



Claves para que la tecnología mejore la gestión sanitaria y la atención al paciente



El sector sanitario tiene que abordar una serie de retos a los que se enfrentan los C-Level. Con el fin de dar respuesta a sus inquietudes DirectorTIC ha llevado a cabo un debate en el que Luis González, director de Allied Telesis Iberia, Cristina Tello, directora de ventas de Fsas Technologies a Fujitsu company, Rodrigo Rebollar, responsable de estrategia en SDG Group y Martín Santandreu, consultor de Secure&IT. Estas son las principales conclusiones.

Inma Elizalde





En el coloquio hemos dado respuesta a estas inquietudes planteadas por los C-Level

- **¿Cómo optimizar el gasto de la tecnología de un centro sanitario teniendo en cuenta, por un lado, que el gasto necesario en tecnología es cada vez mayor y, por otro, que los ingresos están muy mermados por el escenario económico que vive el sector público?**
- **¿Cómo contener el coste cuando la superficie de ataque es tan alta y hay que contar con un gran número de soluciones para mitigar los riesgos asociados?**
- **¿Qué mejoras tipo “quick-win” en relación coste-beneficio podrían proponer con el uso de tecnologías en la relación con el paciente, la mejora de la experiencia de empleado o la eficiencia de procesos?**
- **¿En qué medida los dispositivos IoT están protegidos?**
- **Con una tecnología en constante cambio ¿qué estrategias se plantean para ayudar a los profesionales sanitarios a conseguir el máximo beneficio, y optimizar las prestaciones a largo plazo, teniendo en cuenta las barreras existentes en la Administración pública a la hora de contratar?**
- **El papel de la IA en la toma de decisiones del personal sanitario. Herramientas para la prestación inteligente del cuidado de enfermos, para la capacitación del personal de enfermería ante la escasez de talento, para la humanización entre paciente-médico y para que el médico pueda extraer el mayor valor de los datos para la toma de decisiones. También herramientas para alcanzar una mayor interoperabilidad para mejorar la integración en otros sistemas. Aplicación de la IA para la detección de la evolución del paciente en base a datos médicos.**
- **¿Cómo debería usarse la IA con contenido empresarial e información privada?**
- **¿Cómo conseguir una adopción efectiva de la IA, integrada en los procesos internos asistenciales y no asistenciales, con la regulación y el marco legal que afecta al sector sanitario? ¿Cómo gobernar la IA sin morir en el intento?**
- **¿Cómo se enfrentan los proveedores al nuevo marco regulatorio de la IA? ¿Cómo pueden ayudar al sector sanitario a simplificar la adecuación a la normativa?**
- **El proceso de encadenamiento al que nos están llevando ciertos proveedores cloud donde el poder lo tienen ellos.**
- **¿Cómo conseguir que las organizaciones sanitarias sean realmente *data driven*?**
- **¿Cómo incorporar nuevos perfiles profesionales relacionados con el dato para extraer el máximo rendimiento de la enorme cantidad de datos que se genera en el sector?**
- **Tips para mejorar la calidad del dato.**
- **¿Cuáles son los retos objetivos y los riesgos a los que se enfrentan los centros sanitarios?**
- **¿Cómo combatir las amenazas y la exposición que sufre el sector?**
- **¿Cómo convertirse en una organización ciberresiliente?**



- **Sistemas de detección de caídas no intrusivos.**
Sistemas de detección de errantes no intrusivos.
- **Tras una adquisición, ¿cuál es la mejor estrategia para acelerar la integración de las entidades adquiridas manteniendo la operativa? ¿Y a la hora de integrar nuevos centros, más allá de las adquisiciones, sobre todo a nivel de**

infraestructura?

- **¿Cómo conseguir una alta disponibilidad y redundancia de las comunicaciones de Internet?**
- **¿Cómo modernizar sistemas heredados sin interrumpir la atención clínica?**
- **¿Cómo financiar la innovación del sistema público y privado?**

- **La Junta de Andalucía está inmersa en la definición de un programa de aceleración del *time to market*, también en un programa de aseguramiento de la sostenibilidad digital y en la definición del programa de humanización digital, ¿cuáles serían las iniciativas digitales enfocadas a esos tres ámbitos?**

Optimización de costes

El sector sanitario tiene que enfrentarse a la necesaria inversión en tecnología, con unos ingresos mermados, al menos en el sector público, por lo que optimizar costes se ha convertido en una necesidad. Para lograrlo Luis González propone llevar a cabo un riguroso análisis de las necesidades reales del centro sanitario, con una planificación tecnológica basada en la compatibilidad y la durabilidad ante retos como la rápida obsolescencia de las tecnologías, como ocurre con los estándares del *wifi*. Por ello, recomienda optar por soluciones con retrocompatibilidad o planes de renovación progresiva. Cristina Tello coincide con González en la importancia de llevar a cabo una auditoría previa y detallada, especialmente en lo relativo a la gestión y clasificación

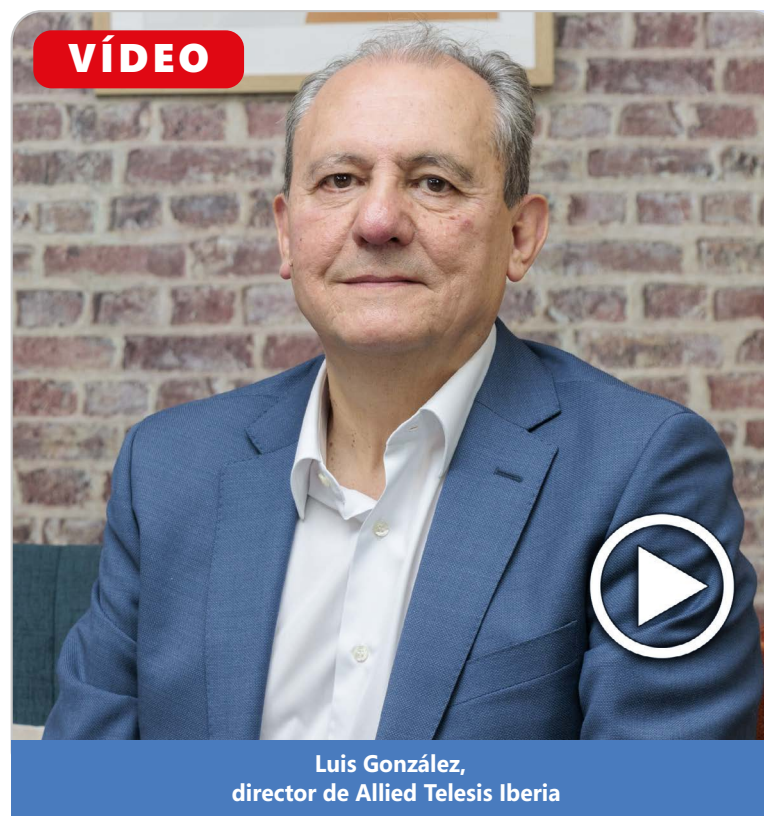




de los datos, al tiempo que pone el foco en los entornos híbridos como otra vía para la optimización. En su opinión es necesario contar con arquitecturas flexibles, contratos ajustables y tecnologías interoperables que permitan combinar soluciones en *cloud* con sistemas locales, siempre acompañadas de procesos de automatización y monitorización continua, recordando asimismo que la formación del personal y la gestión del cambio son elementos fundamentales.

Desde una perspectiva más orientada al análisis del dato, Rodrigo Rebollar incide en que el punto de partida pasa por entender qué se quiere lograr desde el negocio. Tras esto habría que definir con claridad la arquitectura tecnológica que mejor se adapte a las necesidades y capacidades de la organización. Construir una arquitectura sólida y priorizar los casos de uso en función del ROI, la escalabilidad y el impacto de los servicios son otros de sus consejos.

Apostar por mejoras "*quick-win*": acciones de bajo coste y rápida implementación que aporten valor real al paciente, al profesional sanitario y a los procesos internos es fundamental. En este sentido Rebollar apunta que muchas de estas mejoras ya son una realidad como las máquinas de registro automático, los sistemas que indican en qué sala estás o las plataformas donde puedes



Luis González,
director de Allied Telesis Iberia

consultar tus análisis y citas médicas, si bien advierte que el verdadero potencial está aún por explotar. "Antes de lanzarnos a soluciones avanzadas como la inteligencia artificial predictiva, hay un trabajo de base que todavía no se ha hecho: ordenar y estructurar los datos", dice. Aplicar analítica tradicional a datos como el consumo de suministros o la eficiencia energética, por poner algunos ejemplos, puede generar retornos inmediatos, sin necesidad de grandes inversiones, avanza. Cristina Tello respalda esta visión al señalar que no necesitamos ir al

"Para conseguir una alta disponibilidad y redundancia en las comunicaciones de Internet hay que contar con dos proveedores diferentes que permitan hacer redundancia a través de redes independientes"

último grito tecnológico para obtener mejoras significativas", para lo que pone ejemplos de tareas que podrían automatizarse con facilidad como la gestión digital de citas, los recordatorios automatizados o el seguimiento de pruebas médicas, tareas que en muchos casos todavía se realizan manualmente. Algo que puede redundar, en algunos casos, en los profesionales sanitarios.

El papel de la IA

La inteligencia artificial se perfila como uno de los elementos claves para transformar el sistema sanitario. En



el coloquio los expertos coinciden en que puede mejorar la calidad del cuidado, optimizar recursos y ayudar a paliar la escasez de talento en áreas críticas como la enfermería, pero Rodrigo Rebollar hace un llamamiento a la realidad. “Hay que entender que la IA no es magia. Es estadística, matemática y, sobre todo, dato”, apunta. “Sin una correcta estructuración y gobernanza del dato, cualquier intento de desplegar herramientas de IA será ineficaz”, sentencia, por lo que propone empezar por soluciones de analítica avanzada y modelos predictivos como los que ya permiten optimizar la gestión de listas de espera o el uso de quirófanos, antes de pensar en asistentes diagnósticos o algoritmos generativos. Tras esto elegir tecnologías ya disponibles: desde sistemas de recomendación para médicos y pacientes hasta asistentes conversacionales que ayuden al personal sanitario a consultar protocolos o resolver dudas en tiempo real. “Avances que pueden liberar tiempo del personal médico y mejorar la experiencia del paciente, siempre que se respete la privacidad y se cumpla con la normativa legal vigente”.

Cristina Tello va más allá al afirmar que “La IA puede transformar radicalmente la forma en que se toman decisiones clínicas”, pudiendo, además, jugar un papel fundamental en la formación del personal de enferme-



Cristina Tello,
directora de ventas de Fsas Technologies a Fujitsu company

ría, especialmente en un contexto de fuga de talento. “Las simulaciones de realidad virtual, las plataformas de aprendizaje automatizado y los sistemas de *feedback* inmediato podrían convertirse en aliados claves para acortar los tiempos de formación y garantizar la calidad asistencial”, asegura.

Luis González destacó el papel de la IA en la gestión de redes hospitalarias, señalando cómo las capacidades predictivas pueden anticipar fallos de infraestructura antes de que afecten al servicio. Y el uso de gemelos

“La ciberseguridad en el sector sanitario no debe medirse sólo en términos de retorno económico, también en indicadores de valor social”

digitales para simular y validar cambios en la red antes de su implementación real.

También ha puesto sobre la mesa la posibilidad de grabar y transcribir las consultas médicas con el fin de liberar al facultativo de tareas administrativas y devolver tiempo de calidad al paciente, aunque Martín Santandreu considera que es una propuesta que hay que analizar con mucho cuidado ya que la clave no está en cómo se graba la información sino en cómo se almacena y quién tiene acceso a la misma, por lo que habría que enmascarar los datos en entornos de desarrollo y pruebas para garantizar la confidencialidad sin comprometer la confidencialidad.



Continuando con cómo utilizar la IA sin poner en riesgo la información privada o estratégica, Martín hace uso de la frase “Cuando se usa un producto gratuito, el producto eres tú”, con el fin de aludir a la falta de control sobre los datos en modelos abiertos, por lo que insiste en que las organizaciones sanitarias tienen que definir una postura clara frente a la IA, estableciendo normas, formando a los usuarios y regulando el tipo de información que puede ser compartida. ¿Las claves? Clasificar correctamente la información, distinguiendo entre documentos confidenciales, de uso interno o público, con herramientas que permitan al usuario identificar y actuar en función de esa clasificación.

Rodrigo Rebollar pone en el centro del debate el dilema de si comprar o apostar por soluciones propietarias diseñadas a medida y alojadas en los propios entornos sanitarios, que permiten mantener el control sobre los datos y garantizar el cumplimiento normativo. “Esto posibilita integrar sus datos clínicos, operativos y estratégicos en modelos privados más seguros, auditables y transparentes”, añade.

Aquí nuevamente Cristina Tello vuelve a apostar por el modelo híbrido, combinando modelos preentrenados con soluciones cerradas, diseñadas para que los datos del cliente nunca salgan de su entorno. “El cliente



debe entender que sus datos son suyos, y que tiene una responsabilidad legal sobre ellos”, remarca. Sin olvidar que la regulación está avanzando en sectores como la banca, augurando que en breve se extenderá al ámbito sanitario.

Los ponentes también incidieron en la necesidad de educar y concienciar al personal para evitar errores humanos que conlleven a brechas de seguridad.

En cuanto a la integración efectiva de la IA en los procesos del sistema sanitario, tanto asistenciales como no

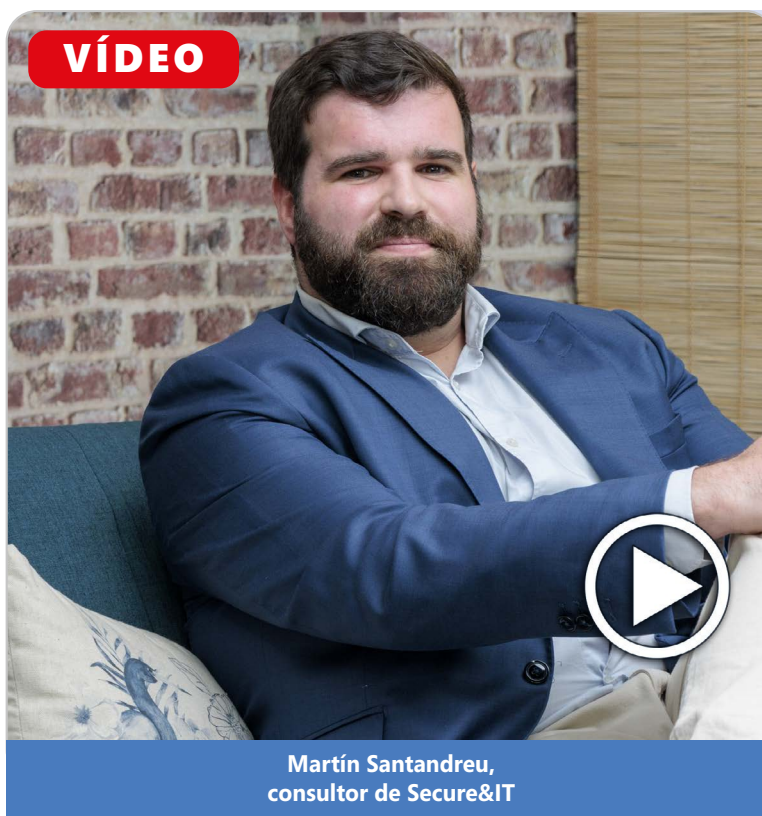
“El verdadero reto ya no es solo tener una estrategia del dato sino mantenerla viva y operativa en todo momento”

asistenciales, no puede hacerse de forma improvisada. Implica una transformación profunda que va más allá de la tecnología y exige una estrategia global de datos, seguridad, gobernanza y cumplimiento. Para Cristina Tello sin una arquitectura de datos es imposible implantar la IA de forma segura y eficaz. “Esta arquitectura tiene que ser capaz de integrar y gestionar la información de manera eficiente con sistemas que garanticen el control total sobre los datos críticos, especialmente en entornos *on-premises* o híbridos que permitan mantener la información dentro del dominio de la organización”. Uno de los pilares para lograr esta integración es la gobernanza del dato, que implica definir quién accede a qué, con qué permisos o bajo qué roles, evolucionando al mismo tiempo la tecnología.



Una transformación que tiene que ser responsabilidad directa del comité de dirección, apunta Tello.

Pero ¿cómo gobernar la IA sin morir en el intento? Contando con una estrategia integral que combine una correcta gestión de los datos, una definición de roles y accesos, la elección de soluciones tecnológicas que garanticen el control del entorno como modelos privados o híbridos, el cumplimiento riguroso de las normativas vigentes. Y, sobre todo, la implicación de la alta dirección. Los proveedores tecnológicos también se enfrentan a un escenario más complejo debido al nuevo marco regulatorio europeo. ¿Cómo pueden ayudar al sector sanitario a simplificar la adecuación a la normativa? Para Tello la clave estriba en acompañar al sector desde una perspectiva estratégica. El primer paso que se debe dar, recomienda, es comprender para qué se quiere aplicar la IA en el centro sanitario y desde ahí construir una estrategia que combine tanto la visión de negocio como el cumplimiento normativo. "Esto implica empezar por la clasificación del dato. Los proveedores pueden ayudar a liderar el proceso de clasificación de la información para identificar qué tipo de datos pueden estar en entornos de nube pública y cuáles deben mantenerse en entornos más seguros como pueden ser infraestructuras *on-premises* o nubes privadas, especialmente



Martín Santandreu,
consultor de Secure&IT

cuando hablamos de historiales clínicos, datos identificables o biomarcadores asociados a un paciente". Por ello vuelve a recomendar el modelo híbrido que permite combinar la flexibilidad y escalabilidad de la nube pública con la seguridad y el control total de entornos cerrados donde se almacenan los datos críticos. Si bien insiste en que no sólo hay que definir una arquitectura técnica, también hay que dotarla de mecanismos robustos de protección que incluyan control de accesos, gestión de identidades, cifrado, *tokenización* y un di-

"Las organizaciones sanitarias tienen que definir una postura clara frente a la IA estableciendo normas y regulando el tipo de información que puede ser compartida"

seño modular y segmentado que permita acotar riesgos en caso de incidentes. Todo ello sin olvidar que los proveedores tienen que asumir un rol activo en la formación y acompañamiento continuo de las organizaciones sanitarias, ya que la tecnología evoluciona más rápido de lo que las instituciones pueden adaptarse o los legisladores pueden regular.

Abordando la gestión del dato

Una gestión del dato que lleva a los responsables sanitarios a plantearse cómo conseguir que su organización se convierta en *data driven*. Para lograrlo Rodrigo Rebollar plantea tener claro en qué consiste esto, ya



Sistemas de detección

Luis González señala que desarrollar sistemas no intrusivos de detección de caídas o de comportamiento errante es un reto complejo, sobre todo porque hay que encontrar el equilibrio entre la seguridad del paciente y su privacidad. Subraya que el objetivo no es sustituir el contacto humano, como tener a una enfermera constantemente vigilando, sino apoyar su labor sin invadir la intimidad del paciente. Destaca que existen tecnologías como sensores o cámaras inteligentes que pueden captar ciertos patrones de movimiento o comportamiento y alertar automáticamente si algo no va bien, como una caída o una conducta anómala, sin necesidad de supervisión directa constante.

González enfatiza en que estos sistemas deben ser lo menos invasivos posible y actuar como apoyo invisible, permitiendo que el paciente mantenga su dignidad y privacidad mientras se garantiza su seguridad.



que hay muchas que no lo tienen claro. “Esto supone que el dato es un activo muy valioso, con dos implicaciones: hay que utilizarlo de manera efectiva, generar casos de uso, desarrollar modelos predictivos o procesos de optimización. Y, por otro lado, asumir que las decisiones dentro de la organización deben basarse siempre en datos, no en intuiciones”. Para avanzar hacia este modelo explica que el punto de partida pasa por contar con una buena estrategia del dato, analizando el nivel de madurez del mismo en las diferentes áreas del negocio. “Se hace una foto actual, se entienden los procesos del negocio, las necesidades analíticas, se identifican los problemas y a partir de ahí se plantea una visión futura alineada con la estrategia global de la compañía. Se diseña un plan para alcanzar esa visión mediante proyectos, casos de uso.

Y se construye un *roadmap* con prioridades bien definidas”, sugiere.

Rebollar reconoce que el modelo tradicional ya no es suficiente porque al ritmo al que avanza la tecnología no permite definir una estrategia de datos a varios años con un único proveedor y limitarse a implementarla. “Ahora el enfoque tiene que ser más dinámico y flexible”, comenta, por lo que propone crear una especie de oficina de datos o de acompañamiento continuo que trabaje de manera constante cerca del negocio, detectando nuevas necesidades, identificando oportunidades y evolucionado al mismo ritmo al que lo hacen las tecnologías y el entorno de negocio. Porque, tal y como relata; “El verdadero reto ya no es solo tener una estrategia del dato sino mantenerla viva y operativa en todo momento”.



Nube

A algunos directivos del sector sanitario les preocupa el proceso de encadenamiento al que les llevan ciertos proveedores *cloud* en el que ellos tienen el poder. Ante esta situación Cristina Tello considera que “Si les das el poder, lo tienen ellos, lo que se traduce en una pérdida de soberanía sobre el dato y un incremento progresivo e incontrolable de los costes. Con el incremento exponencial del dato en sanidad, donde la IA se está utilizando para automatizar tareas diagnósticas o asistenciales, se corre el riesgo de acabar pagando más por almacenar la información que por procesarla”, asegura. Tello aboga por soluciones como el almacenamiento en frío para información que no requiere acceso inmediato y permite no pagar costes extra cada vez que necesitas acceder a esos datos. Para la ejecutiva la solución pasa por diseñar arquitecturas híbridas y *multicloud* que aporten flexibilidad y capacidad de negociación, diversificando proveedores, evitando la dependencia de uno solo. También recomienda utilizar contenedores, estándares abiertos, orquestadores y herramientas de automatización para asegurar que los datos pueden moverse fácilmente entre entornos y que la compañía tiene control real sobre su infraestructura, al tiempo que insiste en que “hay que pensar siempre en la portabilidad del dato y en una gobernanza sólida que permita gestionar su ciclo de vida, sin quedar atrapado por decisiones técnicas que después no se pueden revertir”.

A todo ello Rodrigo Rebollar añade una estrategia de *FinOps* que permita a las organizaciones saber qué están contratando, qué están usando y el coste real de mantener sus soluciones en la nube, lo cual requiere trabajar con personas que conozcan bien el entorno *cloud*, que puedan garantizar que la empresa obtiene lo que necesita al menor coste posible.

Incorporar nuevos perfiles profesionales relacionados con el dato, con el fin de extraer el máximo rendimiento de la ingente cantidad de datos generados, no pasa

sólo por fichar *data scientist* sin más, confiesa Rebollar. “La clave está en enlazarlo con una estrategia del dato sólida. Hay que pensar en qué situación se encuentran,

hacia dónde quieren ir y en función de esto qué perfiles necesitan y cómo van a cubrir esas necesidades, porque en algunos casos, se pueden cubrir internamente. Esto irá cambiando a medida que vaya mejorando el nivel de madurez en la gestión del dato dentro de la organización”, prosigue.

El ponente señala que están viendo en el sector sanitario que al, ser un entorno poco maduro, muchas veces no compensa fichar a esos perfiles de manera interna. Además, suelen tener un coste elevado y se encuentran aislados dentro de la estructura de la compañía, sin un ecosistema que los potencie, reconoce. “No basta con perfiles técnicos, también se necesitan perfiles funcionales como los *data translator* que entienden tanto la tecnología como negocio y permiten conectar ambas”. Y, a la hora de mejorar la calidad del dato, Rodrigo Rebollar aporta algunos consejos: Al introducir los datos muchos se meten manualmente a través de los sistemas informáticos por parte de médicos y enfermeras, trabajo que no les corresponde, por lo que aconseja mejorar estos procesos de entrada de datos. Una vía de mejora pasaría por utilizar tecnologías de lectura de documentos como el OCR. También apoyarse en herramientas de procesamiento de texto o automatización de la gestión documental. Esto, además, reduce errores, añade.



Por otro lado, insiste en la importancia de analizar en qué tipo de información se está trabajando, priorizando la más crítica para la organización y, sobre esos datos claves, realizar acciones proactivas como testeo continuo análisis de calidad y detección temprana de problemas, para poder corregirlos lo antes posible.

Ciberseguridad

Por otro lado, en un escenario en el que los ciberataques se multiplican y la superficie de exposición tecnológica de los centros sanitarios crece sin cesar, la ciberseguridad se convierte en una prioridad indiscutible. Sin embargo, como señala Martín Santandreu, la solución no pasa por desplegar soluciones indiscriminadamente, sino por priorizar. “Lo primero que debe hacer cualquier organización es un diagnóstico claro de su situación en materia de ciberseguridad”, explica. “Ese diagnóstico se traduce habitualmente en un plan director de seguridad, una hoja de ruta que permite evaluar el estado actual, definir objetivos a medio y largo plazo, y establecer una jerarquía de prioridades en base a la criticidad y el impacto de cada riesgo”, especifica. Santandreu también defiende la utilidad de realizar análisis de riesgos continuos, más enfocados al día a día de la organización, que permitan adaptar las estra-

Dispositivos

La proliferación de dispositivos conectados ha transformado radicalmente el funcionamiento de hospitales y centros de salud. Sin embargo, esta revolución digital viene acompañada de una amenaza silenciosa: la falta de protección de los dispositivos IoT. Dispositivos muy sofisticados, en algunos casos, tal y como destaca Luis González, que carecen de los recursos necesarios para protegerse frente a ataques desde la red. Para mitigar estos riesgos defiende que sea la propia infraestructura de red la que actúe como primera línea de defensa, implementando mecanismos como la autenticación por dirección o segmentaciones específicas que impidan que un fallo en un dispositivo comprometa todo el sistema. Martín Santandreu confirma que la situación general, tanto en el ámbito privado como en el público, es de desprotección. “La raíz del problema está en que los dispositivos IoT operan entre IT y OT y muchas veces no está claro quién es responsable de su seguridad. Esa indefinición hace que queden fuera de muchas estrategias de ciberseguridad”, denuncia. No obstante, comenta que la Ley de Ciberresiliencia obliga a fabricantes de hardware y software conectados a cumplir con requisitos específicos de seguridad. Además, en el entorno europeo, los datos médicos están clasificados como sensibles dentro del Reglamento General de Protección de Datos, lo que implica la aplicación de medidas de seguridad reforzadas, incluyendo aspectos técnicos de ciberprotección. También recuerda que el Esquema Nacional de Seguridad, inicialmente diseñado para administraciones públicas, se ha ampliado en su última revisión para incluir a todos los proveedores que trabajen con información pública, lo que impacta en el entorno sanitario. A nivel industrial, apunta a normativas como la IEC 62443, orientada a la ciberseguridad de sistemas industriales, y a certificaciones como la ICSF 2021, que empiezan a marcar estándares de referencia en este ámbito, por que “lo que antes era una recomendación, ahora empieza a ser una exigencia legal”.



Estrategias para optimizar las prestaciones a largo plazo

En un entorno tecnológico cada vez más cambiante y con limitaciones estructurales propias de la Administración pública, una de las grandes preguntas que se hacen los expertos es cómo garantizar que el personal sanitario pueda aprovechar al máximo las herramientas digitales disponibles. El reto es doble: mejorar la formación y experiencia de los usuarios, y al mismo tiempo superar las rigideces normativas y de contratación del sector público. Para Luis González la clave está en automatizar al máximo los procesos, con sistemas de red resilientes, adaptables, inteligentes y proactivas. Y es que, tal y como explica, “Una red moderna tiene que informar con claridad de lo que ha sucedido para evitar fallos encadenados o reincidentes. Pero más allá de la capacidad de recuperación técnica, su propuesta pasa por soluciones “plug & play” que permiten que un dispositivo nuevo se conecte, se identifique y recupere automáticamente su configuración, incluso el sistema operativo, sin intervención especializada. “Esta automatización también mejora la continuidad del servicio, reduce los tiempos de inactividad y alivia la carga operativa en instalaciones donde el personal de IT brilla por su ausencia. Un factor especialmente relevante en hospitales comarcales o centros de atención primaria de zonas rurales”, argumenta.

tegias a un entorno en constante evolución, especialmente marcado por el auge de la inteligencia artificial. “La seguridad total no existe, advierte, pero sí se puede y se debe saber qué riesgos se asumen y cuáles no. Es esencial saber dónde están los puntos vulnerables y actuar en consecuencia”, subraya.

Desde una perspectiva más amplia, Cristina Tello apunta a la necesidad de integrar la ciberseguridad dentro de una visión de continuidad de negocio, ya que con-

sidera que ,en entornos críticos como la sanidad pública, no basta con responder ante un incidente: hay que ser capaces de recuperar sistemas en menos de 72 horas, contar con infraestructuras redundantes, planes de contingencia reales y mecanismos automatizados que clasifiquen y protejan los datos más sensibles. La directiva apunta, una vez más, a la importancia de la hibridez también en la seguridad, combinando recursos locales con soluciones en la nube y optimizando

licencias, al tiempo que observa que la ciberseguridad en el sector sanitario no debe medirse sólo en términos de retorno económico, “también en indicadores de valor social, como la mejora del servicio al paciente o la reducción del estrés del personal sanitario”.

Luis González no quiere dejar pasar por alto una realidad: “Mchos de los ataques no vienen del exterior sino de las malas prácticas internas, con el usuario como principal punto de entrada del riesgo”, por lo que además de mejorar las herramientas, defiende el uso de sistemas ya existentes para contener amenazas desde dentro de la red, a través de la automatización de respuestas y el confinamiento inmediato de dispositivos sospechosos mediante los elementos de red, sin inversiones adicionales en hardware. En definitiva, “reforzar lo que ya se tiene, mejorar la supervisión y concienciar a todos los usuarios del sistema”.

Martín Santandreu destaca que los centros sanitarios actualmente se enfrentan a tres grandes objetivos: deben garantizar en todo momento la confidencialidad la integridad y la disponibilidad de la información. Sobre la confidencialidad señala que los datos de salud son de los más sensibles, según la legislación española y europea y, por tanto, protegerlos es fundamental. En cuanto a la integridad explica que cualquier pérdida



o modificación de la información médica puede tener consecuencias graves, no solo legales sino también clínicas, porque si una persona necesita atención urgente y su historial está alterado o no accesible, puede derivar en errores de diagnóstico o tratamientos inadecuados. Y la disponibilidad es clave porque si el sistema no está operativo cuando un paciente llega a urgencias, el impacto puede ser inmediato y muy serio.

Para abordar estos retos propone contar con un sistema de gestión de la seguridad de la información integral que abarque tanto medidas técnicas como estrategias organizativas. En la parte técnica menciona la segmentación de redes, la gestión de vulnerabilidades y otras herramientas que forman parte de la protección operativa, al tiempo que insiste en que en la parte estratégica la dirección esté totalmente implicada en la toma de decisiones relacionadas con la seguridad y la gestión de los datos.

Santandreu pone el foco también en la importancia de la continuidad de negocio ya que eventos como el apagón, el COVID o Filomena demostraron que muchas organizaciones no estaban preparadas. Por ello propone contar con planes específicos para diferentes escenarios como la indisponibilidad del personal, de las telecomunicaciones o de los suministros críticos. Y, por

Sistemas heredados

A la hora de modernizar sistemas heredados sin interrumpir la atención clínica, Cristina Tello estima que uno de los errores más frecuentes que están cometiendo las organizaciones sanitarias es intentar subir a la nube los sistemas *legacy* tal y como están, como si se tratara simplemente de un cambio de ubicación. “La clave está en adoptar un enfoque gradual que parta de una evaluación cuidadosa de los sistemas actuales y de los procesos internos. Muchos de estos procesos fueron definidos hace años y ya no responden a las necesidades actuales, por lo que resulta absurdo replicarlos sin analizarlos ni actualizarlos. Esta revisión permite identificar qué puede ser mejorado, transformado en microservicios más ágiles y replicables, y qué se puede optimizar para que todo el proceso de modernización sea mucho más eficiente”, declara.

En este proceso es fundamental realizar un análisis de requerimientos, entender el cumplimiento normativo, priorizar los módulos críticos que afectan directamente la atención clínica y prever los aspectos de seguridad y legales. Tello sugiere que, para lograr una modernización sin interrupciones, se debe adoptar una estrategia híbrida en la que los datos sensibles se mantengan *on-premise* o en nubes privadas, mientras que las funcionalidades no críticas se desplieguen en nubes públicas, donde se pueden escalar más fácilmente.

Una parte crucial de su enfoque es el uso de entornos *sandbox* y pilotos de prueba controlados. Además, destaca que los nuevos sistemas deben ejecutarse en paralelo con los heredados durante un tiempo prolongado. “Esta coexistencia garantiza que, en caso de fallo del sistema nuevo, el antiguo sigue funcionando y no hay impacto en la atención. Y lo más importante: migrar funcionalidades, no máquinas. Cada funcionalidad se mueve de forma ordenada, en función de su criticidad, minimizando riesgos”.

Cristina Tello también enfatiza en que la descomposición en microservicios y contenedores no solo facilita la migración progresiva, sino que permite desplegar los sistemas en diferentes entornos sin depender de un único proveedor, algo que aporta agilidad, portabilidad y una mejor gobernanza tecnológica.



Financiación

Ante la pregunta de cómo financiar la innovación del sistema público y privado, Cristina Tello señala que resulta complicado. “El enfoque debe centrarse en áreas como la medicina preventiva, la genómica y la imagen avanzada, donde ambos sectores puedan beneficiarse mutuamente”, observa. “El sector público aporta la masa crítica suficiente de datos y el privado puede aprovechar esos datos anonimizados para generar valor y, a cambio, ayudar a financiar la innovación, ya que los recursos económicos no son infinitos”, indica, al tiempo que aconseja apostar por modelos de pago por resultados y mecanismos de cofinanciación que permitan establecer acuerdos entre ambos sectores. “Otra vía es la creación de infraestructuras de datos robustas y seguras que funcionen como un servicio, donde la medicina pública pueda ofrecer datos anonimizados de gran valor a empresas interesadas en extraer conclusiones útiles para innovación, siempre cumpliendo con las normativas de privacidad y protección de datos”, propone. “Estas estrategias requieren pensar en modelos híbridos”, recuerda.

supuesto, ante ciberataques que muchas veces son el origen del resto de problemas.

Luis González, por su parte, aboga por mentalizarse sobre la importancia de exigir certificaciones en los productos que se integran en los sistemas sanitarios, ya que muchas veces “se elige una solución por ser más barata pero no se evalúa si realmente cumple con los estándares de seguridad necesarios”. Recuerda que el precio de un producto no es solo el hardware, también las licencias, los protocolos y las garantías que lleva detrás. Algunos fabricantes eliminan costes ignorando estos factores y

eso puede suponer un riesgo, menciona. Y pone como ejemplo los *firewalls*: “No basta con tener uno, hay que asegurarse de que está certificado y que cumple lo que promete. Para eso existen laboratorios independientes que lo validan”. También recomienda que los cifrados estén certificados por organismos oficiales y no fiarse solo de lo que diga el *datasheet* del producto. Asegura que muchas veces lo que parece una pequeña diferencia técnica puede convertirse en un gran problema en el funcionamiento de una organización, sobre todo si hablamos de entornos críticos como el sanitario.

A la hora de combatir las amenazas, Martín Santadreu explica que lo más importante es contar con una gestión integral de la seguridad que se despliegue en todos los niveles. Insiste en que no basta con implementar medidas técnicas, también hay que estar preparado ante una posible interrupción operativa y eso pasa por analizar los procesos, identificar los más críticos, definir los tiempos de recuperación para cada uno y establecer prioridades claras sobre qué se debe levantar antes. Pero lo más relevante, según Santadreu, es que estos planes se prueben, realizar simulacros reales para ver si funcionan.

El experto en ciberseguridad añade que otro frente importante es el de las certificaciones, porque muchas veces desde el área de negocio no se percibe el valor directo de obtener un certificado como la ISO 27001 o cumplir con el Esquema Nacional de Seguridad, que ayudan a minimizar riesgos legales, económicos y reputacionales. Además, comenta que estas certificaciones empiezan a ser requisitos en pliegos y licitaciones públicas, por lo que también permiten seguir siendo competitivos en el mercado.

Conectividad

Las compras y adquisiciones están a la orden del día, por lo que Luis González aborda la cuestión de cómo



Iniciativas digitales en Andalucía

Andalucía está inmersa en la definición de un programa de aceleración del *time to market*, en un programa de aseguramiento de la sostenibilidad digital y en la definición del programa de humanización digital. Cristina Tello apunta a las iniciativas digitales enfocadas a esos tres ámbitos.

Para la aceleración del *time to market* avanza que se están implementando soluciones digitales adaptadas a la realidad andaluza que aseguran la calidad del dato, el cumplimiento normativo y la respuesta a las necesidades específicas de la región. “Existen laboratorios de innovación y *hackatones* regionales donde participan la Junta de Andalucía, centros hospitalarios, universidades y actores tecnológicos. También se trabaja con grandes proveedores como Amazon Google y Azure para identificar retos locales y acelerar la creación de prototipos, usando metodologías de inteligencia artificial y análisis de datos. Además, se han creado plataformas de cocreación y *feedback* permanente que permiten a la comunidad sanitaria compartir ideas, aportar retroalimentación y testear soluciones desde fases tempranas integrando DevOps y supervisión experta para evitar problemas regulatorios y técnicos.

Finalmente hay un control regulatorio gestionado por la Consejería de Salud y organismos locales que reduce los tiempos de validación y garantiza el cumplimiento normativo”, señala.

En cuanto a la sostenibilidad digital argumenta que se está realizando un análisis y monitorización en tiempo real del impacto energético, la huella digital y el rendimiento de las infraestructuras tecnológicas. “Organismos regionales y centros de salud ajustan sus operaciones según indicadores para mejorar la eficiencia. Se impulsa la migración a plataformas *cloud* certificadas y *eco friendly* con límites de emisiones y concursos públicos. Se diseñan infraestructuras flexibles y seguras que minimizan el consumo de agua para refrigerar los centros de datos y se utilizan tecnologías como *blockchain* para la trazabilidad y gestión eficiente del dato”.

Respecto a la humanización digital se desarrollan *interfaces* centradas en el usuario andaluz con accesibilidad intuitiva, pensando en la diversidad cultural, se incluyen servicios de traducción simultánea para facilitar la comunicación la telemedicina, etc, explica.

acelerar la integración de entidades adquiridas o nuevos centros sanitarios sin afectar la operativa, desde una perspectiva centrada en la infraestructura y los sistemas. En este sentido explica que, habitualmente, en los procesos de adquisición los equipos de redes y sistemas quedan en un segundo plano, ya que el

foco suele estar más en las aplicaciones, en las bases de datos y en la integración funcional de los sistemas heredados, aunque estos elementos son críticos al constituir la base sobre la que operan las capas superiores. ¿Qué hacer? Llevar a cabo una planificación clara y concisa del proceso de integración, responde.

“Esa planificación debe incluir una prueba de concepto que permita validar que los sistemas van a funcionar correctamente una vez conectados. Y todo esto, sin perder nunca de vista la necesidad de mantener la operativa en marcha, porque en un entorno sanitario esto puede tener consecuencias graves”. Por ello reco-



mienda analizar si es posible implementar una estrategia de integración sin parada.

En cuanto a la integración de nuevos centros, más allá de los procesos de adquisición, destaca la ventaja de contar con soluciones centralizadas y ya probadas. "Cuando una organización dispone de una arquitectura de red o de sistemas que ha demostrado ser eficaz en otros centros, la replicación de esa solución en una nueva ubicación resulta mucho más cómoda y segura", aclara. "Si ya tienes un sistema funcionando bien en una ubicación central, puedes desplegarlo en los nuevos centros con mayor rapidez, utilizando herramientas automatizadas y mecanismos de configuración remota" ya que tal y como señala, "esto permite que los nuevos equipos se integren directamente en los sistemas existentes sin que se requiera intervención presencial intensiva".

Durante el coloquio también se ha hablado sobre cómo conseguir una alta disponibilidad y redundancia en las comunicaciones de Internet. Luis González explica que la solución básica pasa por contar con dos proveedores distintos que permitan hacer redundancia a través de redes independientes, si bien advierte que la dificultad real está en encontrar proveedores cuyos servicios no compartan infraestructura física porque si, por ejemplo, la red principal de Telefónica falla, puede afectar a otros



operadores que dependen de esa misma red, aunque sean diferentes.

Martín Santandreu complementa este enfoque señalando que, dentro de un plan de continuidad de negocio, es fundamental identificar los procesos y proveedores realmente críticos para la operación sanitaria y formalizar acuerdos claros de nivel de servicio que establezcan tiempos de recuperación garantizados, de modo que la responsabilidad esté contractualizada y no dependa solo de la buena voluntad.

Cristina Tello recomienda diversificar las tecnologías de comunicación, no limitándose solo a operadores tradicionales, sino incorporando opciones como satélite, radioenlace o 5G para disponer de rutas alternativas en situaciones de emergencia o caída total, aunque reconoce que estas alternativas aún no tienen el ancho de banda necesario para cubrir toda la demanda de un centro sanitario, pero sirven para mantener operaciones mínimas críticas como correo o comunicaciones básicas.