

El nuevo marco europeo de IA y Ciberseguridad:

Impacto en
las organizaciones sanitarias



relyens

GRUPO MUTUALISTA EUROPEO
SEGUROS Y GESTIÓN DE RIESGOS



sociedad
española de
directivos
de la salud

Hacia una Transformación Sanitaria Segura liderada por y para las personas

Inteligencia Artificial: innovación al servicio de la sanidad

La transformación digital está impulsando una nueva generación de proyectos tecnológicos en el ámbito sanitario, donde la IA se posiciona como un elemento clave para mejorar la asistencia, optimizar la gestión y favorecer una medicina más personalizada.

Este potencial debe desarrollarse bajo **un marco regulatorio que garantice un uso seguro**, ético y transparente de la tecnología, protegiendo los derechos, la privacidad y la seguridad de los pacientes.

En este ámbito, **Europa se ha consolidado como referente internacional** con un modelo regulatorio basado en la confianza y la innovación responsable.

Ciberseguridad: Un pilar imprescindible de la transformación digital

La creciente digitalización e interconexión del ecosistema sanitario amplía la superficie de exposición frente a las amenazas cibernéticas.

Un incidente de ciberseguridad puede comprometer la continuidad asistencial, la confidencialidad de la información clínica e, incluso, la seguridad del paciente, poniendo en riesgo el éxito de los proyectos de transformación digital.

Ante este escenario, **la regulación impulsa un enfoque coordinado** para fortalecer la resiliencia, la gestión del riesgo y la capacidad de respuesta de las organizaciones sanitarias dando garantía y solidez a las inversiones tecnológicas.

Liderazgo: para una transformación digital segura

Los proyectos de Inteligencia Artificial trascienden el ámbito tecnológico y requieren una visión estratégica que integre aspectos clínicos, organizativos, jurídicos, éticos y de seguridad.

La dirección sanitaria desempeña un papel esencial para coordinar a los diferentes profesionales implicados, establecer una gobernanza eficaz durante todo el ciclo de vida de los proyectos y asegurar el cumplimiento de un marco regulatorio cada vez más exigente.

El liderazgo se convierte así en un factor decisivo para implantar soluciones de IA que generen valor de forma segura, sostenible y centrada en el paciente.

La transformación digital de la sanidad exige integrar innovación, ciberseguridad y liderazgo bajo un marco regulatorio común que garantice una aplicación de la Inteligencia Artificial segura, confiable y centrada en el paciente.

El Hospital como Responsable de los proyectos IA

La entrada en vigor del Reglamento de IA europeo clasifica gran parte de los sistemas de IA sanitarios (diagnóstico, prevención, triaje y acceso a prestaciones) como de **alto riesgo**. Algunos puntos clave:

- **Obligaciones Directivas:** Los centros sanitarios deben realizar una **Evaluación de Impacto** en los Derechos Fundamentales antes del uso de sistemas de alto riesgo.
- **Supervisión Humana:** El hospital debe garantizar que la supervisión se realiza por personas con la competencia, formación y autoridad adecuadas; **la IA no sustituye el juicio clínico**, lo apoya bajo estricta vigilancia.
- **Transparencia:** Los pacientes, en determinados casos, deben ser **informados** sobre las decisiones tomadas o apoyadas por algoritmos.

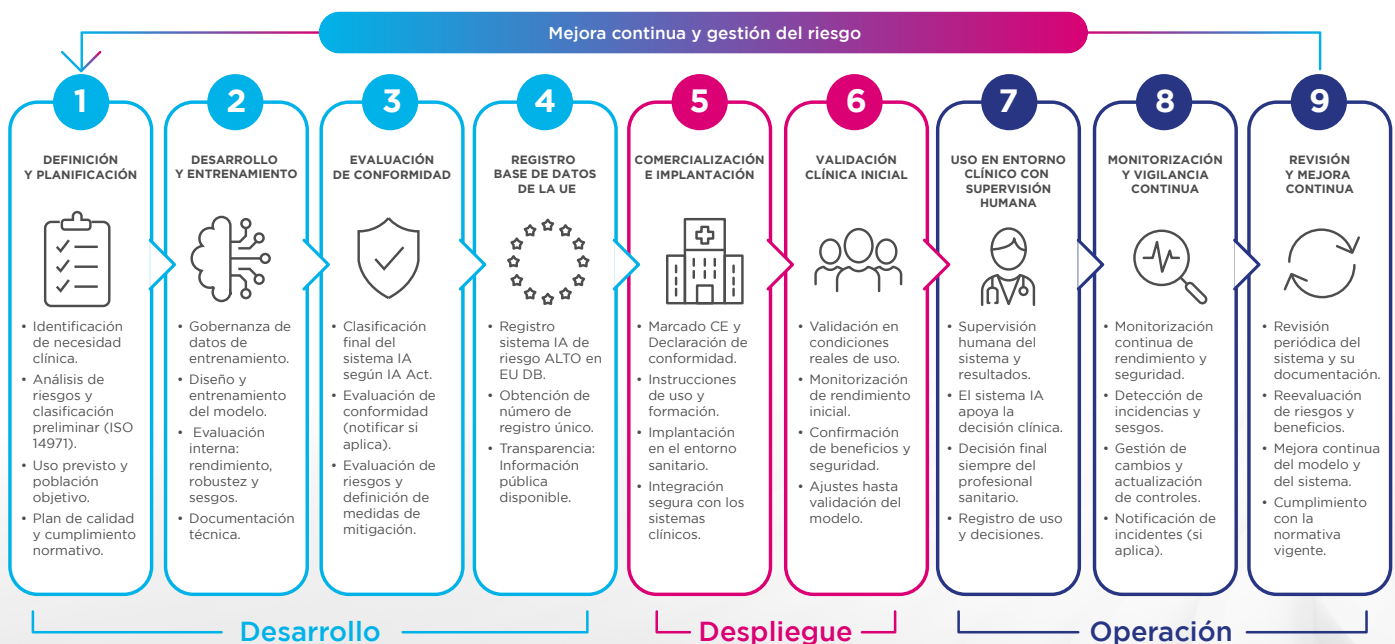
Requisitos como responsable del despliegue:

- Evaluación de impacto en derechos fundamentales.
- Facilitar un uso adecuado.
- Control de los datos de entrada.
- Vigilancia durante la operación de la IA y registro.

Requisitos como proveedor o fabricante:

- Garantizar conformidad del sistema IA.
- Sistema de gestión de la calidad.
- Documentación y registro.
- Registro europeo.
- Respuesta y comunicación de incidentes.

CICLO DE VIDA DE UN SISTEMA IA EN EL SECTOR SANITARIO



La ciberseguridad para la Resiliencia Operativa: Estrategia de Ciberseguridad del SNS

A mayor digitalización, mayor exposición a ciberamenazas, lo que puede implicar un alto impacto en la continuidad del servicio, en la información clínica e incluso en la seguridad del paciente.

En los sistemas de IA, además, existen **amenazas específicas**, como la manipulación de los datos o de los modelos, el acceso no autorizado a información sensible o los ataques dirigidos a alterar el funcionamiento del sistema.

Por ello, la ciberseguridad debe **integrarse desde el diseño** de cualquier proyecto tecnológico y constituye un requisito fundamental para generar confianza y garantizar un uso seguro de la IA en el ámbito sanitario.



Interrupción del servicio sanitario.



Brecha de seguridad de datos de salud.



Pérdida de confianza del ciudadano.

La ciberseguridad ha dejado de ser una opción técnica para convertirse en una condición contractual e indispensable en la digitalización de la sanidad.

Pilares de la estrategia de ciberseguridad del SNS

Asegurar la infraestructura con medidas de seguridad e investigación en nuevos riesgos.

Proteger la **privacidad** y garantizar la **interoperabilidad** de los datos sanitarios.

Crear un **entorno colaborativo** entre las CCAA que incremente la resiliencia conjunta y homogenice el nivel de madurez cibernética.

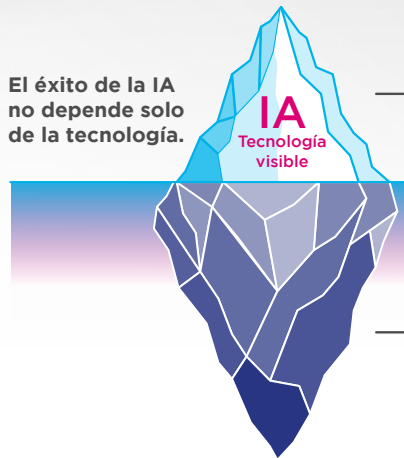
Garantizar la **confianza** del ciudadano en el SNS.

Objetivos de la estrategia de ciberseguridad del SNS



Liderazgo de una nueva cultura operacional como motor de la transformación

El éxito de la Inteligencia Artificial no depende únicamente de la tecnología, sino de la capacidad de la dirección para integrar personas, procesos, regulación y estrategia en torno a un objetivo común: generar valor para el paciente.



Lo que se ve...

- Algoritmos.
- Herramientas.
- Plataformas.
- Datos.

Lo que sostiene el éxito...

- Gobierno y calidad del dato.
- Ciberseguridad.
- Procesos y gestión de cambio.
- Cumplimiento normativo.
- Ética y supervisión.
- Liderazgo y formación.

La Inteligencia Artificial está redefiniendo la sanidad, tanto desde la perspectiva del servicio al paciente como de la propia gestión de los centros sanitarios.

Aprovechar todo su potencial requiere combinar **innovación** tecnológica, **gestión** del riesgo y **liderazgo** para impulsar una transformación segura, ética y sostenible.

Por sí misma, la IA no transforma una organización; amplifica la forma en que ya trabaja. La IA automatiza, consolida y amplifica lo que ya existe: si hay silos, reforzará los silos; si hay cultura de aprendizaje, acelerará la mejora.

Un nuevo liderazgo en sanidad

Gestión Basada en Valor:

- Cambio de una gestión basada en la ACTIVIDAD a una centrada en el VALOR.

Mejora y gestión de proceso:

- La IA debe ser una palanca de optimización de procesos, NO anclaje de sistemas obsoletos.

Nuevas Competencias Directivas:

- Saber formular las preguntas adecuadas.
- Liderar equipos multidisciplinares.
- Decidir en entornos de incertidumbre.

Management Humanista:

- La tecnología debe estar al servicio del talento.
- Vigilar que los algoritmos no generen injusticias o aumenten las desigualdades.
- Liderazgo para potenciar la participación, la mejora y la confianza.



La tecnología escala procesos, pero la cultura escala comportamientos

La transformación del sector sanitario mediante la IA y la digitalización exige un compromiso ineludible con la seguridad y la ética:

Responsabilidad en IA

El cumplimiento del Reglamento de IA no es solo una obligación legal, sino un **compromiso** con la transparencia y la supervisión humana para proteger los derechos fundamentales del paciente.

Ciberseguridad Estructural

Es un **requisito indispensable** para la continuidad asistencial. La resiliencia operativa debe formar parte de la planificación estratégica y financiera de todo centro sanitario.

Liderazgo Humanista

La IA solo será estratégica cuando ayude a **mejorar lo que de verdad importa**. El papel del directivo es asegurar un uso responsable y ético, donde la tecnología escale procesos, pero el liderazgo escale comportamientos orientados al bien común.

Cultura de Cambio

La verdadera competencia central de la era digital no es el manejo de herramientas, sino la capacidad de **dirigir organizaciones inteligentes** que aprendan de sus errores y pongan la tecnología al servicio del talento humano.

« Sin confianza no hay innovación. La regulación de la IA protege al paciente y hace posible una innovación segura, transparente y responsable »»

Juan Carlos Muria
Tarazón

PhD, CISA, CGEIT
Profesor ayudante doctor –
Assistant Professor
**Departamento de
Organización de Empresas
Universitat Politècnica de
València**

« La ciberseguridad deja de ser una opción técnica para convertirse en una **condición contractual indispensable** para cualquier entidad privada que colabore con el SNS »»

Laura Prats
Abadía

CISA, CISM
**Cyber Risk Manager
Relyens España**

« La competencia central no será saber usar una herramienta porque las herramientas cambiarán. **Será saber dirigir organizaciones inteligentes** »»

Conrado Domínguez
Trujillo

Coordinador SEDISA de IA en
gestión sanitaria.
Servicio Canario de Salud



Más información:

Webinar “El nuevo marco europeo de IA y Ciberseguridad”.
Acceso al webinar en el canal SEDISA YouTube: [VER AHORA](#)