

La UE endurece las exigencias para proteger la ciberseguridad del sector sanitario

Ciberseguridad sanitaria: La Directiva NIS2 y su impacto en la sanidad

La Directiva NIS2, que entrará en vigor el 18 de octubre de 2024, sustituye y amplía la anterior normativa europea sobre la seguridad de redes y sistemas de información. Uno de los principales cambios es la inclusión explícita del sector sanitario como parte de los denominados sectores esenciales, lo que implica la obligación de adoptar medidas de seguridad más rigurosas y reportar incidentes dentro de plazos estrictamente definidos.

Los hospitales, clínicas, fabricantes de material médico, industria farmacéutica y centros de salud pública estarán ahora sujetos a controles más exhaustivos, incluyendo autenticación multifactor, cifrado de datos, políticas de gestión de riesgos actualizadas y una mayor supervisión por parte de las autoridades competentes nacionales. Las exigencias de la Unión Europea en esta área están transformando la seguridad sanitaria.

Además, la directiva aumenta la responsabilidad de la alta dirección de las entidades sanitarias, que debe asumir un compromiso directo en la supervisión y aprobación de los mecanismos de ciberseguridad, transformando este asunto en un tema estratégico al más alto nivel corporativo.

La Unión Europea exige mayor protección en ciberseguridad sanitaria

En paralelo al despliegue de la Directiva NIS2, el Reglamento (UE) 2025/327 del Espacio Europeo de Datos de Salud (EEDS) ha entrado en vigor desde marzo de 2025, creando el primer marco legal común para el intercambio seguro y controlado de datos sanitarios electrónicos entre los países de la UE.

Este nuevo reglamento refuerza los derechos de los ciudadanos sobre sus historiales médicos digitales, permitiendo su uso no solo para atención sanitaria directa, sino también para investigación científica, innovación médica y formulación de políticas de salud. Para ello, se establecen requisitos técnicos y de ciberseguridad específicos para los sistemas de historia clínica electrónica, que deberán ser interoperables y seguros para garantizar la protección de datos sensibles.

El EEDS se desplegará progresivamente hasta 2034, e incluye medidas para facilitar el acceso transfronterizo a datos médicos, regulando también cómo la industria tecnológica y las administraciones sanitarias pueden utilizar esta información bajo condiciones estrictas de privacidad y seguridad de la información.

Evaluación sectorial y retos específicos de la ciberseguridad sanitaria

La Agencia de Ciberseguridad de la Unión Europea, ENISA, ha publicado recientemente el informe NIS360, que evalúa el nivel de madurez en ciberseguridad de los diferentes sectores cubiertos por la Directiva. Según dicho análisis, la sanidad muestra un nivel de preparación aún limitado, situándose por debajo de sectores como banca o energía.

Entre los desafíos más relevantes destaca la escasa colaboración entre los distintos actores del sistema de salud (públicos y privados, nacionales y autonómicos), así como la heterogeneidad de sistemas y plataformas tecnológicas utilizadas, que dificulta una respuesta coordinada ante ciberincidentes. Abordar estas limitaciones es esencial para cumplir con las exigencias de la Unión Europea.

El informe sugiere establecer guías sectoriales específicas durante la transposición de la Directiva NIS2 y fomentar sinergias entre sectores como TIC y sanidad, para impulsar prácticas comunes y soluciones interoperables.

España adapta su marco normativo a las exigencias europeas en ciberseguridad sanitaria

En el contexto nacional, España ya ha iniciado la transposición de la Directiva NIS2 a través de un proyecto de ley en tramitación en las Cortes Generales, que contempla la introducción de nuevas obligaciones para entidades críticas, incluidos centros sanitarios y proveedores tecnológicos asociados.

Además, comunidades como la Comunitat Valenciana han aprobado recientemente decretos para adaptar su política de seguridad de la información al nuevo marco europeo, implicando a las consellerias de sanidad, educación y justicia en la organización de la ciberseguridad, y otorgando a la DGTIC la responsabilidad central de coordinar la seguridad digital en la Generalitat y su sector público instrumental. La búsqueda de homogeneidad en la ciberseguridad sanitaria se está convirtiendo en un requisito esencial.

Este esfuerzo por homogeneizar normas y roles responde a la necesidad de alinear las políticas autonómicas con estándares comunes exigidos por la UE, particularmente tras la aprobación del Real Decreto 311/2022, el cual regula el Esquema Nacional de Seguridad y establece principios rectores, funciones, roles y niveles de responsabilidad para garantizar la protección de la información en las administraciones públicas.

Financiación e inversión en ciberresiliencia sanitaria

La Comisión Europea ha anunciado una inversión de 1.300 millones de euros entre 2025 y 2027, con el objetivo de impulsar el despliegue de tecnologías críticas como inteligencia artificial, infraestructuras digitales seguras y capacitación en ciberseguridad. Parte de estos fondos se destinará directamente a reforzar la resiliencia de infraestructuras esenciales como hospitales, considerados objetivos estratégicos desde el punto de vista cibernético.

Uno de los instrumentos clave será la creación de una “Reserva de Ciberseguridad” europea, orientada a responder de forma rápida ante incidentes graves en sectores vitales, incluyendo el sanitario. También se apoyará la adopción de servicios digitales de alta calidad y se fomentará la consolidación de una identidad digital segura para los pacientes dentro del Espacio Europeo de Datos de Salud.

Junto a las nuevas normativas, se están fortaleciendo los requisitos para las entidades que deseen operar como certificadoras de ciberseguridad en la UE. El nuevo Reglamento de Ejecución (UE) 2024/3144 modifica aspectos clave del esquema EUCC (esquema europeo de certificación), exigiendo conocimientos especializados, colaboración con laboratorios acreditados y una certificación piloto revisada como condiciones para actuar como organismo de evaluación autorizado.

Certificación, auditorías y competencias técnicas

Esto implica que los sistemas sanitarios y sus proveedores tecnológicos podrían verse obligados a someterse a auditorías por parte de entidades que cumplan con estándares rigurosos, lo que a su vez garantizará un mayor nivel de confianza tanto en productos como en servicios digitales utilizados en entornos clínicos.

También se están promoviendo programas de formación avanzada y desarrollo de talento en ciberseguridad, para asegurar que el personal en el sector sanitario cuente con las competencias necesarias para gestionar entornos digitales cada vez más complejos y expuestos.

Con estos cambios normativos y la inversión planificada, la UE pretende elevar el nivel general de ciberseguridad sanitaria y preparar al sector para los retos del entorno digital. Esto no solo incluye prevenir ataques, sino también asegurar la continuidad operativa y la privacidad de los datos en una era donde los sistemas de salud cada vez dependen más de lo digital.

La ciberseguridad sanitaria se perfila como un eje central de la transformación digital europea, con nuevas obligaciones legales, inversiones estratégicas y una arquitectura regulatoria común que unifica esfuerzos nacionales. El objetivo es claro: proteger a pacientes, profesionales y sistemas frente a amenazas crecientes en un entorno cada vez más interconectado. Comparte la información y así más usuarios conocerán la noticia.

Fuente: https://www.msn.com/

LINK DE LA NOTICIA

La ciberseguridad sanitaria se ha convertido en una de las principales prioridades para la Unión Europea, que está impulsando una batería de normas y medidas orientadas a reforzar la protección digital de uno de los sectores más críticos para la sociedad. Esta creciente preocupación ha dado lugar a exigencias normativas cada vez más estrictas, como la Directiva NIS2 y el recién aprobado Reglamento del Espacio Europeo de Datos de Salud (EEDS), cuyo cumplimiento será obligatorio para los Estados miembros en los próximos meses.