# El sector salud, objetivo principal de ciberataques: *Ransomware*, filtraciones de datos y el riesgo de pérdidas millonarias

**Juan Díez González**
*Responsable de ciberseguridad del sector de salud de INCIBE*

El estudio de la Agencia Europea de Ciberseguridad (*ENISA:TL2024*), sitúa al sector salud con un 4% de todos los ataques registrados en sectores estratégicos a nivel europeo, y dentro de este sector son los de tipo ransomware (22%) y filtraciones de datos (13%), y en muchas ocasiones, una combinación de ambos a la vez, los más frecuentes. En el caso del ransomware, los ciberdelincuentes toman el control de los activos de su víctima y exigen un rescate a cambio de la devolución de la disponibilidad del activo o a cambio de no exponer públicamente los datos incautados. A nivel mundial al 27% de las entidades que han sido víctimas de este tipo de ataque les ha supuesto pérdidas de casi 900.000 euros para la recuperación de la normalidad y en un 78% reconocen el pago de rescates superiores a los 440.000€ según el *estudio de Claroty*.

Estos estudios ponen de manifiesto que los ciberdelincuentes se están centrando en este sector motivado, principalmente porque les proporciona un beneficio económico importante debido a cuatro particularidades concretas de este sector:

- Alta criticidad de los servicios, principalmente los asistenciales. Cualquier parada de servicio puede suponer un fuerte prejuicio en la asistencia a pacientes, incluso con consecuencias vitales, lo cual crea una fuerte alarma social y daño reputacional por lo que los responsables sanitarios están dispuestos a ceder a posibles chantajes y pagar por recuperar "la normalidad".
- Alto valor de los datos que gestionan. Los datos de salud tienen un alto valor en el mercado negro, donde una historia clínica puede costar entre 30$ y 1.000$, mientras que una tarjeta de crédito vale entre 1 y 6$ de media (fuente Kaspersky).

- Heterogeneidad e hiperconectividad de sistemas y dispositivos. La transformación digital en el sector salud, favorecida por aumentos de inversión motivados por la situación vivida durante la pandemia, así como aparición de fondos europeos de financiación a este sector, han permitido incorporar gran cantidad de tecnología que ayuda en el diagnóstico, tratamiento y seguimiento de los pacientes, haciendo la vida más fácil a los profesionales de la salud. Se han incorporado nuevos dispositivos en infraestructuras asistenciales; pero, también, se cuenta con dispositivos que se lleva el paciente a casa y permite al profesional realizar un seguimiento de su evolución. Nuevos sistemas, a su vez, conviven con sistemas más antiguos, incluso legados, aumentando así la gestión de su operación y mantenimiento.

- Aumento del volumen y flujos de datos entre sistemas. No solo se ha incrementado el volumen y la heterogeneidad de datos que se generan, transmiten y procesan, sino que se interconectan entre sí, dentro y fuera de la propia organización. Toda esta complejidad requiere de mucho más esfuerzo para mantener actualizada y segura toda la infraestructura tecnológica y su información de forma constante, ampliando el perímetro de ataque para los cibercriminales.

Es fundamental que las organizaciones del sector salud (entre las que se encuentran los hospitales, clínicas, centros de salud, centros sociosanitarios, laboratorios, farmacias o empresas farmacéuticas, entre otros) comprendan que la tecnología es un catalizador y habilitador de negocio pero que trae consigo nuevos riesgos de negocio puesto que su correcta protección está directamente relacionada con la seguridad y privacidad del paciente.

## La tecnología como habilitador y reto en el sector salud

Por tanto, debe ser una prioridad mantener seguros los sistemas de información de salud, las redes y los dispositivos médicos porque son esenciales para la prestación de servicios de salud. También se debe garantizar la seguridad de información puesto que implica datos de salud de los pacientes y propiedad intelectual relacionada con la investigación e innovación médicas.

Estas entidades deben también conocer el marco normativo o regulatorio en materia de ciberseguridad que les es de aplicación en función de su actividad, los servicios o productos que provee o gestiona, así como la información que genera, procesa y almacena. Se prevé una renovación de esta normativa nacional motivada por la Directiva Europea NIS2, cuya transposición al ordenamiento jurídico nacional se espera para el último trimestre de 2024. El cambio es importante, puesto que será de aplicación para más entidades del sector, incluirá un seguimiento e inspección a las entidades sujetas a la normativa y un régimen sancionador estricto así como será más exigente con los niveles de cumplimiento de las medidas de ciberseguridad.

INCIBE ofrece en su web una sección dedicada al sector salud con información sobre el estado de la ciberseguridad y un catálogo de servicios gratuitos para ayudar a cumplir con normativas y necesidades de ciberseguridad, gestionados por INCIBE-CERT, el centro de referencia para operadores privados de sectores estratégicos. Además, proporciona guías prácticas y recomendaciones específicas para mejorar la protección frente a ciberamenazas.