



**MÁS ALLÁ DE LO DIGITAL:
CÓMO GARANTIZAR LA
CIBERSEGURIDAD EN
HOSPITALES**

Entelgy·Innotec
SECURITY

CONVERGENCIA IT/OT

El aumento de dispositivos conectados (*IoMT, Internet of Medical Things*, por sus siglas en inglés) en el entorno hospitalario hace necesario analizar la ciberseguridad del sector desde un punto de vista **ciberfísico**, más allá del ámbito digital (TI).

La ciberseguridad industrial (OT) es determinante en este espacio y tiene por delante retos que solo se solventarán con un trabajo de convergencia.



Sistemas ciberfísicos

Gestionados por **sistemas digitales** o que proporcionan algún **servicio** y pueden generar un efecto en las **personas**. Producen **información que se comparte** con los distintos servicios de un hospital.



Fallo en sector IT

La intrusión en un sistema digital deja en una **situación vulnerable** a las tecnologías utilizadas en el entorno hospitalario, que están conectadas entre ellas y se conectan a su vez con los sistemas digitales del hospital.



Fallo en sector OT

El fallo o intrusión en un equipo hospitalario puede provocar **problemas irreversibles en la salud** física del paciente: compromiso de marcapasos, máquinas de rayos X, máquinas de tomografía, robots de cirugía, etc.

ENTENDER LA PROBLEMÁTICA DEL SECTOR HOSPITALARIO



PLAN PARA GARANTIZAR LA SEGURIDAD EN HOSPITALES

