

Ciberseguridad en la sanidad: “La protección de datos de salud no puede considerarse únicamente cuestiones técnicas o regulatorias”

ASPE reclama reforzar la prevención, la gestión del riesgo y la capacidad de respuesta ante el aumento de las amenazas digitales

Según datos de la Agencia de la Unión Europea para la Ciberseguridad (Enisa), la sanidad ha sido el sector más afectado por incidentes significativos de ciberseguridad en Europa durante los últimos cuatro años consecutivos de los que existen datos, entre 2020 y 2023. Solo en 2023 se notificaron 309 incidentes de ciberseguridad que afectaron a organizaciones sanitarias europeas. A ello se suma que el 54% de los ataques registrados en el sector sanitario europeo corresponden a ransomware. Asimismo, los hospitales concentran el 42% de todos los incidentes notificados en el ámbito sanitario, lo que pone de manifiesto el especial interés que despiertan estas organizaciones para los ciberdelincuentes.

Ante estas cifras, la Alianza de la Sanidad Privada Española (ASPE) ha alertado sobre el crecimiento de las amenazas cibernéticas que afectan al ámbito sanitario y ha hecho un llamamiento a continuar reforzando la protección de los datos de salud y aumentar la capacidad de respuesta de las organizaciones sanitarias ante un escenario cada vez más complejo.

El 42% de todos los incidentes notificados sobre ciberseguridad en el ámbito sanitario se concentran en hospitales

En España, durante 2025 se gestionaron 122.223 incidentes de ciberseguridad, un 26% más que el año anterior, confirmando el crecimiento sostenido de las amenazas digitales que afectan a ciudadanos, empresas y organizaciones esenciales, según los datos del Instituto Nacional de Ciberseguridad (Incibe).

Para ASPE, estos datos evidencian la necesidad de mantener una vigilancia constante y seguir fortaleciendo las capacidades de prevención, detección y respuesta en un sector que desempeña una función crítica para la sociedad. “La tendencia es clara y no hay motivos para creer que pueda sufrir un cambio drástico. El sector debe estar preparado y trabaja a diario para ello”, explica José Manuel Baltar, presidente de ASPE.

El aumento de la relevancia de la ciberseguridad coincide con la transformación tecnológica de la sanidad privada española. “La transformación digital representa una enorme oportunidad para seguir mejorando la asistencia sanitaria, pero debe avanzar de la mano de una estrategia sólida de protección de la información y gestión del riesgo. Garantizar la seguridad de los datos de salud y la robustez de nuestras organizaciones es hoy una condición indispensable para seguir ofreciendo una atención de calidad y mantener la confianza de los pacientes”, añade el presidente de la patronal.

Según datos del sector, el 80% de los hospitales privados dispone ya de consulta digital implantada, mientras que el 50% realiza seguimiento digital de pacientes tras el alta hospitalaria y cerca del 30% ha comenzado a integrar información procedente de dispositivos wearables en sus sistemas de información. “La protección de los datos de salud y la seguridad de nuestros sistemas ya no pueden considerarse únicamente cuestiones técnicas o regulatorias. Son elementos esenciales para preservar la confianza de los pacientes y proteger uno de los activos más valiosos que gestionan las organizaciones sanitarias: la información de su salud”, señala Baltar.

Según la patronal, “la transformación digital debe avanzar de la mano de una estrategia sólida de protección de la información y gestión del riesgo”

La evolución tecnológica sanitaria también amplía la superficie de exposición a potenciales amenazas. Cada nueva herramienta digital, cada sistema conectado y cada intercambio de información sanitaria requiere mecanismos de protección capaces de garantizar la confidencialidad, integridad y disponibilidad de unos datos especialmente sensibles.

Desde ASPE se recuerda que la información sanitaria constituye uno de los activos más valiosos que gestionan las organizaciones sanitarias, tanto por su relevancia clínica como por la confianza que depositan los pacientes en los centros donde reciben atención. Destaca igualmente el papel decisivo que desempeñan los profesionales sanitarios y no sanitarios en la prevención de riesgos. La formación continua, la concienciación y el desarrollo de una cultura de seguridad sólida continúan siendo una de las herramientas más eficaces para reducir vulnerabilidades y prevenir incidentes.

Por ello, la patronal considera prioritario seguir avanzando en la implantación de modelos de gobernanza del dato, en la adaptación a los nuevos marcos regulatorios europeos y en la aplicación de medidas de seguridad que permitan afrontar los riesgos asociados a un entorno cada vez más digitalizado e interconectado. Asimismo, la patronal considera especialmente relevante la adaptación del sector a las nuevas exigencias derivadas de la directiva europea NIS2, así como el fortalecimiento de la seguridad en toda la cadena de suministro tecnológica y la colaboración entre organizaciones para compartir buenas prácticas y mejorar la capacidad de respuesta frente a amenazas emergentes.

Fuente: Ciberseguridad en la sanidad: “La protección de datos de salud no puede considerarse únicamente cuestiones técnicas o regulatorias”