

UNA INFRAESTRUCTURA SEGURA Y FLEXIBLE, CLAVE PARA LA TRANSFORMACIÓN DIGITAL DE LA SANIDAD

La digitalización está transformando la manera en que los hospitales prestan asistencia, gestionan sus recursos e impulsan la investigación. La inteligencia artificial abre nuevas posibilidades para analizar imágenes médicas, identificar patrones clínicos, anticipar necesidades asistenciales y mejorar la toma de decisiones. Sin embargo, estas innovaciones dependen de algo menos visible: una infraestructura tecnológica capaz de sostenerlas de forma segura, estable y eficiente. Sin sistemas fiables, datos accesibles y entornos preparados para ejecutar nuevas aplicaciones, el potencial de la IA difícilmente puede trasladarse a la práctica hospitalaria.



Miguel Pérez Colino

General Manager Linux Business Unit de SUSE

En España, uno de los grandes retos de la transformación digital sanitaria es modernizar los sistemas sin interrumpir servicios esenciales. Los hospitales conviven con aplicaciones desarrolladas durante años, dispositivos médicos con requisitos específicos y entornos tecnológicos que no siempre pueden actualizarse al mismo ritmo. A esto se suma la necesidad de proteger los datos de pacientes, mantener el cumplimiento de las políticas de seguridad y garantizar la continuidad de la actividad clínica. A medida que se incorporan nuevas cargas de trabajo basadas en IA, estos requisitos adquieren todavía más importancia.

La protección de estas infraestructuras es también una prioridad para las instituciones europeas. La Directiva NIS2 incluye al sector sanitario entre los sectores esenciales sujetos a requisitos reforzados de ciberseguridad. En paralelo, la Comisión Europea destinó en 2025 145,5 millones de euros a impulsar soluciones de ciberseguridad en las

administraciones públicas y los proveedores sanitarios, dentro de sus iniciativas digitales europeas.

La ciberseguridad, por tanto, no consiste únicamente en prevenir ataques. También implica conocer qué sistemas están funcionando, mantenerlos bajo soporte, controlar sus configuraciones y planificar las actualizaciones sin poner en riesgo procesos críticos.

En el caso de la IA hospitalaria, contar con una infraestructura bien gestionada es igualmente importante para garantizar la disponibilidad de los datos y las plataformas que necesitan las aplicaciones, así como para controlar los accesos y proteger la información clínica. El Hospital Clínic de Barcelona ha demostrado cómo abordar estos desafíos.





La complejidad de mantener sistemas críticos

Fundado en 1906, el Hospital Clínic es uno de los principales centros universitarios públicos de referencia en España. A lo largo de su evolución tecnológica, ha construido un entorno Linux heterogéneo, con distintas distribuciones y sistemas adaptados a las necesidades de sus aplicaciones.

Esta diversidad es habitual en organizaciones que incorporan nuevas tecnologías sin poder sustituir de inmediato las anteriores. El problema surge cuando la variedad dificulta obtener una visión global de la infraestructura, coordinar el mantenimiento o garantizar que todos los sistemas cuentan con soporte adecuado.

En el caso del Clínic, alrededor de 100 servidores funcionaban sin soporte empresarial. Algunos entornos, además, estaban vinculados a aplicaciones heredadas y dispositivos médicos cuya actualización debía planificarse cuidadosamente para evitar incompatibilidades.

La respuesta no consistía simplemente en renovar todos los sistemas. Era necesario encontrar un equilibrio entre seguridad, continuidad operativa y capacidad de evolución. Para ello, el hospital amplió su colaboración con SUSE, con el objetivo de centralizar la gestión de sus diferentes entornos Linux y recuperar la cobertura de soporte allí donde era necesaria.

Una gestión coordinada para reducir riesgos

El hospital incorporó SUSE Multi-Linux Manager para centralizar la administración de las distintas distribuciones Linux, integrándolo con Ansible, la tecnología de automatización que ya utilizaba. De este modo, la nueva capacidad de gestión se suma a los procesos existentes y facilita el trabajo diario del equipo de sistemas y operaciones.

La recuperación del soporte fue otro elemento fundamental. Mediante SUSE Multi-Linux Support, el centro pudo cubrir entornos críticos que habían alcanzado el final de su ciclo de soporte.

Esto permite gestionar un entorno diverso con un único punto de contacto para el soporte empresarial.

Asimismo, el hospital utiliza el soporte extendido de SUSE Linux *Enterprise Server* para disponer de mayor margen al planificar determinadas actualizaciones.

El resultado es una gestión más coordinada, en la que las decisiones de mantenimiento pueden adaptarse a las necesidades operativas del hospital, en lugar de depender exclusivamente de los ciclos de actualización de cada tecnología. Esta capacidad de evolución progresiva es especialmente relevante cuando la infraestructura debe responder tanto a las necesidades actuales de asistencia como a nuevas cargas de trabajo basadas en datos e IA.

La seguridad como parte de la operativa diaria

Mantener una infraestructura segura requiere convertir las medidas de protección en parte del trabajo cotidiano. Aplicar parches, comprobar configuraciones y detectar desviaciones respecto a los estándares establecidos son tareas esenciales, pero su ejecución manual puede consumir recursos y dificultar la supervisión de entornos amplios.

En el Hospital Clínic, la automatización facilita estas comprobaciones y ayuda a reducir la dependencia de procesos manuales. La integración de OpenSCAP permite evaluar las configuraciones de seguridad de los servidores y realizar auditorías para comprobar su adecuación a las políticas definidas.

Estas capacidades también ayudan a establecer una base operativa para abordar las exigencias de ciberseguridad y gestión de riesgos asociadas a marcos regulatorios como NIS2, sin que la adopción de una herramienta concreta garantice por sí sola el cumplimiento normativo.

La estabilidad es igualmente importante. Aproximadamente el 65 % de los servidores Linux del centro ejecutan SUSE Linux Enterprise Server y dan soporte a operaciones hospitalarias durante las 24 horas del día.

Esta continuidad también resulta esencial para las aplicaciones que necesitan acceder de forma fiable a datos clínicos y recursos de procesamiento. Si los sistemas operativos, las plataformas de datos o los entornos de ejecución

no están disponibles cuando se necesitan, las aplicaciones avanzadas pueden perder eficacia, con independencia de la calidad de sus algoritmos. Por eso, la seguridad, el mantenimiento y la disponibilidad deben formar parte de la estrategia tecnológica desde el principio.

Preparar la infraestructura para los próximos avances

La evolución tecnológica del hospital continúa con la adopción de servicios en la nube y arquitecturas basadas en contenedores. El centro está trasladando parte de sus cargas de trabajo a Amazon Web Services (AWS) y Amazon Elastic Kubernetes Service (EKS), utilizando SUSE Rancher Prime para facilitar su gestión.

El hospital también explora nuevas posibilidades para simplificar la gestión de contenedores y reforzar la seguridad y la observabilidad. En entornos híbridos, contar con herramientas de gestión coherentes ayuda a supervisar las cargas de trabajo y aplicar políticas

de forma coordinada, aunque los controles específicos deben adaptarse a cada aplicación y a sus requisitos clínicos y operativos.

En este escenario, principios como *zero trust* y la soberanía de los datos adquieren especial importancia. La innovación debe acompañarse de mecanismos que permitan controlar los accesos, supervisar los sistemas y mantener la información protegida durante todo su ciclo de vida. En el ámbito sanitario, esto exige prestar especial atención a dónde se almacenan y procesan los datos, quién puede acceder a ellos y qué garantías existen sobre su uso, de acuerdo con las obligaciones legales y las políticas de cada organización.

El caso del Hospital Clínic pone de manifiesto que la transformación digital no empieza necesariamente con una nueva aplicación. También requiere ordenar, proteger y modernizar la infraestructura que la hace posible. Porque avanzar hacia una sanidad más digital exige, ante todo, que la tecnología sobre la que se apoya sea segura, fiable y gestionable.

