IA	7

A la pregunta abierta: “Indique la denominación de la Oficina del Dato de Salud o de la unidad específicamente creada para esos fines” contestaron con las denominaciones que se indican a continuación, donde se aprecia que no existe ninguna normalización en estas denominaciones.

Denominaciones de la Oficina del Dato de Salud (en 2025)
Subdirección Técnica Asesora de Gobierno del Dato
Oficina del Dato de Salud
Subdirección de Gestión y Gobernanza del Dato
Subdirección de la Oficina del Dato e IA
Oficina del Dato de la CA
Oficina del dato del sistema de salud de la CA
Oficina del Dato Servicio de Salud
Oficina del Dato
Oficina de Gobierno del Dato
Sección Oficina del Dato
(Dirección Técnica de Sistemas de Información y Resultados en Salud) DTSIRS - Oficina BI

JUAN FERNANDO MUÑOZ MONTALVO, SECRETARIO GENERAL DE SALUD DIGITAL, INFORMACIÓN E INNOVACIÓN DEL SISTEMA NACIONAL DE SALUD



“El sistema sanitario está inmerso en una transformación digital completa”

La modernización tecnológica vivida por el Sistema Nacional de Salud en los últimos años, vitaminada por los fondos europeos, una trabajada estrategia gubernamental y una loable colaboración interterritorial, es incontestable. El desafío ahora, reconoce el secretario general de Salud Digital, Información e Innovación del Sistema Nacional de Salud, es garantizar “que todo lo construido se mantiene, evoluciona y genera resultados medibles en salud para los ciudadanos y en eficiencia para el sistema”.

Esther Macías



El vuelco que ha experimentado la sanidad pública española en materia de digitalización y modernización tecnológica desde la crisis de la pandemia ha sido ingente. Como expone a COMPUTERWORLD uno de los artífices de este logro, Juan Fernando Muñoz Montalvo, en la actualidad, el Sistema Nacional de Salud (SNS) cuenta con servicios que ya funcionan en todo el país como la Historia Clínica Digital, la Receta Electrónica Interoperable, el acceso a MyHealth@EU o el Espacio Nacional de Datos de Salud; sin contar con los más de 700 proyectos de transformación digital que están activos en las comunidades autónomas. Unos hitos, explica por escrito a este medio el secretario general de Salud Digital, Información e Innovación del Sistema Nacional de Salud, que constituyen todo un termómetro de madurez digital.

La sostenibilidad y la consolidación de la transformación tecnológica realizada en los últimos años son los grandes desafíos de un SNS más digitalizado que nunca. ¿Cómo definiría el panorama actual?

El panorama actual es el de un sistema sanitario inmerso en una transformación digital completa, con el reto de hacerla sostenible y universal. Estamos pasando de una fase de despliegue intensivo —impulsada por los fondos europeos del Mecanismo de Recuperación y Resiliencia— a una fase de con-

solidación, maduración y generación de valor real. Tenemos servicios nacionales plenamente operativos como la Historia Clínica Digital del SNS, la Receta Electrónica Interoperable, el acceso a MyHealth@EU o el Espacio Nacional de Datos de Salud. Y más de 700 proyectos de

transformación digital activos en las comunidades autónomas. El reto ahora es asegurarnos de que todo lo construido se mantiene, evoluciona y genera resultados medibles en salud para los ciudadanos y en eficiencia para el sistema.

2026 marca un punto de inflexión

“Estamos pasando de una fase de despliegue intensivo —impulsada por los fondos europeos— a una fase de consolidación, maduración y generación de valor real”

con la finalización de los fondos europeos. ¿Serán capaces las CCAA de mantener el ritmo sin la ayuda de la UE? ¿Aumentará la brecha en calidad asistencial?

Es una preocupación compartida. En el marco de la Estrategia de Salud Digi-

tal, hemos gestionado un presupuesto adicional al habitual de más 1.000 millones de euros distribuidos entre las 17 comunidades autónomas e INGESA. Ese volumen de inversión no es fácil de replicar de forma inmediata con presupuestos nacionales y autonómicos.

Pero hay dos factores que nos dan confianza. Primero, no partimos de cero: las infraestructuras están construidas y muchos proyectos están operativos; el coste de mantenimiento es muy inferior al de despliegue. Segundo, Europa sigue apoyando: vía la senda FEDER Sanidad 2021-2027 gestionada por Red.es y con la aportación de la aportación regional por el propio Ministerio de Sanidad hemos conseguido destinar 223 millones de euros adicionales a los planes 2026-2029 en inteligencia artificial, imagen médica y extensión de la atención digital personalizada / red ÚNICAS. Más del 45% de ese importe se destinará a soluciones de inteligencia artificial.

En cuanto a la brecha territorial, sabemos que es un riesgo real y una de nuestras prioridades como Secretaría General es precisamente evitar que la digitalización genere o amplíe desigualdades. Por eso el modelo de gobernan-

za cooperativa a través de la Comisión de Salud Digital del CISNS es tan importante: compartimos lo que funciona, las mejores CCAA en cada área lidera al resto con el apoyo del Ministerio, evitamos duplicidades y garantizamos que ninguna comunidad se quede atrás.

El ÍNDICE SEIS de 2025 apunta que el gasto TIC de las CCAA en sanidad creció por encima del 20% en 2025. ¿Le ha sorprendido el porcentaje?

Es un dato que confirma lo que intuíamos: la madurez digital ha llegado para quedarse en las agendas de los servicios de salud. El crecimiento del gasto TIC no es un fenómeno aislado ni circunstancial; responde a una realidad nueva. Las comunidades autónomas han incorporado a sus estructuras permanentes equipos, proyectos y compromisos de continuidad que antes no existían. La Estrategia de Salud Digital ha actuado como acelerador y como marco de referencia que ha dotado de legitimidad y sentido estratégico a esas inversiones. Cuando una consejería puede justificar el gasto en interoperabilidad, en historia clínica digital o en analítica de datos como parte de un proyecto nacional co-

herente —y no como una iniciativa tecnológica aislada—, el respaldo político e institucional es mucho mayor. Ese es el efecto palanca de la Estrategia.

¿Hasta qué punto la Estrategia de Salud Digital condiciona ya las decisiones tecnológicas de las CCAA?

Condiciona, pero en el buen sentido: orienta, no impone. La Estrategia funciona como un marco de referencia compartido que define en qué áreas debe haber homogeneidad —estándares de interoperabilidad, modelos de datos, criterios de ciberseguridad— y en cuáles cada comunidad decide que puede

innovar de forma autónoma, y en función de sus intereses y estrategias ligadas a su territorio, aportando soluciones que luego pueden compartirse con el resto. El mecanismo concreto han sido los planes de trabajo vinculados a fondos europeos, condicionando la financiación al cumplimiento de los hitos

no es necesariamente total —la heterogeneidad del SNS es una realidad estructural, que también tiene aspectos positivos— pero es mucho mayor que en cualquier otro momento de nuestra historia reciente.

El modelo de cooperación entre el Ministerio y las CCAA es clave. ¿Qué funciona mejor del modelo y qué no?

Lo que funciona excepcionalmente bien es el modelo de coliderazgo: en lugar de que el Ministerio diseñe soluciones que luego las comunidades autónomas adoptan de forma pasiva, trabajamos en grupos de trabajo mixtos donde las CCAA más avanzadas en cada materia lideran el desarrollo de las soluciones, que luego se ponen a disposición de todo el sistema. Es un modelo federado, que convierte la descentralización —que a veces se percibe como un obstáculo— en un activo real, que multiplica la capacidad de avance por 18 y refuerza el sentido de pertenencia a su Sistema Nacional de Salud, único. La diversidad de los 17 sistemas de salud se transforma en laboratorio de innovación compartida. Lo que presenta

“La diversidad de los 17 sistemas de salud se transforma en laboratorio de innovación compartida”

y estándares acordados en la Comisión de Salud Digital. Eso crea una disciplina virtuosa: quien se alinea con el marco común accede a mejores recursos del programa y obtiene un mayor reconocimiento a sus esfuerzos. Los datos de ejecución de la ESD por comunidad autónoma así lo confirman. La alineación

más dificultades es la velocidad: cuando hay que tomar decisiones técnicas que afectan a todos, los procesos de coordinación llevan tiempo y requieren muchos recursos de gestión en las dos partes. Pero como dice el viejo adagio africano, si quieres ir rápido ve solo, si quieres llegar lejos ve acompañado, y nuestra historia reciente nos hace valorar mucho lo que se puede conseguir todos juntos.

También detectamos diferencias de capacidad técnica y de gobernanza interna entre comunidades que a veces dificultan la homogeneidad de los resultados. Por eso en la nueva estrategia en la que estamos trabajando queremos reforzar los mecanismos de acompañamiento y la sostenibilidad de los avances como objetivos explícitos.

Desde principios de año está en marcha la infraestructura base del Espacio Nacional de Datos de Salud (ENDS). ¿Cómo garantizan que no acabe siendo un repositorio técnico infrautilizado?

La pregunta toca la clave de todo: la tecnología es necesaria pero no suficiente. El ENDS no puede ser un fin



en sí mismo; su valor se mide exclusivamente por los casos de uso que habilita. Hemos aprendido mucho de experiencias previas en otros países donde se construyeron grandes infraestructuras de datos de salud que luego no generaron conocimiento aplicable. Nuestra apuesta es radicalmente distinta: el ENDS se diseña desde la demanda, no desde la oferta tecnológica. Eso significa que la Oficina del Dato del SNS, que actúa como supervisor del uso secundario, evalúa y aprueba los casos de uso concretos antes de que se desarrollen, asegurando que respondan a preguntas clínicas o de política sanitaria reales. Además, el reglamento del Espacio Europeo de Datos de Salud —publicado en el Diario Oficial de la UE en marzo de 2025— impone obligaciones que nos dan un horizonte de demanda muy claro hasta 2031. Saber que hay una agenda regulatoria europea que exige resultados nos obliga a no quedarnos en lo técnico y nos permite avanzar en el trabajo de la Oficina del Dato del SNS con la vista puesta en el futuro organismo de acceso a datos de salud nacional.

¿Qué casos reales del ENDS destacarías?

Actualmente tenemos dos casos de uso relevantes porque combinan impacto clínico inmediato con valor metodológico para el sistema. El primero analiza el uso de antibióticos en el SNS; nos permite identificar patrones de prescripción que contribuyen a la resistencia antimicrobiana. El segundo estudia la descompensación de la EPOC —la enfermedad pulmonar obstructiva crónica— para identificar pacientes en riesgo antes de que requieran hospitalización. Ambos son ejemplos de lo que queremos que sea el ENDS: no un análisis estadístico retrospectivo, sino un sistema que aprende y que apoya decisiones clínicas y de gestión con datos reales del sistema. Además, hay varios casos más en distintas fases de evaluación propuestos por comunidades autónomas o por algunas asociaciones.

¿En qué tecnologías y proyectos esperan que se destine más inversión dentro del SNS a corto y medio plazo?

Sin duda, la inteligencia artificial es el vector de mayor crecimiento, y los da-

tos lo confirman. Vamos a destinar un mínimo del 45% de la financiación de FEDER Sanidad 2021-2027 combinada con fondos del Ministerio de Sanidad —en total 223 millones de euros— a soluciones de IA.

Vemos también las redes de imagen médica y la ciberseguridad, como líneas claras de despegue. El proyecto de red de imagen médica interoperable del SNS y la Estrategia de Ciberseguridad

del SNS aprobada en 2025 contemplan una inversión estructural planificada, frente a la tradicional situación reactiva en ciberseguridad.

A medio plazo, los gemelos digitales, la integración de la genómica en el proce-

so asistencial —a través del SIGenES—, las terapias digitales como prestación del SNS, y la monitorización remota de pacientes crónicos son las apuestas de mayor impacto potencial.

“El Espacio Nacional de Datos de Salud (ENDS) no puede ser un fin en sí mismo; su valor se mide exclusivamente por los casos de uso que habilita”

¿Cómo está el SNS digiriendo la irrupción de la IA generativa y de los agentes autónomos? ¿Cree que se usará la IA clínica a gran escala? ¿Cuándo?

El SNS está siendo muy activo en este ámbito, aunque con una diferencia fundamental respecto a otros sectores: aquí no nos podemos permitir el enfoque de “mover rápido y romper cosas”. Estamos hablando de sistemas que apoyan decisiones clínicas sobre personas. Por eso la Estrategia de IA del SNS —el eIASNS— pone tanto énfasis en el gobierno de la IA: el registro de algoritmos, un sello SNS de calidad, la monitorización posdespliegue, la certificación en el marco de los Reglamentos de IA y de productos sanitarios... En julio de 2025 realizamos un primer inventario: había más de 150 algoritmos de IA activos en los servicios de salud del SNS, comerciales y de desarrollo propio, principalmente en diagnóstico por imagen y apoyo a la toma de decisiones clínicas.

Lo que cambia con la IA generativa y agentiva es la escala y la interfaz: la transcripción automática de la interacción médico-paciente, la generación de



resúmenes de historia clínica o la gestión de citas son aplicaciones con un potencial enorme que ya están siendo pilotadas. Sobre cuándo habrá uso a gran escala: para aplicaciones de soporte administrativo y documentación clínica, diría que estamos en el horizonte 2027-2029. Para IA clínica de diagnóstico validada y escalada en todo el SNS, el horizonte realista es 2028-2030, condicionado a la disponibilidad de datos de calidad en el ENDS y al despliegue del AI Act europeo.

La Ley de Salud Digital está en desarrollo legislativo tras la publicación del Anteproyecto en septiembre de 2025. ¿Qué impacto tendrá la nueva norma y por qué es importante?

La Ley de Salud Digital es la pieza normativa que nos faltaba para que todo el edificio de la transformación digital del SNS tenga una base legal sólida y estable. Hasta ahora hemos operado con una combinación de regulaciones sanitarias generales —la ley general de Sanidad, que hace unos días cumplía 40 años, la ley de Cohesión y calidad, la ley de autonomía del paciente— que

no contemplaban el escenario digital actual, con el marco general de protección de datos del Reglamento 2016/679 y la ley orgánica 3/2018 de protección de datos personales y garantía de derechos digitales y de instrumentos de co-

laboración voluntaria como los convenios con las comunidades autónomas.

El anteproyecto de Ley en el que trabajamos viene a hacer tres cosas fundamentales. Primera, ordena la interoperabilidad obligatoria de la historia clínica

electrónica también para los proveedores de sanidad privada, cumpliendo así lo que exige el reglamento del Espacio Europeo de Datos de Salud. Segunda, establece el modelo de gobernanza del dato adaptado a la estructura descentralizada de España, definiendo quién hace qué en el uso primario y secundario de la información sanitaria. Y tercera, sienta el marco legal básico para el uso de tecnologías digitales, incluida la IA, en el SNS, con las garantías éticas y de derechos digitales que los ciudadanos merecen. Sin esta ley, el cumplimiento del reglamento EHDS a partir de 2027 sería mucho más complejo. Con ella, España estará en condiciones de liderar en Europa la implementación de ese espacio de datos.

¿Le preocupa la ciberseguridad del SNS? ¿Está preparado para un potencial ciberataque a gran escala?

Sí, me preocupa, y creo que cualquier responsable de servicios públicos digitales que diga que no le preocupa está mintiéndose a sí mismo y al ciudadano. La digitalización crea valor y crea vulnerabilidades: son dos caras de la misma moneda. El sector sanitario es posible-

“La transcripción automática de la interacción médico-paciente, la generación de resúmenes de historia clínica o la gestión de citas son aplicaciones con un potencial enorme que ya están siendo pilotadas”



mente el objetivo más atacado a nivel global, precisamente porque los datos de salud tienen un valor altísimo para los ciberdelincuentes y porque la continuidad asistencial es crítica. Los ataques de *ransomware*, *phishing* e intrusión en infraestructuras sanitarias se han multiplicado en toda Europa. Frente a eso, hemos dado un paso cualitativo muy importante: en noviembre de 2025 el Consejo Interterritorial del SNS aprobó la primera Estrategia de Ciberseguridad del SNS para el período 2025-2028, que convierte la ciberseguridad en una política estructural del sistema, no en una respuesta reactiva a incidentes. Los ocho objetivos de esa estrategia —desde establecer redes de alerta temprana entre servicios de salud hasta garantizar la resiliencia operativa y la capacitación continua del personal— nos sitúan en la dirección correcta. Tenemos también alineamiento con la directiva NIS2, que clasifica al sector salud como servicio esencial de alta criticidad. Respecto a si estamos preparados para un ciberataque a gran escala, sin duda, estamos mejor preparados que hace tres años, y seguimos mejorando. Pero en ciberseguridad no existe el “preparado al cien

por cien”: el objetivo es la resiliencia, la capacidad de responder y recuperarse con rapidez manteniendo la continuidad asistencial. Hacia ahí vamos y seguiremos trabajando todos juntos.

La visión que guía nuestra estrategia ESD 2030 es la de un sistema sanitario digital, conectado y proactivo, que apoye el derecho a una atención justa, continua y adaptable. En concre-

zada en cualquier hospital o centro de salud de España o de Europa en cuestión de segundos. Un sistema donde la IA apoya al médico en el diagnóstico y sugiere basándose en las guías clínicas el mejor tratamiento para ese paciente concreto con la información de su historia, la parte relevante de su genoma y los datos de miles de pacientes similares, pero siempre bajo supervisión clínica y con criterios de transparencia y explicabilidad. Un sistema donde los gemelos digitales diseñan de forma personalizada la atención a pacientes crónicos, anticipando descompensaciones antes de que ocurran, y donde la monitorización remota reduce los ingresos hospitalarios innecesarios. Un sistema que aprende: que a medida que genera datos de calidad en el ENDS, los transforma en conocimiento, en mejores protocolos, en políticas sanitarias más precisas. Todo ello dentro de un marco ético firme, con plena soberanía sobre los datos de los ciudadanos y una ciberseguridad que garantiza la continuidad y la confianza. No es ciencia ficción: es parte de la hoja de ruta que ya hemos trazado para 2030 y en la que ya estamos trabajando. **cw**

“Estamos mejor preparados que hace tres años para un ciberataque a gran escala y seguimos mejorando. Pero en ciberseguridad no existe el ‘preparado al cien por cien’”

¿Cómo será el SNS en un futuro próximo gracias a la adopción de las últimas tendencias tecnológicas y digitales?

to, imaginamos —y trabajamos para que sea realidad— un SNS donde el paciente que puede compartir la información clínica significativa y actuali-

Los desafíos de un SNS más digitalizado que nunca

Los avances en modernización tecnológica y digital del Sistema Nacional de Salud (SNS) español han sido significativos en los últimos años gracias a los fondos europeos y a toda una batería de medidas gubernamentales como la puesta en marcha de la Estrategia de Salud Digital del SNS; pero 2026 marca un punto de inflexión para el sector, con la finalización de dichos fondos en el horizonte.

Gonzalo Díaz Bonet | Imagen: Garpress





Luciano Sáez, presidente de la Sociedad Española de Informática de la Salud (SEIS).



Sobre estos desafíos se profundizó en un almuerzo/debate organizado el pasado 25 de marzo por COMPUTERWORLD y la SEIS, realizado con la colaboración de las compañías Everpure, Oesía y el partner de esta última, Nunsys, y en el que participaron los máximos responsables tecnológicos de gran parte de las comunidades autónomas y del Ministerio de Sanidad. Un encuentro en el que se pusieron sobre la mesa retos como el reto de gestionar la gobernanza de la

IA, la retención de talento, la creciente amenaza de la ciberseguridad o el complejo momento geopolítico que atravesamos.

El aumento del gasto TIC en sanidad pública, una positiva “sorpresa”

El encuentro, moderado por Esther Macías, directora editorial de COMPUTERWORLD, arrancó con una reflexión por parte del presidente de la SEIS, Luciano Sáez Ayerra, quien reconoció que los datos del último ÍNDICE son



Esther Macías, directora editorial de COMPUTERWORLD.



Yolanda López Mínguez, subdirectora de Infraestructuras y Servicios Técnicos en el Servicio de Salud del Principado de Asturias (SESPA).

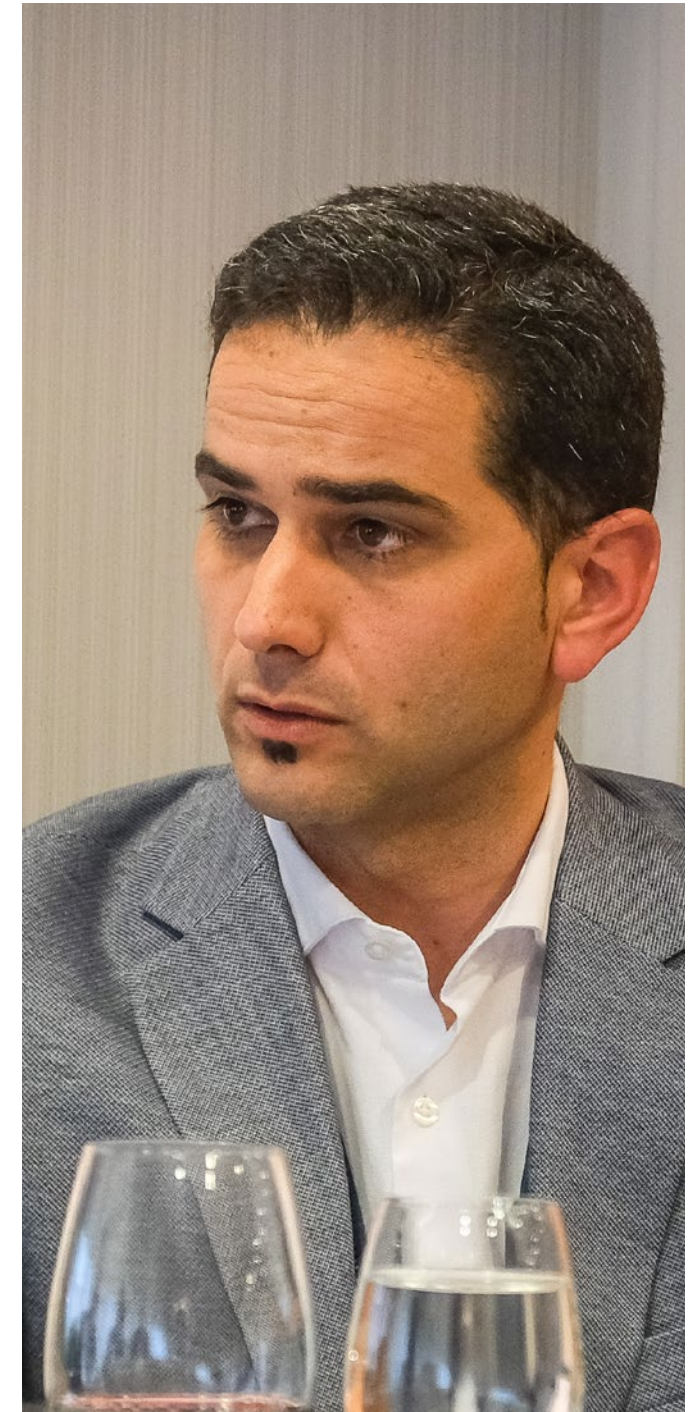
“una sorpresa” positiva, en cuanto suponen un incremento de la cifra destinada a la tecnología sanitaria, algo que la mayoría de los asistentes atribuyeron a la ejecución de los fondos europeos.

“El problema será la cifra de 2027”, indicó Yolanda López Mínguez, subdirectora de Infraestructuras y Servicios Técnicos en el Servicio de Salud del Principado de Asturias (SESPA). En este punto, explicó que será en ese año cuando se haga notar la discontinuidad de unos fondos que han impulsado el gasto en el ámbito sanitario.

Para buena parte de los responsables tecnológicos, la llegada del 30 de junio, fecha de finalización de la ejecución de los fondos europeos también pondrá fin a “un momento de tensión”, provocado por la sobrecarga de trabajo a la que se han visto abocados buena parte de los trabajadores de las áreas de TIC de los Servicios de Salud. “Esperamos que sea un alivio para la parte administrativa y de contratación”, dijo Óscar Fernández Torre, director general de Planificación, Ordenación, Gestión del Conocimiento y Salud Digital del Gobierno de Cantabria.



Óscar Fernández Torre, director general de Planificación, Ordenación, Gestión del Conocimiento y Salud Digital del Gobierno de Cantabria.



José Pérez Alonso, director de Sistemas, Tecnologías e Innovación para la salud del Servicio Riojano de Salud.



Joaquín Velilla Moliner, director general de Salud Digital e Infraestructuras del Departamento de Sanidad del Gobierno de Aragón.



Josean Bizkai Urrutia, director general de Telecomunicaciones y Digitalización en el Gobierno de Navarra.

Una situación tensa que, sin embargo, genera también una nueva incertidumbre. “¿Y ahora qué?”, se preguntaba José Pérez Alonso, director de Sistemas, Tecnologías e Innovación para la salud del Servicio Riojano de Salud. “Es el momento de evaluar los proyectos y ver cuáles han funcionado mejor”, advirtió.

Para Joaquín Velilla Moliner, director general de Salud Digital e Infraestructuras del Departamento de Sanidad del Gobierno de Aragón, es el momento de invertir en herramientas tecnológicas que ya han quedado obsoletas. “El principal reto es la gobernanza de la IA, que se nos está yendo de las manos. No estamos suficientemente organizados, nos falta arquitectura”, dijo tras revelar que desde su departamento se están testando agentes de IA, algo que todavía “va despacio”.

Josean Bizkai Urrutia, director general de Telecomunicaciones y Digitalización en el Gobierno de Navarra, coincidió en la necesidad de afrontar el reto que supone la irrupción de la IA en el sistema sanitario. “Hay que definir cómo se embebe en las soluciones, y cómo afrontamos la certificación del producto sanitario”, advirtió.



Benjamín Juez, subdirector Corporativo de Informática y Sistemas de Información en la Dirección General de Osakidetza.



Javier Martínez Gilabert, director general de Transformación Digital de la Región de Murcia.



La fragilidad del momento geopolítico

Benjamín Juez, subdirector Corporativo de Informática y Sistemas de Información en la Dirección General de Osakidetza (el Servicio de Salud del País Vasco), introdujo un nuevo elemento de debate entre los asistentes al encuentro: la fragilidad del momento geopolítico, provocada por los conflictos en Irán, Ucrania y otras regiones del planeta. “Hay precios que se están disparando, y en momentos de crisis el gasto se recorta”, dijo, mostrando su preocupación por los posibles efectos de una recesión económica.

Desde la Región de Murcia, Javier Martínez Gilabert, director general de

Transformación Digital de la comunidad, apuntó otro de los grandes retos en 2026: la retención del talento. “La gente se está yendo a la empresa privada y eso es un problema serio”, denunció. José Manuel Alcaraz, subdirector general de Tecnologías de la Información en Servicio Murciano de Salud, coincidió con su planteamiento. “Los principales problemas son presupuestarios, de personal y de falta de estrategia en el ámbito de la IA”, dijo.

Roberto Pizarro, subdirector de Sistemas de Información del Servicio Extremeño de Salud, añadió también otros retos adicionales para la gestión tecnológica del sistema sanitario: el seguimiento



José Manuel Alcaraz, subdirector general de Tecnologías de la Información en Servicio Murciano de Salud.



Roberto Pizarro, subdirector de Sistemas de Información del Servicio Extremeño de Salud.

remoto a pacientes, el acercamiento del paciente al profesional y la necesidad de potenciar la Oficina del Dato.

El reto de autoeficientar las áreas de TI sanitarias

Para Ismael Vargas Pina, director general de sistemas de información y comunicaciones del Servicio Andaluz de Salud, el principal reto en la actualidad es “saber gestionar una IA que es ilimitada”. “Todos los días hay nuevos casos de uso, pero el presupuesto no es ilimitado, así que hay que saber elegir bien”, dijo. “Tenemos que incorporar la IA al propio ámbito TIC, el desarrollo copilotado por IA mejora tiempos y reduce costes, no nos olvidemos de autoeficientarnos”, agregó.

Áurea Morillo, secretaria general de Investigación, Innovación y Salud Digital de la Junta de Andalucía, coincidió con su compañero y resaltó el valor de encuentros como el organizado por la SEIS y COMPUTERWORLD para “aprender de otras comunidades autónomas cómo gestionar la IA y el dato”.

Por su parte, Benigno Rosón, subdirector general de sistemas y tecnologías de información de la Conselleria de Sa-



Ismael Vargas Pina, director general de sistemas de información y comunicaciones del Servicio Andaluz de Salud.



Áurea Morillo, secretaria general de Investigación, Innovación y Salud Digital de la Junta de Andalucía.



Benigno Rosón, subdirector general de sistemas y tecnologías de información de la Consellería de Sanidad del Servicio Gallego de Salud en la Xunta de Galicia.



Miguel Ángel Benito Tovar, subdirector de Transformación, Innovación y Salud Digital del Servicio de Salud de las Islas Baleares (IB-SALUT).

nidad del Servicio Gallego de Salud en la Xunta de Galicia, definió este último ejercicio como “muy satisfactorio”. “Los fondos europeos nos han servido para ejecutar proyectos como el despliegue de la IA y la automatización y para introducir tecnología y su gobernanza”, aseguró.

“En Baleares hemos implementado cuatro estrategias de salud digital en el último año, lo que demuestra que los fondos sirven para algo”, dijo Miguel Ángel Benito Tovar, subdirector de Transformación, Innovación y Salud Digital del Servicio de Salud de las Islas Baleares (IB-SALUT). “Nos sirven para crear una nueva cartera de servicios que no teníamos”, recalcó.

Algo más crítico se expresó Carlos Gallego Pérez, director de Salud Digital en el Institut de Diagnòstic per la Imatge de la Generalitat de Catalunya, quien recordó que, pese al aumento, los fondos destinados a TIC suponen poco más de un 1% del presupuesto de las consejerías de Sanidad. “Hay hospitales que dedican más presupuesto a lavandería que a TIC”, denunció.

Nuria Ruiz Hombrebueno, directora general de Salud Digital de la Consejería de Digitalización de la Comunidad de Ma-



Carlos Gallego Pérez, director de Salud Digital en el Institut de Diagnòstic per la Imatge de la Generalitat de Catalunya.



Nuria Ruiz Hombrebueno, directora general de Salud Digital de la Consejería de Digitalización de la Comunidad de Madrid.

drid, destacó el “gran esfuerzo” realizado para ejecutar los fondos. “Hemos trabajado para que todo tuviese una buena valoración y que no se quedase en pilotos, que fuesen proyectos escalables”, dijo.

Desde el Ministerio de Sanidad, la directora general de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, Noemí Cívicos Villa, afirmó que, tras el 30 de junio, surge “una oportunidad de consolidar proyectos emblemáticos”. En este sentido, confió en que la documentación remitida cada seis meses desde su departamento “sirva para trasladar a los consejeros la necesidad de invertir en tecnología”.

Visión de la industria

El debate se completó con la visión de la industria. Para Adela de Toledo, directora general de Everpure (antes Pure Storage) para Iberia, el sanitario es el sector que tiene que hacer una transformación más profunda en los próximos años. “La sostenibilidad financiera debe estar asociada al futuro, porque hay una crisis de componentes. Nosotros no vamos a crecer en precios y ofrecemos nuestro servicio a todas las áreas sanitarias”, reflexionó.



Noemí Cívicos Villa, directora general de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud del Ministerio de Sanidad.



Adela de Toledo, directora general de Everpure para Iberia.



Carmen Derlinchán, directora preventiva para el Sur de Europa.



Eduardo Zubizarreta, responsable del sector salud en Nunsys Group.

Su compañera Carmen Derlinchán, directora preventiva para el Sur de Europa, ahondó en esta visión: “Los proveedores no siempre pueden seguir el ritmo de la Administración, pero nuestra compañía puede mantener una oferta cinco años asegurando que no va a subir de precios, algo muy valioso en tiempos de incertidumbre”, explicó. “Además, cada versión de nuestra tecnología es más sencilla y reduce el consumo energético”, aseveró.

Eduardo Zubizarreta, responsable del sector salud en Nunsys Group, apuntó una posible solución al problema de la escasez de talento: reconocer a los profesionales TIC del sector Salud como profesionales sanitarios. También planteó otro espacio para la reflexión. “¿Es justo –se preguntó– que el departamento TIC asuma el gasto de implantar la IA cuando va a revertir en beneficios para todos?”.

Por último, el gerente de estrategia digital y delegado territorial en Madrid de Nunsys, Jorge Reverte, especialista en IA, apuntó la necesidad de reforzar la inversión en ciberseguridad no solo para proteger la información, sino también las máquinas (OT) de ataques maliciosos y de emplear la IA en el *backoffice* “para agilizar trámites de forma espectacular”. **CW**



Jorge Reverte, gerente de estrategia digital y delegado territorial en Madrid de Nunsys.

El viaje de la Comunitat Valenciana hacia una salud digital más inclusiva, ética y eficiente

El sistema valenciano de salud está inmerso en un ambicioso viaje de transformación hacia un modelo más conectado, predictivo, personalizado y sostenible. Al frente de la estrategia TIC de la Estrategia de Salud Digital de la Comunitat Valenciana, el mapa de ruta de esta aventura, está María José Tarazón Muñoz. La CIO explica el estado de los proyectos estratégicos de una iniciativa que aúna innovación digital, interoperabilidad, IA y gobernanza del dato para mejorar la experiencia de pacientes y profesionales.

Esther Macías

El sistema sanitario público valenciano se halla en pleno proceso de modernización tecnológica gracias a la ejecución de la Estrategia de Salud Digital de la Comunitat Valenciana. Presentada a finales de 2024 y dotada de una inversión de 235 millo-

nes de euros hasta 2027, la Estrategia conlleva adoptar un nuevo paradigma tecnológico y de gestión, diseñado para dar respuesta a los grandes desafíos que afronta el sistema autonómico en la actualidad, marcados por la elevada presión demográfica y la dispersión geográfica de su población, así como la



Sede de la Conselleria de Sanidad de la Generalitat Valenciana.

cronicidad de enfermedades, las elevadas expectativas de los pacientes y la escasez de profesionales sanitarios.

Una figura clave en la materialización de este ambicioso proyecto es María José Tarazón Muñoz, subdirectora general de Tecnologías de la Información y las Comunicaciones para la Salud de la Conselleria de Sanidad de la Generalitat Valenciana. La responsable, en el cargo desde septiembre de 2023, cuenta con una amplia trayectoria en la aplicación de las tecnologías de la información al servicio público, de cuyo colectivo TIC forma parte desde hace décadas. La directiva desgana a COMPUTERWORLD el estado actual de la implantación de la citada Estrategia, que se estructura en siete ejes de actuación (Servicios Digitales, Espacios de Datos Sanitarios e Inteligencia Artificial, Historia Clínica Única, Transformación de Procesos Eficientes, Confianza digital, Mejora de Infraestructuras y Gobierno de Tecnologías de Información) y contempla más de 200 proyectos, entre los que destaca la puesta en marcha de la historia clínica única y centralizada para la Comunitat Valenciana y el anillo radiológico.

Al arrancar la entrevista, realizada por videollamada, Tarazón rememora el com-



María José Tarazón Muñoz, subdirectora general de Tecnologías de la Información y las Comunicaciones para la Salud de la Conselleria de Sanidad de la Generalitat Valenciana.

plicado arranque de la Estrategia de Salud Digital, cuya presentación oficial tuvo lugar el día que ocurrió la tragedia de la DANA de Valencia, una coincidencia que no solo eclipsó el anuncio de la modernización de la sanidad regional, sino que además “ralentizó ciertos procesos de tramitación de contrataciones porque, obviamente, había que cumplir con otras urgencias de mayor relevancia en ese momento”, como explica la responsable.

Desde entonces, agrega, se han producido avances en este camino hacia una sanidad que ponga el dato en el centro. “Porque gobernar el dato sanitario supone gobernar la sanidad que ponga el dato en el centro. Solo así podremos aplicar y construir una sanidad inteligente. Y si es inteligente también será más sostenible. También debemos hacerla más cercana. Inteligente, sostenible y cercana, así queremos que sea nuestra sanidad”.

Servicios digitales y espacios de datos sanitarios

“A nivel de Servicios Digitales, ya hemos puesto en marcha una nueva *app*, GVA Salud, a la que podremos ir añadiendo



funcionalidades y que nos va a proporcionar mucha más agilidad a la hora de comunicarnos con el ciudadano. Además, los ciudadanos pueden acceder (también con huella biométrica) tanto a los informes médicos como a las pruebas de imagen. Desde ahora iremos desarrollando más elementos para añadir agendas de salud pública, de salud mental y otro tipo de contenidos a la *app*".

En materia de Espacios de Datos Sanitarios, Tarazón rememora la puesta en marcha de varias oficinas del gobierno del dato. "Queremos definir qué modelo de gobernanza tienen que cumplir los organismos, las fundaciones y los institutos sobre los que recae la actividad investigadora en la comunidad"; un modelo de gobernanza que, avanza, espera que esté completamente definido después del verano.

De cara a materializar esta gobernanza del dato, añade, la institución cuenta con "tecnología que nos permite ingerir, limpiar, catalogar, segmentar información y después ponerla al servicio o bien de la explotación para un uso primario o la explotación para un uso secundario, con todas las cautelas de anonimización que corresponda".

Además, indica, se ha abierto una Oficina para el Gobierno de la IA, que está definiendo y sentando la metodología de despliegue de la IA en la organización, garantizando el cumplimiento normativo y un despliegue ordenado, ético, seguro y equitativo de esta tecnología.

"El uso de la IA no debe ser oportunista y como quiera cada departamento, sino corporativo. Además, cuando se aplique una IA debe hacerse tras haber analizado una necesidad y teniendo muy clara la expectativa y el objetivo que se quiere cubrir". Subraya Tarazón en que, ante cualquier proyecto de transforma-

ción digital, "no solo hay que comprobar que la tecnología cubra con el objetivo, sino que la organización esté preparada y ordenada para encajar dicha tecnología". En este momento, dice, ya está en fase de ejecución un sistema de IA para diagnóstico de mama y está a punto de

adjudicarse otro sistema de IA para tórax y hueso.

En materia de IA, la Conselleria también tiene ya contratos en marcha para ampliar capacidades en Atención Primaria con asistentes virtuales. "La idea es mejorar la gestión de la demanda, porque actualmente se pierde el 50%

de las llamadas de los pacientes". La IA llegará también a los médicos. "Hemos hecho proyectos piloto, con la colaboración del Ministerio de Sanidad, para aplicar la IA durante la cita médica, de forma que el facultativo pueda atender al paciente mientras se transcribe automáticamente lo que este último cuenta. La idea, además, es que el médico cuente después con un resumen del relato del paciente. De momento, la experiencia ha sido positiva".

Centralización de la historia clínica, "el proyecto estrella"

La centralización no solo de la historia clínica sino del resto de aplicaciones sanitarias conforma uno de los ejes más relevantes de la Estrategia porque, explica Tarazón, "venimos de un ecosistema de aplicaciones bastante distribuido y con falta de gobierno, lo que dificulta después la normalización tanto de los datos como de los procesos".

El proyecto "estrella" para Tarazón es establecer una Historia Clínica Única. "El proyecto se ha retrasado por algunas incidencias ajenas a nosotros en la tramitación, pero confío en que podamos

La centralización de la historia clínica y del resto de aplicaciones sanitarias es uno de los ejes claves de la Estrategia de Salud Digital de la Comunitat Valenciana



entrar en fase de ejecución en junio". Se trata, insiste, de un proyecto "decisivo". "Actualmente, 24 hospitales utilizan Orion Clinic como estación clínica, mientras que otros centros mantienen soluciones tecnológicas diferentes, deriva-

das de la evolución histórica del sistema y de los distintos modelos de gestión. Nuestro objetivo es converger hacia una solución corporativa única, que reduzca la fragmentación, refuerce la continuidad asistencial y garantice una gestión

más homogénea, eficiente y equitativa en toda la Comunitat Valenciana".

Para ello, expone, se está trabajando para incluir toda la parte de Atención Hospitalaria dentro de esta la Historia Clínica Unificada; posteriormente, se incluirá

también toda la parte de Atención Primaria dentro de esta solución de historia clínica unificada. "La herramienta no crea la norma, pero sí ayuda. Y aquí la normalización y homogeneización del dato en toda su extensión va a venir de la mano de unificar la herramienta", añade Tarazón.

Además, en la actualidad, la entidad está lanzando procesos de contratación y proyectos con el objeto de centralizar las soluciones de gestión del anillo de imagen, genómica, anatomía patológica e incluso laboratorio. "Y estamos centralizando también la catalogación de pruebas y de todos los resultados para cada una de las pruebas".

Otro proyecto importante en marcha es el despliegue de una plataforma sobre la que modelar todos los procesos de cribado. "En la actualidad, el proceso de cribado de cáncer de cérvix ya está en producción, el de cáncer de mama está en piloto (se desplegará a finales de julio) y después llegarán otros como el de colon".

Hacia una sanidad más eficiente

La transformación de procesos es otro de los puntales de la Estrategia de Salud

Digital de la Comunidad Valenciana. El objetivo es avanzar hacia una sanidad más eficiente, homogénea y orientada a resultados”, explica la CIO. Desde el inicio, su equipo identificó la necesidad de incorporar una tecnología corporativa capaz de modelar, automatizar, monitorizar y mejorar procesos transversales, más allá de los sistemas de información tradicionales. “Disponemos de una plataforma que nos permite rediseñar procesos asistenciales, administrativos y de salud pública, incorporando automatización, trazabilidad y capacidad de mejora continua. No se trata solo de digitalizar lo que ya hacemos, sino de revisar cómo lo hacemos para ganar eficiencia, calidad y capacidad de respuesta”.

Además, como parte de este objetivo, se está trabajando en desplegar soluciones para homogeneizar el actual ecosistema de gestión de recursos humanos. “Es decir, todo el control de la gestión de registro de puestos, la Relación de Puestos de Trabajo (RPT) del colectivo de instituciones sanitarias, la gestión de bolsas, etc. Y, unido a esto, la gestión de la nómina de todos los profesionales que están en activo”. “El

pliego del proyecto está prácticamente para tramitar”, cuenta Tarazón.

No hay salud digital sin confianza digital

“No podemos hablar de salud digital si no hablamos de confianza digital”, sentencia Tarazón. Para cambiar la relación con el paciente y hacerla cercana, cuenta, hay que poner el dato en el centro, pero ga-

rantizando no solo que tiene calidad, sino que es seguro. “Solo así podemos hablar de construir un sistema de salud inteligente, sostenible y, desde luego, preparado para la gobernanza del dato en su uso primario y uso secundario, para potenciar la investigación y la innovación. Nada de esto es posible si no nos ocupamos de la seguridad de la información”.

Ocuparse de la seguridad de la información, relata la portavoz, supone que los procedimientos cumplan con todos los requisitos que marca la regulación de protección de datos en toda su extensión, lo que incluye también la regulación del Espacio Europeo de Datos Sanitario, y el Reglamento de IA. En esta línea, cuenta Tarazón, el organismo ha definido toda una estrategia de

ciberseguridad que tiene en su haber diversos proyectos, “como la normalización de toda la topología de red de los hospitales y de los centros de primaria, la actualización de la infraestructura...”. Reconoce que el cumplimiento del Esquema Nacional de Seguridad es una prioridad para la Conselleria: “Ya hemos iniciado contratos específicos

de adecuación al ENS que nos están permitiendo identificar mejoras y aplicar medidas concretas en procesos, sistemas e infraestructuras. Nuestro compromiso es avanzar con rigor y rapidez hacia la certificación, reforzando la seguridad y la confianza en los servicios digitales sanitarios.

Mejora de la ‘cocina’ sanitaria TIC: las infraestructuras

“Aunque hablar de infraestructuras (como yo las llamo: la ‘cocina’ de todo) no vende, lo cierto es que éstas son esenciales”, reflexiona Tarazón, que explica que la Conselleria ha hecho todo un esfuerzo por “contar con infraestructuras escalables, robustas, respaldadas y con aplicaciones preparadas para que puedan ser balanceadas”.

En esta línea, la entidad ha realizado “un esfuerzo tremendo en virtualizar aquello que todavía no estaba virtualizado, en homogeneizar el cómputo en todos los departamentos, en crear una metodología de trabajo a nivel de administración de sistemas similar en todas las áreas y en desplegar capacidades de almacenamiento”.

“Buscamos eficiencias en las TIC, pero también sanitarias y de gestión sanitaria”

En el momento actual, marcado por la tendencia a la hibridación, no sorprende que la institución esté optando por tecnologías en nube, además de *on-premise*. Por ejemplo, el *data lake* y la HCU. El primero se halla en la nube de IBM, el segundo lo estará en la de AWS. “Creemos que la nube nos va a facilitar el cumplimiento del ENS porque, de forma nativa, las soluciones ya vienen con respaldo”.

Cambio cultural en el gobierno de TI

“Para mí, el eje más importante de la Estrategia de Salud Digital es el relativo al gobierno de las TI”, dice Tarazón. Esta parte descansa en los conceptos de “gobernanza TIC federada” y “convergencia y mejora de las aplicaciones”.

Se trata, añade, de “un cambio cultural en la forma de proveer las TIC” basado en la idea de que las TIC deben brindarse de manera centralizada y, por tanto, ser diseñadas “para cubrir una necesidad corporativa desde la equidad, buscando máxima potencia y capacidad a la compra que se realice (sea esta de infraestructura o de software) y pensando en responder a requisitos como

la interoperabilidad, la gobernanza del dato, la seguridad y el cumplimiento normativo...”.

Esta nueva forma de gobierno de TI se ha diseñado en paralelo a la nueva organización sanitaria a nivel territorial. El fin último, en definitiva, es “bus-

car eficiencias de todo tipo: en las TIC, pero también sanitarias y de gestión sanitaria”.

Por tanto, explica la portavoz, en el área de salud de la Comunidad Valenciana actualmente este modelo se articula en tres niveles de gobierno. “Un primer nivel estratégico, situado en

la Conselleria, donde se adoptan las principales decisiones de planificación, priorización e inversión, con la participación de equipos multidisciplinares TIC y funcionales en función de la naturaleza de cada necesidad. Un segundo nivel táctico, vinculado a las Agrupacio-

nes Sanitarias Interdepartamentales, con un papel más ejecutivo y de coordinación territorial, orientado a ordenar necesidades, definir criterios comunes de despliegue, priorizar actuaciones y elevar propuestas al nivel estratégico. Y un tercer nivel operativo departamental, donde reside gran parte del cono-

cimiento funcional y técnico necesario para implantar las soluciones, acompañar a los profesionales y garantizar que la tecnología se adapta correctamente a la realidad asistencial y organizativa de cada ámbito”.

En definitiva, explica, “estamos transformando el modelo de provisión tecnológica hacia un enfoque corporativo, participativo y orientado a resultados. Las decisiones deben responder a criterios de equidad, seguridad, interoperabilidad y cumplimiento normativo, pero también a necesidades reales de la organización. Por eso, el éxito de la transformación digital requiere coliderazgo entre los equipos TIC y los profesionales funcionales, para asegurar que la tecnología se adopta correctamente y genera valor efectivo en los procesos asistenciales y de gestión”.

Cuenta Tarazón que, a la hora de elaborar la Estrategia de Salud Digital, se organizaron sesiones participativas “para que los profesionales de distintas áreas se sintieran representados y supieran qué viene de la mano de esta iniciativa. Esta decisión, asegura, “fue muy positiva; facilitó que todo el mun-

“Los profesionales TIC no podemos ser los líderes únicos de los proyectos de transformación [...]. La garantía de éxito está en el coliderazgo funcional y técnico”



do se viera reflejado en la Estrategia y ha agilizado la puesta en marcha de los proyectos”.

Esta colaboración entre las áreas funcionales y la de TIC “se está consiguien-

do”, según la portavoz. “Un ejemplo es todo el equipo que ha participado en la redacción de un contrato tan complejo como el de Historia Clínica Unificada, para cuya elaboración hemos extraído

conocimiento de las diferentes áreas hospitalarias”.

Además, agrega Tarazón, como parte del mencionado modelo federado la Conselleria de Sanidad también ha im-

pulsado la contratación de nuevos perfiles acordes con el momento actual. Se ha creado un cuerpo de tecnología sanitaria con el fin de integrar científicos de datos, ingeniero de organización y sistemas, biotecnólogos, ingenieros biomédicos e ingenieros informáticos y de telecomunicaciones.

Aprendizajes

Preguntada por cuáles han sido los grandes aprendizajes en este viaje hacia la salud digital y qué recomendaría a homólogos de otras comunidades autónomas que estén inmersos en un proyecto similar, Tarazón lo tiene claro: “Para que un proyecto TIC funcione debe estar respaldado por un liderazgo potente (de una o varias personas), que conozca las áreas de negocio y las carencias. Porque el éxito de la tecnología que nosotros adquiramos desde el área TIC va a depender de una correcta definición de los requisitos y los objetivos que se pretenden cumplir”.

Desde el lado técnico, continúa la experta, se garantiza la interoperabilidad y la seguridad y la disminución de la complejidad, analizando el sistema del que se viene y la migración que hay que ha-



cer. “Los profesionales TIC no podemos ser los líderes únicos de los proyectos de transformación, ya sean asistenciales, de administración sanitaria, recursos humanos o logística. La garantía de éxito está en el coliderazgo funcional y técnico: visión asistencial y de gestión, junto con solvencia tecnológica, interoperabilidad, seguridad y capacidad de ejecución”.

Además, reflexiona, “transformar no es solo invertir en tecnología. Requiere también tiempo, liderazgo funcional y profesionales con conocimiento, experiencia y capacidad para acompañar el cambio. Sin esa implicación directa de la organización, la tecnología difícilmente genera valor real”.

Otro aprendizaje es que “gobernar y proteger el dato no es solo una responsabilidad tecnológica, sino organizativa. Los equipos TIC impulsamos los controles, la seguridad y el cumplimiento, pero la protección de la información y el uso responsable de la inteligencia artificial deben formar parte de la cultura y de los procesos de toda la organización”.

Por otra parte, lanza una exigencia compartida por muchos responsables TIC de la Administración Pública. “La

contratación pública necesita seguir evolucionando para acompañar la velocidad de la tecnología. No es lo mismo contratar suministros ordinarios que soluciones en nube, inteligencia artificial o plataformas digitales complejas. Sería deseable avanzar hacia marcos más claros y adaptados a este tipo de tecnologías, siempre manteniendo las garantías de transparencia, concurrencia y control público”.

Cooperación interterritorial y futuro próximo

Tarazón valora muy positivamente la labor realizada los últimos años por la Secretaría General de Salud Digital y su defensa de los fondos europeos para destinarlos a modernizar las TIC en el Sistema Nacional de Salud, así como su estrategia de poner el dato en el centro. “La secretaría general nos ha dado un empujón con una doble ayuda: económica y de gestión y coordinación. Se ha preocupado de que los responsables de TI de las comunidades autónomas participemos en este proceso y busquemos soluciones homogéneas”.

Sin embargo, se lamenta la portavoz, “no todas las comunidades partimos de la misma casilla de salida. Hay comunidades que, por circunstancias históricas, ya tienen soluciones centralizadas y, por tanto, mucho terreno ganado de cara, por ejemplo, a desarrollar modelos de IA. Pero otras, como la nuestra, no, debido a decisiones que se tomaron en el pasado y que en su día eran buenas”.

Respecto al futuro de la innovación TIC en las comunidades una vez que finalicen los fondos (este año), Tarazón reconoce: “La finalización de los fondos europeos nos obligará a priorizar aún más y a demostrar que las inversiones realizadas generan eficiencia y valor público. Ahí estará el reto: consolidar lo desplegado, obtener retorno organizativo y seguir avanzando con criterios de sostenibilidad”.

En el caso particular de la Comunidad Valenciana, la portavoz confía en que las actuaciones que han abordado en materia de centralización generen eficiencia. “Estamos en una fase de transición exigente: debemos consolidar los proyectos estratégicos en marcha y, al mismo tiempo, sostener con garantías los sistemas actualmente en producción. El reto es priorizar, ejecutar con agilidad y

convertir la inversión realizada en valor real para la organización, los profesionales y la ciudadanía”.

“La transformación que estamos acometiendo en la Comunidad Valenciana es profunda, valiente y necesaria. No podíamos responder a la normativa de continuidad asistencial con 33 historias clínicas. No es posible que, ante cualquier petición de datos a esta Comunidad, previamente tengamos que agregar datos de 33 hospitales. El cambio que estamos haciendo es esencial. Pero me preocupa que haya continuidad en el tiempo. Estos proyectos tienen que ir más allá de las legislaturas políticas”.

Tarazón finaliza con una reflexión sobre el impacto de este proyecto de transformación del sistema valenciano de salud: “Lo verdaderamente transformador para el paciente será la redefinición de su relación con el sistema sanitario: una relación más cercana, más ágil y adaptada a sus necesidades. Ante esto es esencial estar atentos a la “brecha digital”. Para los profesionales, supondrá también un cambio relevante, al facilitar su trabajo diario, reducir cargas administrativas y liberar tiempo para tareas de mayor valor asistencial”. **CW**

Los hospitales frente al cibercrimen: así gestionan las amenazas de ciberseguridad

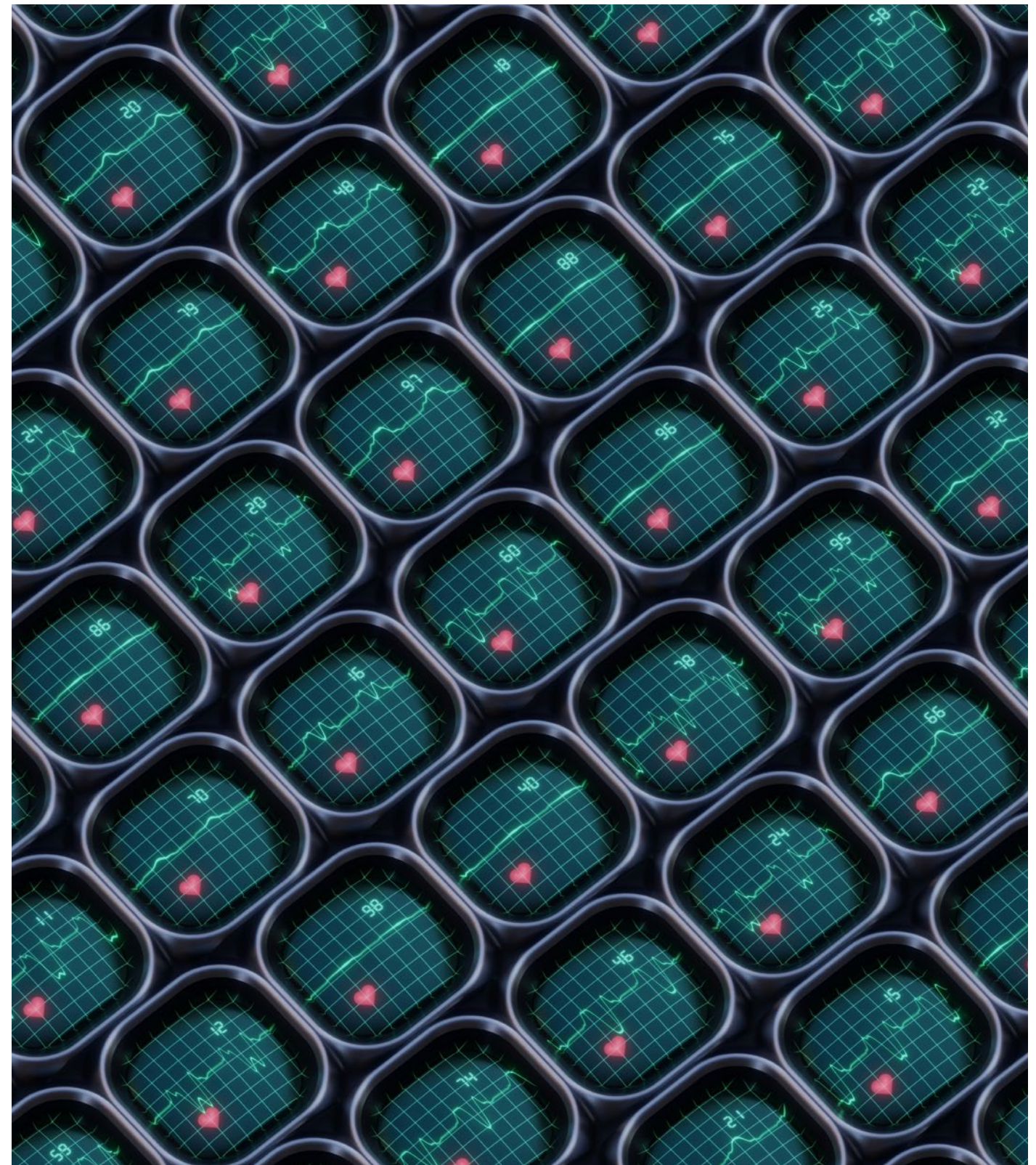
En la última temporada de *The Pitt*, ante una amenaza de ciberseguridad, apagan todos sus sistemas y se pasan al papel. No es una decisión muy realista, confirman desde la Sanidad española. Pero ¿cómo se hacen las cosas en el mundo real?

Raquel C. Pico

En la última temporada de *The Pitt*, la popular serie médica de HBO, el drama lo pone la ciberdefensa. Los hospitales de la ciudad están cayendo uno tras otro en secuestros cibercriminales y, antes de ser los siguientes, los responsables del centro protagonista apagan toda su infraestructura TI. Adiós a las *tablets*, a los historiales digitales, a los envíos de peticiones de pruebas por

correo interno. Bienvenido de nuevo el protocolo que se había abandonado allá por los 90.

¿Una respuesta efectiva ante un potencial ataque de ciberseguridad o una licencia dramática? “Lo segundo”, responde al otro lado del teléfono Jorge Prado, jefe del Servicio de Protección de Datos y Gestión del Servicio de Sistema de Tecnologías de la Información del Servicio Gallego de Salud (Sergas), “por-





que el resultado de ciberataque sería precisamente eso. O sea, estás haciéndote tú mismo ese ciberataque”. “Siempre es una decisión compleja, estresante y con muchos factores a tener en cuenta”, suman de forma conjunta desde la Agencia de Ciberseguridad de Catalunya y el CatSalut a través del correo electrónico. “En estos casos es necesaria una buena evaluación de riesgos y las posibles consecuencias para tomar la mejor decisión”, señalan, estudiando el potencial riesgo, pero también el impacto que esto tendrá para ciudadanía.

“El objetivo actual de la ciberseguridad es intentar que los sistemas estén funcionando 24/7 y, en caso de ciberataques, la estrategia siempre es la misma, intentando contener, frenar el ciberataque, y a partir de ahí limpiar y recuperar”, explica Prado.

El ataque de ficción puede pecar de exceso de dramatización, pero si esta serie ha optado por este argumento para crear conflicto y hacer avanzar la historia es porque los ciberataques están a la orden del día y, en el caso de la sanidad, es algo que preocupa intensamente al sector. De hecho, otras series médicas, como *Anatomía de Grey*, han



Complejo del SERGAS, IGAPE e IGAES, en Galicia.

dedicado ya alguno de sus episodios a lo que ocurre cuando un hospital es hackeado.

Los datos del *Global Cybersecurity Outlook 2026* del Foro Económico Mundial apuntan que los riesgos en ciberseguridad han aumentado y que la IA y el panorama geopolítico global se han convertido en puntos candentes que hacen más importante que nunca la resiliencia en ciberseguridad. España [no permanece al margen](#) de esta tendencia. En este contexto macro, la sanidad es tanto un sector clave para la

ciudadanía como especialmente sensible por los datos que maneja, así que se ha convertido también en un goloso *target* para el cibercrimen. En 2025, se registraron un 42% más ataques en el sector sanitario que en el año precedente, según un [estudio](#) de Secure&IT.

La sanidad no permanece al margen de los demás sectores, sino que más bien está en el ojo del huracán. “Es normal y habitual que cualquier sistema expuesto a internet reciba miles de millones de ataques”, apuntan las fuentes catalanas. “En el 2025, la

Agencia de Ciberseguridad de Catalunya detectó, en sus ámbitos de competencia, un total de 9.100 millones de ataques, de los cuales 2.038 millones se concentraron en el ámbito de Salud”, señalan. De estos, más de 7.000 millones fueron bloqueados “de forma automática e inmediata”. “La mayoría de estos incidentes tuvieron un impacto leve en el entorno sanitario y solo un incidente se valoró como una afectación grave”, indican, destacando el valor de la prevención. El Sergas, según datos que recoge [La Voz de Galicia](#),



se enfrenta cada día con una media de 8 millones de intentos de ataque.

Son cifras elevadas, pero, como apunta Prado, “si le preguntas al responsable de ciberseguridad de tu empresa te dará cifras semejantes en proporción al número de usuarios que tenéis o a los servicios que prestáis”. “Esa es la dificultad. Estamos sujetos a muchas amenazas”, confirma.

Desde el sector confirman que las amenazas han aumentado en volumen, aunque se siguen manteniendo los tipos de ataque que ya circulaban años atrás (*ransomware*, intentos de robos de credenciales, *phishing*...). “Las dos principales amenazas de ciberseguridad que se pronostican en el ámbito de salud para el 2026 son el despliegue manual de *ransomware* y el compromiso de credenciales asociado a *infostealers*”, apuntan desde la Agencia de Ciberseguridad de Catalunya y el CatSalut. Prado suma, eso sí, que este es un “sector muy innovador”, también en su lado criminal. “Por un lado hay que controlar la cantidad de amenazas que sabes que están y, por otro, tener mucha capacidad de anticipación para las cosas nuevas que van saliendo”, ex-



Jorge Prado, jefe del Servicio de Protección de Datos y Gestión del Servicio de Sistema de Tecnologías de la Información del Sergas.

plica. “Es una mezcla de todo”, indica, y la capacidad de reacción crucial para sobrevivir.

Eso sí, esto es algo que la sanidad tiene muy presente y que se está priorizando. Tanto a nivel europeo (con fondos de resiliencia) como a nivel estado se han creado líneas maestras y estándares. “Nos hemos blindado muchísimo más”, asegura Prado. “Lo que sí tiene el sistema sanitario es muchísimos proveedores, desde el que te trae el pan hasta quien te proporciona medicamentos”, añade. Ahí es donde se está viendo un crecimiento de los ataques. “En cuanto hemos subido nuestro nivel de seguridad, hemos notado que se han dirigido más a nuestros proveedores”.

Datos reales y sensibles

Si algo tienen en común todas las historias de ficción es que el ataque paraliza el hospital, complica el trabajo del personal sanitario y llega incluso a poner en peligro a sus pacientes (lo que, por supuesto, da el drama necesario para hacer un capítulo que enganche). En la vida real, los pacientes no son giros dramáticos, sino personas reales y la información que manejan en los centros



sanitarios especialmente sensible. Si el hackeo de una red social puede ser un problema, que roben tu información de salud resulta algo pesadillesco.

“Yo siempre uso la misma frase: que en las redes sociales presumimos y, sin embargo, las enfermedades se padecen”, apunta Prado. “Es una información que muy poca gente hace pública”, apunta. “Te hace vulnerable y que se revelen ciertos datos tuyos puede tener muchísima influencia en tu vida”, señala. “Los precios de venta en la *dark web* son muy elevados. Los datos médicos como una historia clínica, resultados de pruebas o imágenes diagnósticas, entre otros, cuentan con costes mucho más altos que datos de otros ámbitos”, añaden las fuentes catalanas. Si una tarjeta de crédito se cotizaba en los mercados del cibercrimen a unos 17 euros, una historia clínica se va a 216.

Los servicios de salud con los que ha hablado COMPUTERWORLD confirman que son plenamente conscientes de la importancia de salvaguardar estos datos, de que es algo que hace que sean especialmente responsables.

Aun así, es justo este atractivo el que hace que los cibercriminales se centren

en estos destinos y que los ataques de *ransomware* usen los datos como palanca para las extorsiones.

El fundido a cero

Los hospitales de la ficción se inspiran en los hospitales reales que ya fueron víctimas de uno de estos ataques. En Estados Unidos se han registrado unos

cuantos: uno en febrero de 2024 bloqueó a la empresa subsidiaria sanitaria responsable de uno de cada tres historiales médicos en ese país, Change Healthcare. El 74% de los hospitales de la red reconocieron después en una [en-](#)

[cuesta](#) de la American Hospital Association, que había tenido un impacto directo en la atención a pacientes y un 94% que había tenido un impacto financiero. Para volver a la normalidad, el 60% de los hospitales necesitaron entre dos semanas y tres meses.

En España, el caso más conocido es el del hospital Clínic de Barcelona, que víc-

Agencia cuando se les pregunta por ese caso concreto. “Aunque estamos acostumbrados a momentos críticos, este fue realmente duro y estresante por su gran impacto mediático”, explican. En el momento, se dotó de equipos para que los profesionales de urgencias pudiesen seguir trabajando. 48 horas después del ataque, la prensa [recogía](#) que se recuperaba progresivamente la actividad echando mano del papel y de ordenadores de contingencia. Ahora, tres años después, tanto el sistema sanitario catalán como su agencia de ciberseguridad explican que la experiencia los llevó a acelerar “determinadas acciones que ya se estaban implementando progresivamente” y el despliegue integral de su Modelo Integral de Ciberseguridad.

Las experiencias en ciberseguridad de los hospitales y de las empresas sirven, además, de aprendizaje colectivo. Si algo señalan las fuentes es que poner en común entre ellos lo que aprenden y lo vivido es una pasarela más para ganar resiliencia.

Los ordenadores de contingencia de los que se habla en el caso del Clínic muestran también una historia un tanto distinta al salto analógico que hacen

“En caso de ciberataques, la estrategia siempre es la misma: intentar contener, frenar el ciberataque, y a partir de ahí limpiar y recuperar”, explica Prado



Hospital Clínic de Barcelona. Créditos: HCB/Francisco Avia.

en *The Pitt*. Allí echan mano de hojas de calco para pedir análisis de sangre, los pacientes que están en su sistema de Urgencias se apuntan en una pizarra blanca a la vista de todo el mundo (algo

que, a quien conoce un poco la normativa europea de protección de datos, le resulta chocante) y, del fondo de algún almacén, han rescatado un olvidado fax. Todo es tan raro y tan nuevo para el

personal más joven que acaban pidiendo a una administrativa jubilada que venga a echarles un cable. Ella fue la última de quienes trabajaban *así*. Desde fuera, todo parece muy complicado y

hasta escasamente realista. ¿Podría un hospital sobrevivir otra vez a un mundo de papel?

“En el contexto de urgencias, y si contemplamos una situación de mínimos enfocada a la supervivencia de la actividad asistencial, sí. Pero garantizar el nivel de calidad que nos exigimos en el sistema público de Cataluña no sería posible”, explican de forma conjunta desde la Agencia de Ciberseguretat de Catalunya y el CatSalut. “Fuera de urgencias, existen medidas complementarias dentro de lo que denominamos planes de contingencia que permitirían mantener la actividad asistencial durante 48 horas”.

“No es solo volver al papel, es que hay muchos dispositivos que directamente ya no funcionarían”, apunta Prado. Algo tan básico como una radiografía se volvería un imposible, porque ya no se imprimen y se ven en pantallas. “Los hospitales son instituciones altamente informatizadas y no pueden llevar a cabo actividad asistencial sin los sistemas de información”, confirman también desde Cataluña.

Y, además, como suma el experto gallego, un hospital cuenta con sistemas

tan básicos como los que puede tener un edificio de oficinas: el aire acondicionado del trabajo seguramente se controle con un aparato de domótica. “En un hospital, como en vuestro medio o como en el ciudadano, todo está basado en tecnologías, todo”, resume Prado. “No es planteable volver al papel, a los 90, porque muchas cosas directamente no funcionarían”.

Cómo responder entonces a un ataque

Apagar para sobrevivir no parece, por tanto, una decisión muy acertada, o al menos no una que deberían aprender de la ficción los responsables de ciberseguridad de la vida real.

Si se les pide a los expertos que hagan un diagnóstico de lo que han hecho los de la ficción, apuntan que otras soluciones serían factibles. “Nos faltaría información para entender por qué motivo no se han tomado otras medidas como, por ejemplo, aislar el centro totalmente de Internet sin llegar a apagar todos los sistemas, con el objetivo de mantener el acceso a las historias clínicas de los pacientes, o mantener el envío de los resultados de analíticas o de radiología





internamente”, señalan los expertos catalanes. Pagar el rescate ante una amenaza (otro de los recursos dramáticos que se han usado en otras series) nunca es una buena estrategia, recuerdan. “Nadie nos asegura que vayamos a recuperar la información después de ese pago y, haciéndolo, estaríamos financiando una actividad criminal”. Y puede incluso tener efecto llamada.

En todo caso, siempre es clave valorar el impacto potencial de los incidentes, tener siempre copias de seguridad, tomar decisiones teniendo en cuenta al área de ciberseguridad y a la de salud y, sobre todo, prepararse. La mejor estrategia pasa por la ciberdefensa.

Prado recomienda certificar en nivel alto de la Escala Nacional de Seguridad a todos los servicios del sistema sanitario, no solo lo que se ven como más clínicos “sino en cualquier servicio que se te ocurra”. Al final, todos los servicios y todos los dispositivos van a estar conectados a la red. “Lo mismo pasa en tu casa”, recuerda. Evitar que cualquier terminal o punto de conexión sea vulnerable ayuda a la seguridad global. “Después, también hay que proteger a todo lo que es el circuito”, señala. Desde

las personas que cubren turnos de forma especial hasta la logística. “La visión de ciberseguridad debe ser totalmente integral”, señala.

Desde Cataluña hablan igualmente de una “concienciación global por capas y para todos los niveles” cuando se les pregunta por las buenas prácticas. “Eso requiere disponer de una capa de protección mediante el uso de herramien-

tas tecnológicas, pero también acciones de formación, concienciación y simulacros, entre otras, dirigidas al personal de los centros sanitarios”, señalan. “La concienciación de los usuarios es una capa igual de importante que la tecnología que aplicamos”, aseguran, en línea con lo que comenta Prado. Y recuerdan que todo lo sospechoso debe ser detectado y “generar una alerta que provoque el análisis”. Para que todo funcione los

puntos vulnerables deben minimizarse al máximo posible.

De las palabras de estos expertos se desprende que no solo hay que apostar por una tecnología robusta y actualizada, sino también por buenos hábitos, prácticas y estrategias. Se necesita también a personal que trabaje en estos terrenos y que esté alerta para proteger en tiempo real frente a

las amenazas. Los sistemas sanitarios miman sus infraestructuras. El Sergas [cuenta](#) con un bunker en Santiago de Compostela dedicado al procesamiento de sus datos. Aun así, que sea propio o ajeno no es tan determinante como que se hagan bien las cosas. “La certeza absoluta no existe, lo que tienes que procurar es tener tus servicios debidamente gestionados y medidos”, responde Prado.

Los retos de la era de los cisnes negros

El [apagón de 2025](#) dejó importantes lecciones: las cosas que parecían imposibles (esos llamados cisnes negros) no lo eran tanto. Mientras el país se fundía a negro, los hospitales resistían. “Nosotros estábamos preparados”, confirma Prado, “porque dentro de las exigencias que tiene una metodología como el Plan Nacional de Seguridad está tener un sistema de alimentación ininterrumpida en caso de un apagón”.

Aunque este experto apunta, eso sí, que cabe preguntarse si el apagón se hubiese prolongado durante días. “Igual conseguimos que la tecnología siga funcionando, pero los problemas son igual de índole diferente”. Durante Filomena, el problema más grave para los hospitales madrileños era que sus profesionales no podían llegar a trabajar. Estar preparados ante los riesgos no es, por tanto, algo solo tecnológico, sino mucho más holístico. “La ciberseguridad son recursos tecnológicos, lo que nos parece más obvio, pero también son personas, también son circuitos, protocolos. Eso es lo que tienes que ver en su globalidad”, señala el experto. **CW**

La mejor estrategia pasa por la ciberdefensa

Comentarios sobre el 'ÍNDICE SEIS 2025'

Con el objetivo de ayudar a conocer la situación de la implantación de las TIC en el sector sanitario público español y su evolución en el tiempo, en el año 2012 la Sociedad Española de Informática de la Salud (SEIS) y los responsables TIC de los Servicios de Salud de las Comunidades Autónomas, con la colaboración del Ministerio de Sanidad y de la Entidad Pública Empresarial Red.es, abordaron la elaboración del ÍNDICE SEIS.

El ÍNDICE SEIS se viene publicando de forma ininterrumpida desde el año 2012 por lo que esta es la decimocuarta edición. Al disponer de datos contrastados procedentes de fuentes fiables, el estu-

dio aporta una valiosa información sobre la situación actual de la implantación de las TIC en la sanidad pública española.

Además de la información que directamente nos da la publicación anual del ÍNDICE, conviene aclarar que, bajo petición y manteniendo el principio de confidencialidad y anonimato al que estamos comprometidos, podemos suministrar información resultante del cruce de diversos indicadores y de su evolución a lo largo de los años. De acuerdo con esta posibilidad, y a modo de ejemplo, a continuación, vamos a profundizar en la evolución, durante los últimos diez años, de tres aspectos que consideramos son factores críticos para la transformación digital del SNS.



Carlos García Codina

Coordinador del 'Índice SEIS'

Tabla 1: Presupuesto sanitario frente a presupuesto y gasto TIC

Nivel Nacional	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Presupuesto Sanitario (en millones de €)	55.077	57.232	59.209	61.093	63.232	66.214	70.920	75.743	79.758	82.329
Presupuesto TIC (en millones de €)	674	696	729	707	784	899	958	883	848	1.028
Gasto TIC de las CCAA (en millones de €)	639	675	736	701	781	849	896	956	1.011	1.240
% (Presup.TIC/ Presup. Sanitario)	1,224%	1,215%	1,231%	1,158%	1,239%	1,358%	1,351%	1,166%	1,064%	1,248%
% (GastoTIC de las CCAA/ Presup. Sanitario)	1,161%	1,180%	1,243%	1,148%	1,236%	1,283%	1,263%	1,262%	1,268%	1,507%

Análisis de aspectos críticos

Para este análisis utilizaremos tablas y gráficas similares a las que aparecen en el ÍNDICE con el fin de facilitar su comprensión y posibles relaciones con los datos de este.

Presupuestos y gastos TIC

En la **Tabla 1** se indica, a nivel nacional, la evolución de los presupuestos sanitarios, de los presupuestos TIC propios de las CCAA y de los gastos TIC de las CCAA, así como la evolución de los porcentajes de estos dos últimos con respecto a los presupuestos sanitarios.

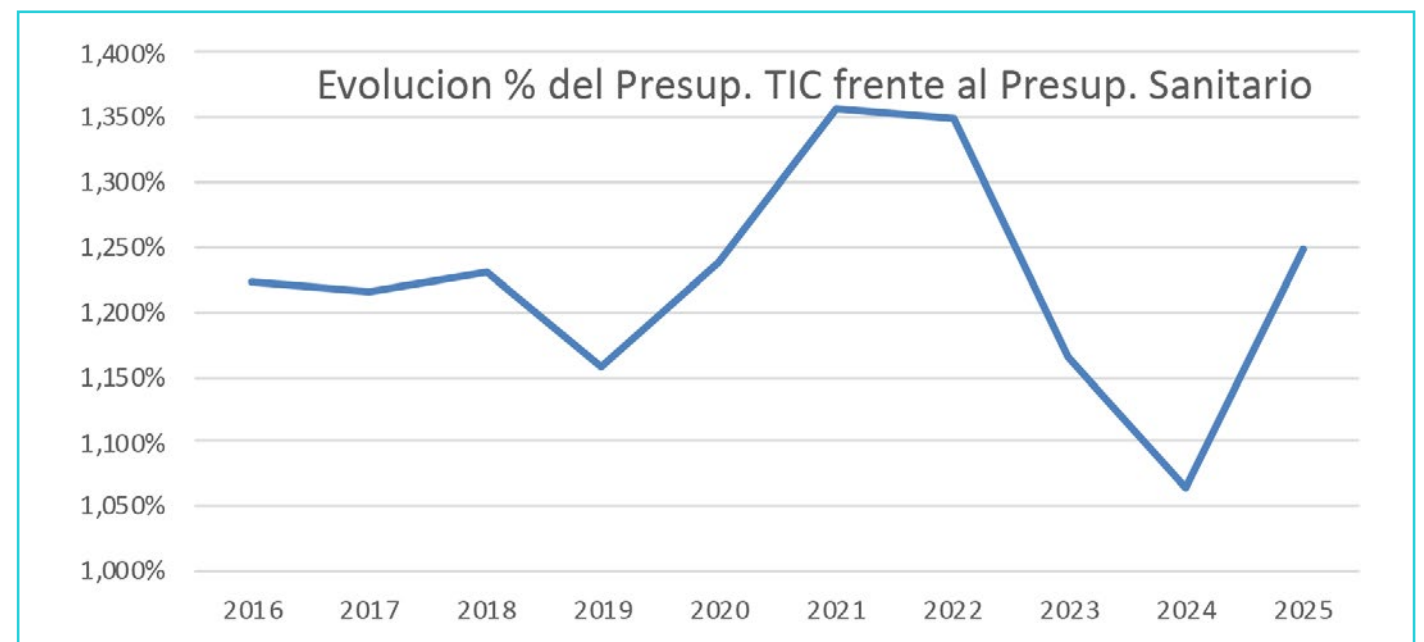
En esta tabla observamos que:

- En los años 2023 y 2024 los presupuestos propios TIC de las CCAA disminuyeron significativamente, tanto en valor absoluto como en la proporción con los presupuestos sanitarios. El motivo de esa disminución puede deberse a que los Servicios de Salud de las CCAA, globalmente considerados, al disponer temporalmente de fondos estratégicos adicionales, optaron por rebajar los presupuestos propios asignados a las TIC.
- El porcentaje del presupuesto TIC con respecto al presupuesto sanitario, fue en 2025 el 1,248% valor

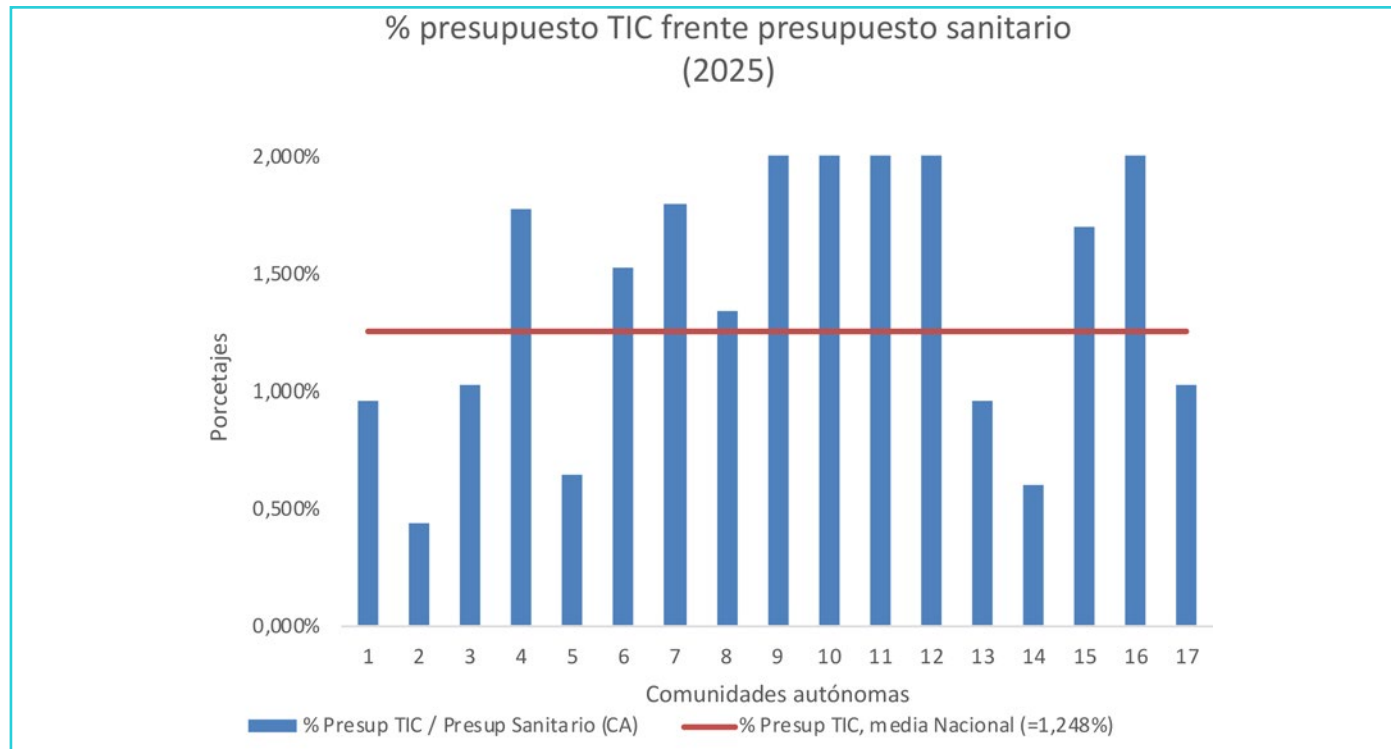
similar al del 2020 pero inferior a los valores de 2021 y 2022, tal y como se resalta en la **Gráfica 1**.

- El porcentaje del gasto TIC de las CCAA frente al presupuesto sanitario se está incrementando de

Gráfica 1: Evolución del porcentaje del presupuesto TIC frente al presupuesto sanitario



Gráfica 2: Porcentaje presupuesto TIC frente a presupuesto sanitario por CCAA



forma continua hasta alcanzar el 1,507% en 2025, pero aun está lejos del 2,5% que la SEIS considera sería el recomendable.

La **Gráfica 2** nos muestra, para el 2025, la desigual distribución del % del presupuesto TIC con respecto al presupuesto sanitario entre las CCAA, donde podemos comprobar que, en ese año, hay siete CCAA que se quedaron por debajo de la media nacional del 1,248%.

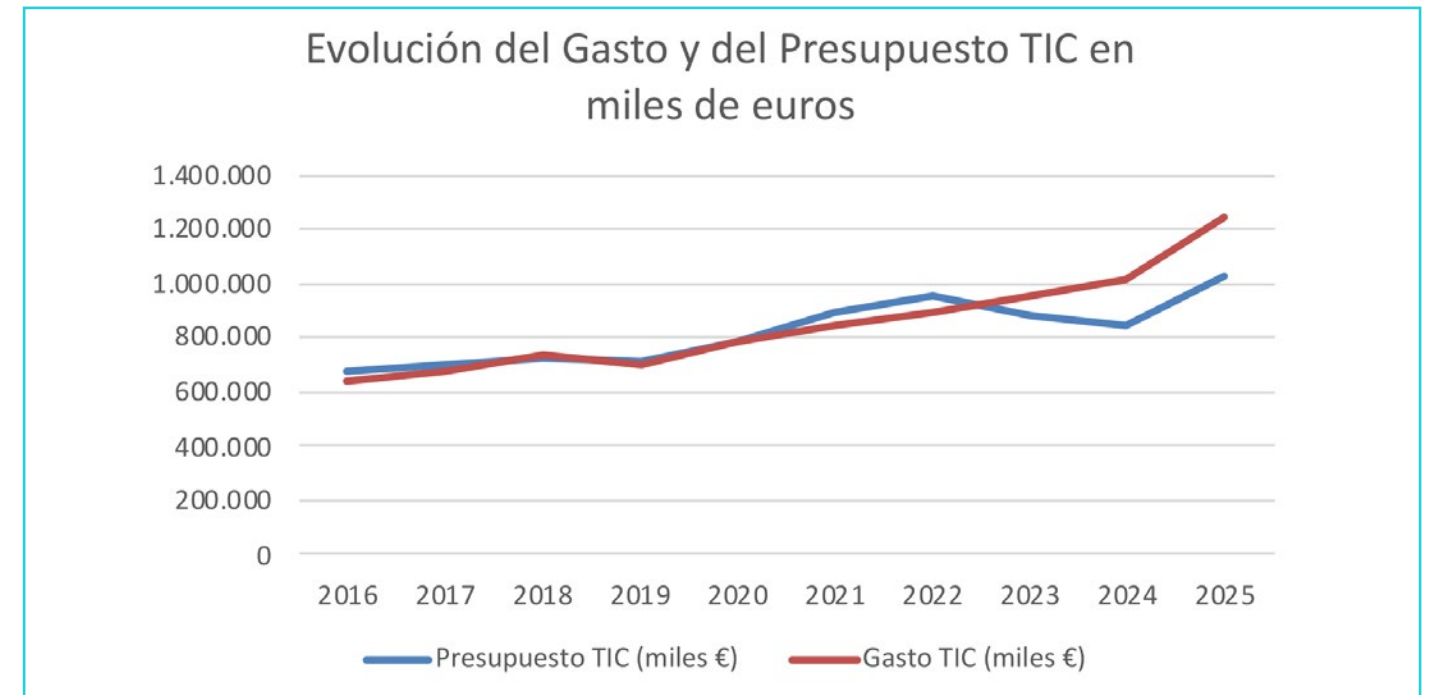
En la **Gráfica 3** se representa la evolución, a nivel nacional, del presu-

to TIC propio de las CCAA y del gasto TIC, donde se observa que en los últimos años el gasto es superior al presupuesto.

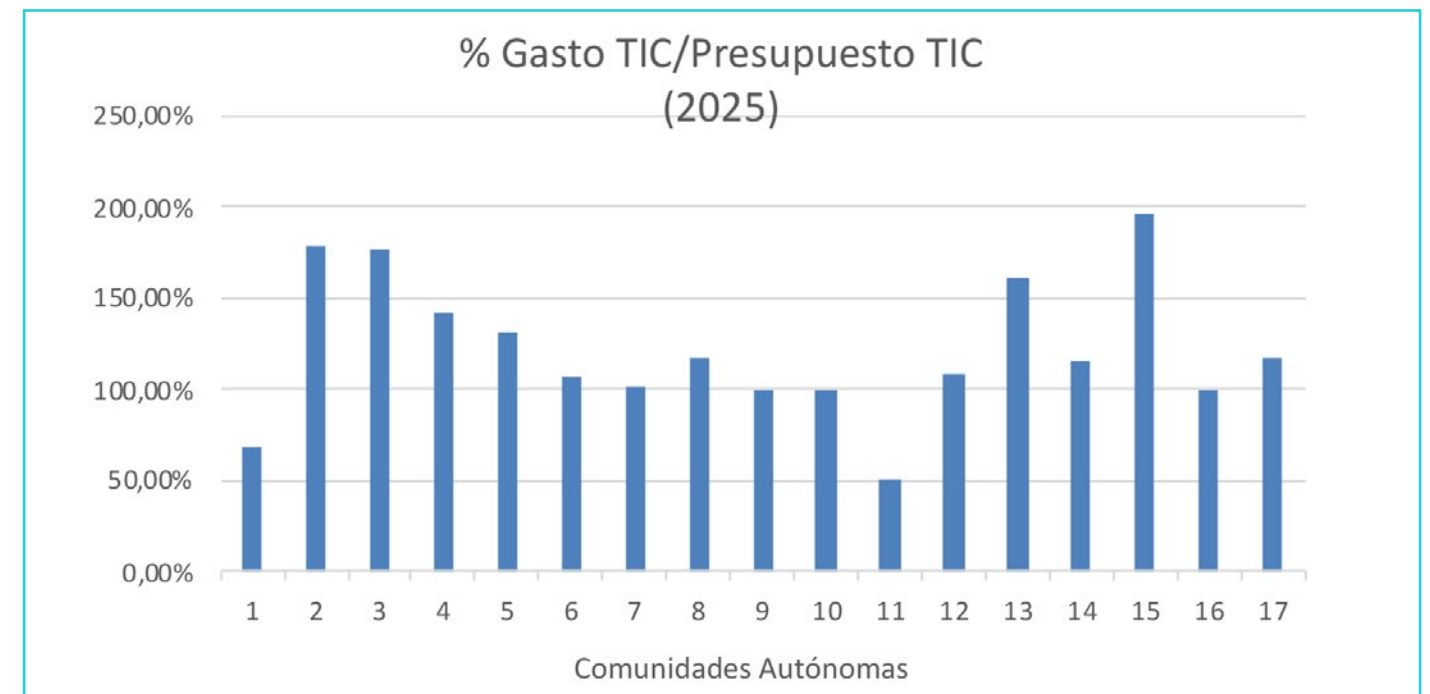
Al igual que ocurre con los presupuestos TIC también existe gran variabilidad en relación con los gastos TIC.

La **Gráfica 4** nos indica que, en el 2025, hay dos CCAA que gastaron menos del 70% del presupuesto propio disponible, sin embargo, hay cuatro CCAA que gastaron más del 150% del presupuesto propio inicial.

Gráfica 3: Evolución del presupuesto TIC frente al gasto TIC



Gráfica 4: Porcentaje del gasto TIC respecto presupuesto TIC



En relación con los presupuestos y gastos TIC, podemos concluir que la tendencia creciente de las inversiones (gastos) de las CCAA en TIC en salud a nivel nacional es positiva, pero para alcanzar unos niveles de inversión adecuados debe mantenerse esta tendencia en los próximos años. Para ello es necesario incrementar los presupuestos propios y/o conseguir financiación externa para proyectos estratégicos, pero teniendo en cuenta que luego hay que mantenerlos.

Recursos humanos dedicados en exclusiva a las TIC

Los RRHH son el motor de toda organización, son los que llevan a cabo sus avances y mejoras y son clave para lograr la innovación y la transformación de esta.

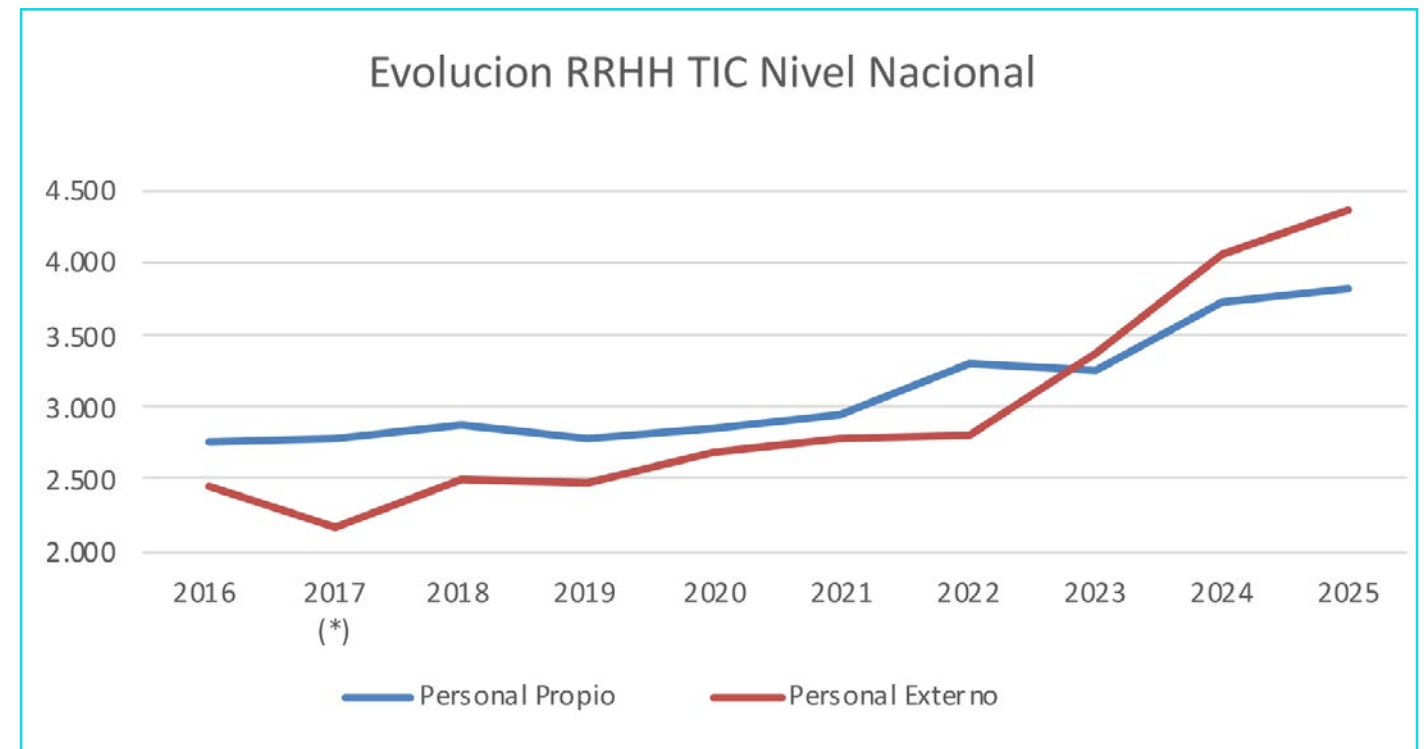
Los RRHH especializados en TIC son un pilar fundamental para la transformación digital del SNS.

La **Tabla 2** contiene, a nivel nacional, el número de RRHH propios y externos disponibles de los últimos diez años, donde comprobamos que en ese periodo los RRHH externos se han incrementado un 78,27% mientras que los RRHH propios, sólo se han incrementado en un 38,34%.

En la **Gráfica 5** se visualiza la evolución de los RRHH propios y externos.

En esta gráfica observamos que desde el 2023 el número de RRHH externos sobrepasa al número de RRHH propios. Esta situación puede deberse a tener que asumir la ejecución de proyectos colaborativos incluidos en los Planes de Transformación Digital de Atención Primaria y de Atención Digital Personalizada, financiados con fondos europeos

Grafica 5: Evolución de los RRHH dedicados a las TIC



asociados al Mecanismo de Recuperación y Resiliencia (MRR) y transferidos a las CCAA para su ejecución. No obstante, no parece lo más adecuado que en

el 2025 el personal externo alcance el 53,17% del total de RRHH TIC.

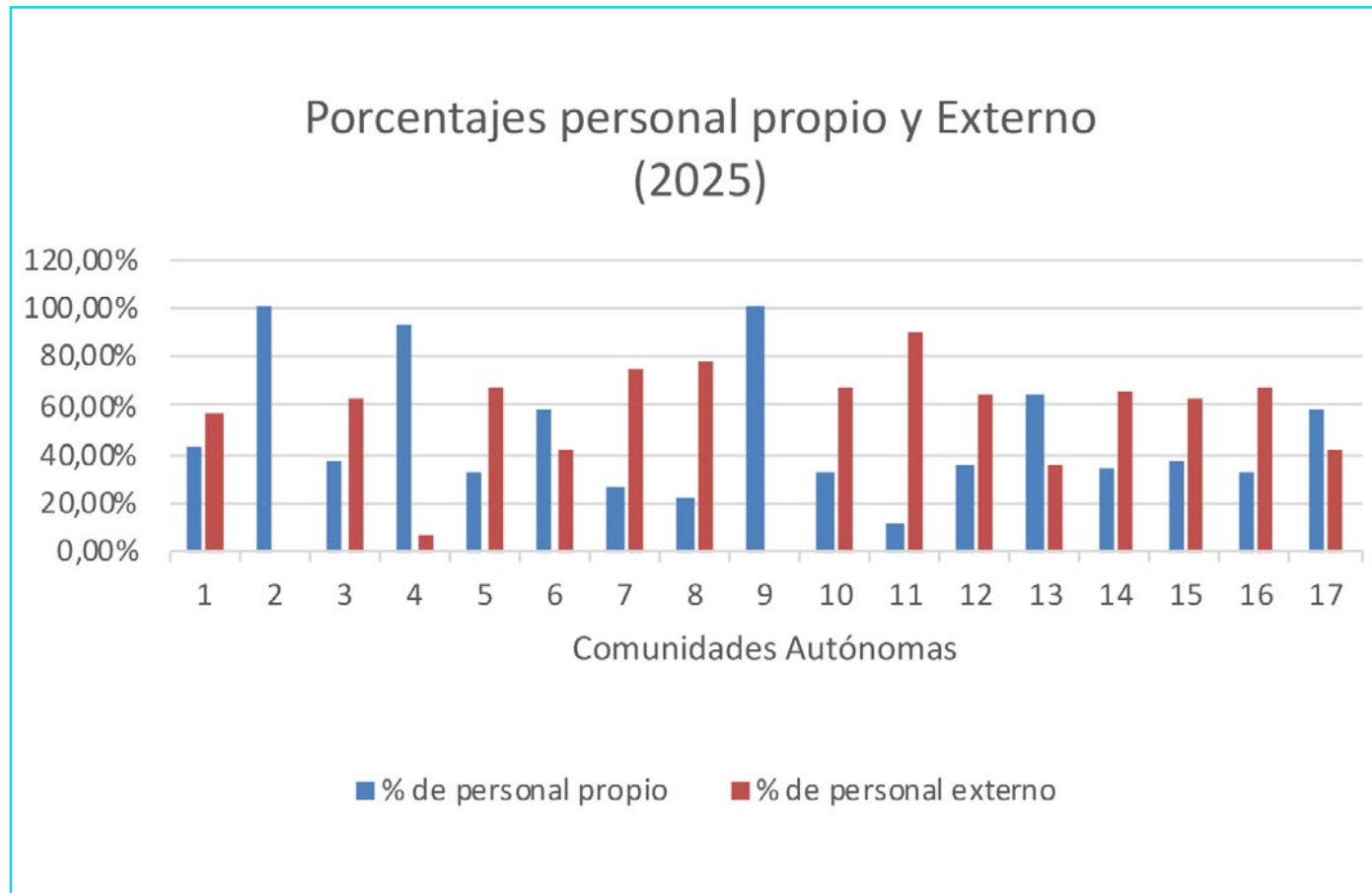
Además de los datos globales a nivel nacional, hay que tener en cuenta que

Tabla 2: RRHH dedicados a las TIC

Recursos humanos dedicados en exclusiva a las TIC	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Personal propio	2.762	2.777	2.880	2.793	2.845	2.962	3.308	3.261	3.724	3.821
Personal externo	2.453	2.161	2.489	2.476	2.689	2.790	2.798	3.370	4.073	4.373
Total	5.215	4.938	5.369	5.269	5.534	5.752	6.106	6.631	7.797	8.194

(*) Después de la publicación del ÍNDICE 2017, se detectó un error en el nº de RRHH tanto propios como externos, el error se subsanó en 2018.

Grafica 6: Porcentajes de personal propio y externo por comunidad autónoma



la proporción entre personal propio y personal externo no es homogénea en todas las CCAA, ni mucho menos, tal como nos muestra la **Gráfica 6**.

Sin entrar en consideraciones sobre las nuevas especializaciones necesarias (analítica de datos, bioestadística, inteligencia artificial, ciberseguridad, supercomputación o computación cuántica contempladas en el Plan España Digital

2025), podemos afirmar que los 3.821 profesionales TIC propios son a todas luces insuficientes para una organización como el SNS, en el que trabajan unas 730.000 personas, con aproximadamente 3.000 centros de salud, 465 hospitales y 575.000 puestos de trabajo (PC, impresoras, tabletas...).

Es muy recomendable que cuando finalicen los procesos de estabiliza-

ción de empleo temporal y consolidación de plazas que, en relación con el personal TIC, se están llevando a cabo en la mayoría de los Servicios de Salud, se emprendan medidas urgentes para incrementar los RRHH propios especializados en TIC. El ÍNDICE del 2025 refleja los efectos de los procesos de estabilización de empleo temporal y consolidación de plazas, ya que en el 2025 se ha producido una disminución del 23,15% del personal laboral, con respecto al 2024, y esta disminución es más significativa en el nivel A1 donde se ha reducido un 38,03%.

La seguridad de los sistemas de información

Si garantizar la seguridad de los sistemas de información (SI) es imprescindible en cualquier sector de actividad, en el sector salud es un factor crítico. La seguridad de los SI debe considerarse como un servicio asistencial más y como factor determinante de la calidad asistencial.

Aunque la mayoría de los incidentes de seguridad aún provienen de debilidades internas a las propias institu-

ciones, el sector salud, dada la repercusión social y económica que tiene, está en el punto de mira de los atacantes del exterior, los ciberataques. El impacto de los posibles ataques es variado; por una parte, existe el riesgo de una brecha de datos, afectando a la confianza de los pacientes, a la reputación del sistema sanitario, a las responsabilidades legales y financieras, etc. y, por otro lado, el riesgo a la discontinuidad del servicio, una caída o no disponibilidad de los SI puede resultar en un incidente grave para la continuidad asistencial de los pacientes.

A medida que los ataques a una organización evolucionan, se requiere que la capacidad de respuesta de la organización evolucione en la misma medida, es necesario un esfuerzo y una inversión permanente en seguridad, tanto en recursos humanos como técnicos. No es posible tener un servicio de salud de calidad si no se destinan los recursos adecuados para la protección de los sistemas de información que lo soportan.

La **Tabla 3** nos muestra un crecimiento continuo de los RRHH dedica-



dos a la seguridad de los SI, del gasto en seguridad y de la proporción de este gasto con respecto al presupuesto TIC, y nos dan idea de que, en estos últimos años, la importancia de la seguridad de los SI sanitarios está calando en los responsables de estos.

Desde el 2016 al 2025, el incremento de RRHH TIC (propios y externos) fue de 57,12%, mientras que los RRHH dedicados a la seguridad se incrementaron en un 250,00%. En ese mismo periodo el gasto TIC se incre-

mentó en un 93,99% y el gasto en seguridad se incremento en 369,57%. No obstante, a estos datos, y según la opinión de expertos en seguridad, los niveles de inversión y de recursos humanos dedicados a la seguridad siguen siendo bajos y no se corresponden con los riesgos que las vulnerabilidades en seguridad pueden acarrear en los sistemas de salud, por lo que se considera imprescindible continuar con la tendencia del incremento progresivo de los recur-

sos dedicados a la seguridad de los SI del SNS.

Conclusiones

Independientemente de que el ÍNDICE SEIS nos aporta mucha información sobre los avances producidos en la implantación de las TIC en el SNS, en este artículo hemos querido resaltar que, de los tres factores críticos analizados, dos de ellos no están resueltos de forma satisfactoria:

- Los RRHH TIC, insuficientes cuantitativa y cualitativamente.
- Los presupuestos TIC, que, a nivel nacional en 2025, sólo representan el 1,248%, con respecto al presupuesto sanitario.

Para finalizar, nos reafirmamos en el compromiso de la SEIS de mantener y evolucionar el ÍNDICE para que siga siendo un referente tanto a nivel nacional como internacional, que aporta una valiosa información sobre la implantación de las TIC en la sanidad pública española. **CW**

Tabla 4: Seguridad de los Sistemas de Información

Seguridad de los SI	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
RRHH en Seguridad (propios y externos)	59	61	60	67	99	106	111	142	198	207
Gasto en Seguridad en miles de €	10.568	12.918	16.512	20.407	16.242	20.532	26.471	26.986	37.039	49.624
% Gasto en Seguridad/Presupuesto TIC	1,57%	1,86%	2,27%	2,89%	2,07%	2,28%	2,76%	3,05%	4,37%	4,83%



IA y salud: por qué la infraestructura es el corazón de la medicina del futuro

Adela de Toledo, country manager de Everpure para España y Portugal

La inteligencia artificial (IA) ha dejado de ser una promesa de futuro para convertirse en el motor de una revolución sin precedentes en el sector sanitario. No hablamos solo de algoritmos; hablamos de una transformación profunda que está redefiniendo el cuidado del paciente, la investigación farmacéutica y la eficiencia de nuestros hospitales. Sin embargo, en esta carrera

hacia la medicina de precisión, a menudo olvidamos un elemento crítico: la IA es tan potente como la infraestructura de datos que la sustenta.

Desde Everpure, observamos cómo la capacidad de procesar volúmenes masivos de datos a velocidades increíbles está permitiendo abordar desafíos que hasta hace poco parecían inalcanzables. Pero, ¿dónde está impactando realmente esta tecnología?





1. Diagnóstico de precisión y detección temprana

La IA está entrenando algoritmos para detectar patrones en imágenes médicas (rayos X, TAC, RM) que el ojo humano podría pasar por alto. Un ejemplo paradigmático es la oncología, donde sistemas de IA ya predicen la aparición del cáncer de mama con años de antelación. Esta capacidad requiere sistemas de almacenamiento de alto rendimiento, como el *all-flash*, que permitan recuperar y procesar datos históricos de forma instantánea para el entrenamiento continuo de los modelos.

2. Aceleración en el descubrimiento de fármacos

Tradicionalmente, desarrollar un nuevo fármaco podía costar miles de millones y más de una década. Hoy, la IA está reduciendo el proceso de descubrimiento de cinco años a tan solo uno. Al analizar bases de datos moleculares inmensas,

los investigadores pueden predecir interacciones con una velocidad asombrosa. Pero esto solo es posible si la infraestructura garantiza una latencia mínima y una capacidad de procesamiento en paralelo masiva.

3. Hiperpersonalización del tratamiento

Gracias a la integración de la genómica y los datos de dispositivos *wearables*, estamos pasando de una medicina generalista a una hiperpersonalizada. La IA permite cruzar el historial médico con el perfil genético para recomendar tra-

tamientos específicos para cada individuo. Para gestionar esta complejidad multidimensional, las organizaciones sanitarias necesitan plataformas de datos que unifiquen silos y ofrezcan acceso inmediato a la información crítica.

4. Democratización del acceso mediante telemedicina

Los asistentes virtuales de salud y las plataformas de telemedicina potenciadas por IA están rompiendo las barreras geográficas. Estos sistemas no solo gestionan agendas, sino que realizan cri-

bados de síntomas y monitorizan constantes vitales en tiempo real, alertando ante cualquier cambio preocupante. Aquí, la disponibilidad y la seguridad del dato son innegociables.

El reto: una infraestructura 'AI-Ready'

La ambición de innovar en salud debe ir acompañada de una inversión en infraestructuras diseñadas para la era de la inteligencia de datos. En Everpure, a través de nuestra arquitectura Evergreen, ayudamos a los sistemas de salud a eliminar la deuda técnica y los silos de información.

La medicina del futuro no se construye solo en los laboratorios, sino en la capacidad de convertir datos brutos en conocimiento accionable. Solo con una base tecnológica sólida, ágil y escalable podremos garantizar que la IA no sea solo una herramienta brillante, sino un aliado que salve vidas de forma eficiente y sostenible. **CW**

Solo con una base tecnológica sólida, ágil y escalable podremos garantizar que la IA sea un aliado que salve vidas de forma eficiente y sostenible

Ciberseguridad sanitaria: la visión de Oesía y Nunsys para garantizar los datos y la continuidad asistencial

Miguel Ballesteros, responsable de Producto de Ciberseguridad de Grupo Oesía

La digitalización del sector sanitario es un camino que promete revolucionar la atención al paciente, la investigación y la gestión hospitalaria. Sin embargo, esta transformación trae consigo un desafío en materia de ciberseguridad. La convergencia de redes de tecnologías de la información (IT), tecnologías de la operación (OT) y el internet de las cosas médicas (IoMT) ha expandido la superficie de ataque, poniendo en jaque no solo la privacidad de los datos, sino la propia continuidad asistencial y la seguridad del paciente.

En este escenario, los enfoques tradicionales de ciberseguridad, a menu-

do basados en servicios gestionados genéricos, resultan insuficientes. La sanidad no necesita únicamente un vigilante, sino un sistema nervioso central tecnológico, capaz de entender el contexto, tomar decisiones inteligentes y actuar de forma automática para neutralizar amenazas y reducir la exposición al riesgo antes de que se materialice sin interrumpir la operativa clínica.

Con esta visión, y en el marco de un proyecto de Compra Pública Innovadora (CPI) financiado por INCIBE, se ha desarrollado un CyberSOC sanitario tecnológico, una iniciativa liderada por la empresa española Nunsys que va más





allá del concepto de servicio para consolidarse como una solución integral y soberana.

La propuesta se articula en torno a un ciclo cerrado de ciberseguridad: visibilidad, contexto, decisión, acción y aprendizaje. Este bucle no es solo una declaración de intenciones, es el método de un nuevo paradigma de protección. En su núcleo, encontramos dos tecnologías clave que operan en perfecta sinergia.

Por un lado, Sirena, la plataforma de Nunsys Group, actúa como la capa central de orquestación, correlación y gobierno del riesgo. Es el cerebro del CyberSOC. Sirena no se limita a agregar y correlacionar alertas, sino que las enriquece con contexto operativo, normativo (cumpliendo con ENS y NIS2) y de negocio. Su función es traducir el ruido técnico en información accionable y relevante para el CISO y el CTO, permitiendo una gestión dinámica del riesgo y orquestando la respuesta a incidentes y contribuyendo a la gestión proactiva del riesgo.

Por otro lado, OpenNAC Enterprise de Cipherbit (Grupo Oesía) funciona como los ojos y las manos de este sistema. Aporta una visibilidad profunda y continua de todos los activos conectados —desde un servidor hasta un ecógrafo o una bomba de infusión—,

creando un inventario preciso en entornos complejos de IT, OT e IoMT. Su capacidad de perfilado de precisión y análisis de tráfico de red permite detectar anomalías y comportamientos de riesgo. Pero su rol no termina en la visibilidad; también ejecuta la respuesta. OpenNAC Enterprise aplica

controles de acceso Zero Trust, realiza microsegmentación dinámica, especialmente relevante para dispositivos IoMT con limitaciones de parcheo o gestión y es capaz de contener amenazas automáticamente, siguiendo las directrices definidas desde Sirena

y aportando contexto operativo clave para su definición, todo ello sin afectar a la operativa clínica.

El valor diferencial de este proyecto se encuentra en esta integración que cierra el círculo de la ciberseguridad. Sin embargo, su principal fortaleza estratégica radica en su enfoque de tec-

nología soberana. Estamos hablando de un proyecto liderado por una empresa española, con una plataforma de orquestación de un integrador nacional y una tecnología de visibilidad y control de un fabricante español, Cipherbit, certificada en el Catálogo STIC 105.

Esta apuesta por la soberanía tecnológica es importante. Refuerza la seguridad de nuestro sistema sanitario, garantiza un alineamiento nativo con normativas nacionales y europeas como el ENS y NIS2, y contribuye a reducir la dependencia de tecnologías no europeas en un sector crítico.

La colaboración entre Nunsys y Cipherbit en este proyecto CPI marca un punto de inflexión. Demuestra que el futuro de la ciberseguridad sanitaria no pasa por añadir más capas de seguridad, sino por integrar de forma inteligente la visibilidad, la orquestación y la acción en una plataforma tecnológica cohesionada y soberana. Un modelo que será protagonista en el próximo XXIX Congreso Nacional de Informática de la Salud. **CW**

La propuesta se articula en torno a un ciclo cerrado de ciberseguridad: visibilidad, contexto, decisión, acción y aprendizaje



FOUNDRY