Luis Pérez Pau (FutuRS): “La seguridad total es incompatible con el modelo actual”

Luis Pérez Pau es European Chief Information Security Officer en FutuRS, la tecnológica del grupo sanitario Ribera. Desde este puesto lidera la estrategia de ciberseguridad de una organización que ha hecho de la innovación tecnológica un elemento diferencial en la atención al paciente. FutuRS centraliza los servicios de IT del grupo, impulsa proyectos basados en inteligencia artificial y participa en iniciativas europeas como NEMECYS, centrada en la ciberseguridad de dispositivos médicos conectados. En este entorno hiperconectado, Luis aborda los retos de proteger los datos clínicos, garantizar la disponibilidad de los sistemas y mantener la confianza del paciente.

Luis Pérez Pau,
European Chief Information Security Officer en **FutuRS**

IR A PÁGINA SIGUIENTE

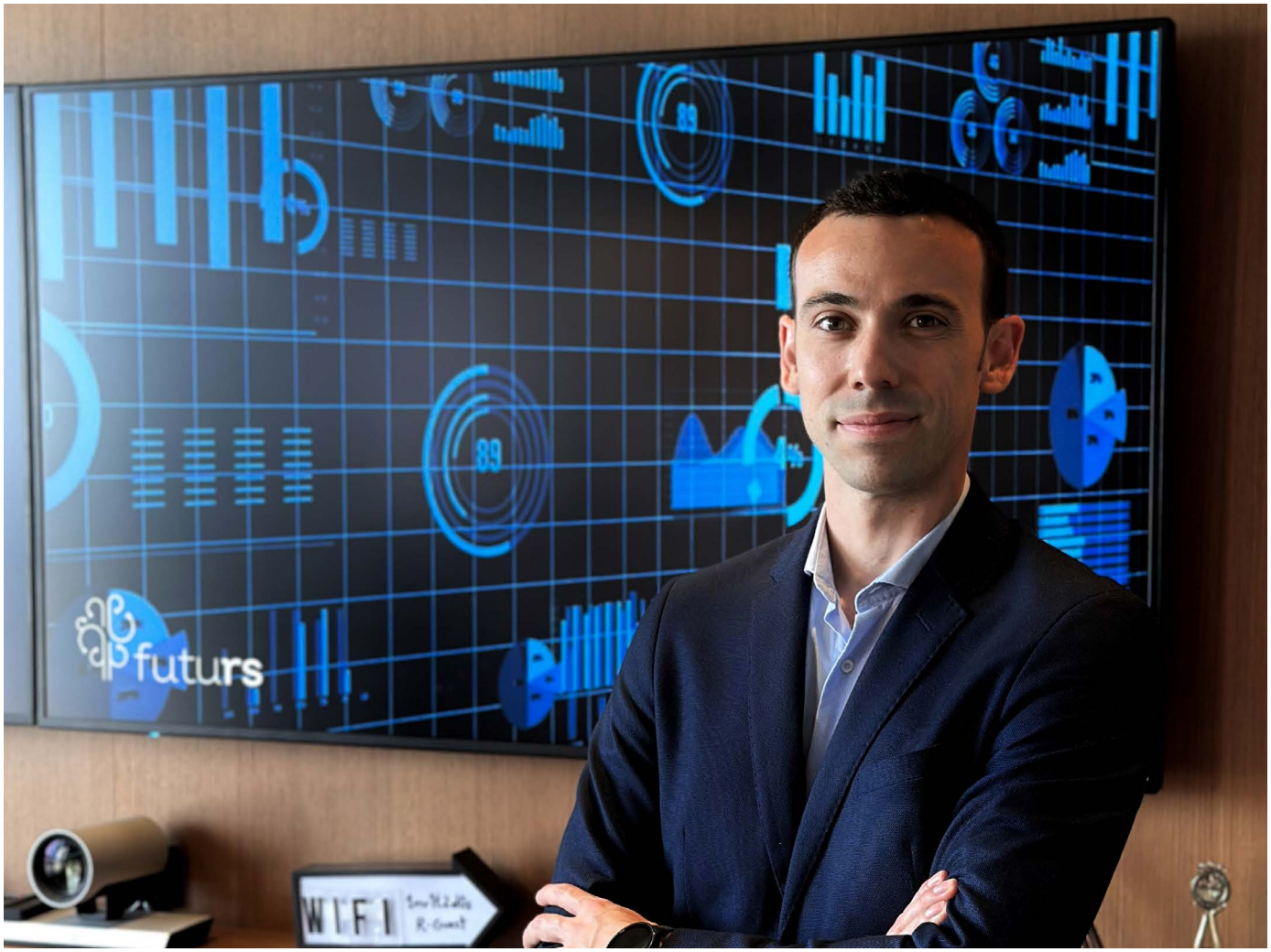
Luis Pérez Pau reflexiona sobre la evolución del rol del CISO, el impacto de la inteligencia artificial en el sector salud y los desafíos regulatorios que plantea la directiva NIS 2, todo ello desde una posición de liderazgo técnico y estratégico en un entorno sanitario cada vez más digitalizado.

“Un buen CISO debe estar alineado con el negocio”, afirma Luis Pérez Pau. Desde su punto de vista, esta figura no puede limitarse a la parte técnica: debe liderar iniciativas estratégicas para la organización, traducir riesgos a lenguaje comprensible para el negocio y adaptarse con agilidad a los cambios regulatorios.

Junto a esa visión estratégica, destaca también habilidades como la capacidad de comunicación asegurando que un buen CISO “tiene que saber hablar muchos idiomas y, sobre todo, hacerse entender en los comités de dirección”, además de tener tolerancia al incidente: “La seguridad total no existe”, recuerda. Por eso, considera clave asumir que habrá fallos y prepararse para responder con resiliencia. En su opinión, el CISO debe anticiparse, liderar con criterio y mantener la curiosidad para estar al día en un mercado en constante evolución.

Aunque reconoce que el rol se está orientando más al negocio, asegura que aún no se ha desligado de la base técnica. La ciberseguridad sigue requiriendo conocimiento profundo y actualizado, especialmente en sectores críticos como el sanitario, donde la amenaza del ransomware está muy presente.

El sector sanitario, en su opinión, está en el centro del huracán. “El ransomware es la amenaza que más nos preocupa, especialmente cuando se puede combinar el cifrado con la exfiltración de datos sensibles de pacientes”. Y lo es aún más si se aprovecha una vulnerabilidad de día



> “El entorno sanitario actual es altamente complejo y conectado: la superficie de ataque se ha multiplicado”

cero: “Cuando pasa eso, empieza una carrera contra reloj para cerrar puertas, muchas veces sin tener aún un parche disponible”, asegura Luis Pérez Pau.

La complejidad del entorno sanitario no lo pone fácil. “El paciente es el centro del sistema, y sus datos circulan por un entorno muy conectado: presencial, telemático, telefónico, dispositivos en casa, información que va y viene de la nube”. A esto se suma una gran dependencia de proveedores de electromedicina con sistemas obsoletos: “Son cajas negras difíciles de actualizar. La gestión del tercero cobra aquí una importancia crítica”.

Ante el auge de la inteligencia artificial generativa, FutuRS ha optado por regular su uso dentro de políticas corporativas claras. Han apostado por soluciones corporativas seguras, con acuerdos de confidencialidad y uso específico, evitando modelos públicos. Además, la IA ya se aplica tanto en el ámbito clínico —por ejemplo, en la predicción de enfermedades— como en la detección y respuesta ante incidentes, median-

te algoritmos de aprendizaje automático. “Nos ayuda, pero también nos obliga a mantener una vigilancia ética y transparente”, advierte, al tiempo que subraya la importancia de seguir de cerca el reglamento europeo de IA.

En relación a la NIS 2, destaca la lógica de establecer un nivel base común de ciberseguridad y fomentar la colaboración con autoridades nacionales y CSIRT. Sin embargo, señala que uno de los mayores retos es asegurar la cadena de suministro asegurando que “homologar proveedores, revisar contratos, pedir certificados... todo eso va a ser uno de los trabajos más complicados. Y más si cada país transpone la directiva de forma distinta”. Explica que en FutuRS aplican un proceso de homologación para todos los proveedores estratégicos, evaluando su nivel de riesgo, sus certificaciones y su alineación con las políticas de ciberseguridad del grupo.

> “Hemos optado por regular el uso de la IA dentro de la empresa y apostar por modelos corporativos seguros”

Tras comentar que la colaboración con el resto del mercado es esencial, asegura Luis Pérez Pau que FutuRS cuenta con un SOC propio que forma parte de la Red Nacional de SOC del Centro Criptológico Nacional. Además, participan activamente en redes como ENISA, IDIS o asociaciones profesionales, compartiendo indicadores de compromiso, buenas prácticas y organizando talleres para reforzar la comunidad entre CISO del sector.

Sobre los servicios gestionados de seguridad,

Luis Pérez cree que no basta con contratar una solución y esperar resultados: “Muchos SIEM se convierten en vertederos de logs. Sin análisis, sin inteligencia, no sirven”. Reclama inteligencia real, capacidad de correlación y un compromiso auténtico por parte de los proveedores. “El valor está en conectar señales, identificar patrones y reaccionar a tiempo. Si no hay cariño por los datos, no hay seguridad eficaz”.

El factor humano también cuenta. “Llevamos años haciendo simulaciones de phishing a toda la plantilla y hemos observado una gran mejora en la disminución de tasas de clic ante estos engaños”. A esas campañas se suman formaciones, píldoras de concienciación, además de establecer un control estricto sobre herramientas de compartición de archivos: sólo se permiten por excepción y previa validación del departamento de IT.

A nivel personal, uno de los proyectos de los que se siente más orgulloso es la certificación del grupo en estándares internacionales de seguridad. Tras una auditoría basada en el marco

NIST, impulsada por un inversor estadounidense, iniciaron un proceso de certificación en la ISO 27001 y el Esquema Nacional de Seguridad (ENS). “Fue un esfuerzo exigente, pero ha rendido frutos significativos en términos de madurez, reputación y tranquilidad para todos los stakeholders”, explica el CISO de FutuRS.

De cara al futuro, identifica varias tecnologías clave: soluciones de protección y respuesta apoyadas en IA, una gestión de identidad adaptada al entorno híbrido y, sobre todo, la transición hacia la criptografía postcuántica. Advierte que para 2029 esta tecnología deberá estar implantada, y que muchas organizaciones aún no están preparadas: “Si almacenas datos cifrados hoy con criptografía tradicional, podrías tener un problema mañana”.

Luis Pérez confía en que 2025 sea el año de impulso real de la NIS 2 y que actúe como catalizador para mejorar la postura de seguridad a nivel europeo. Y lanza un mensaje claro: “La seguridad es responsabilidad de todos: personas, instituciones y empresas. Solo desde la colaboración podremos estar preparados para lo que viene”.