Foro TAI

"Retos tecnológicos para el futuro empresarial de la Comunidad Valenciana"

TAI

it. Colegio Oficial Ingenieros de Telecomunicación Comunidad Valenciana

ENTIDAD COLABORADORA

Tecnología para los negocios | Cámara Valencia

PATROCINADORES

Allied Telesis™

cipher a Prosegur company

hp / AMD

nunsys Tu socio tecnológico

Lenovo | AMD

]pexip[

SOPHOS

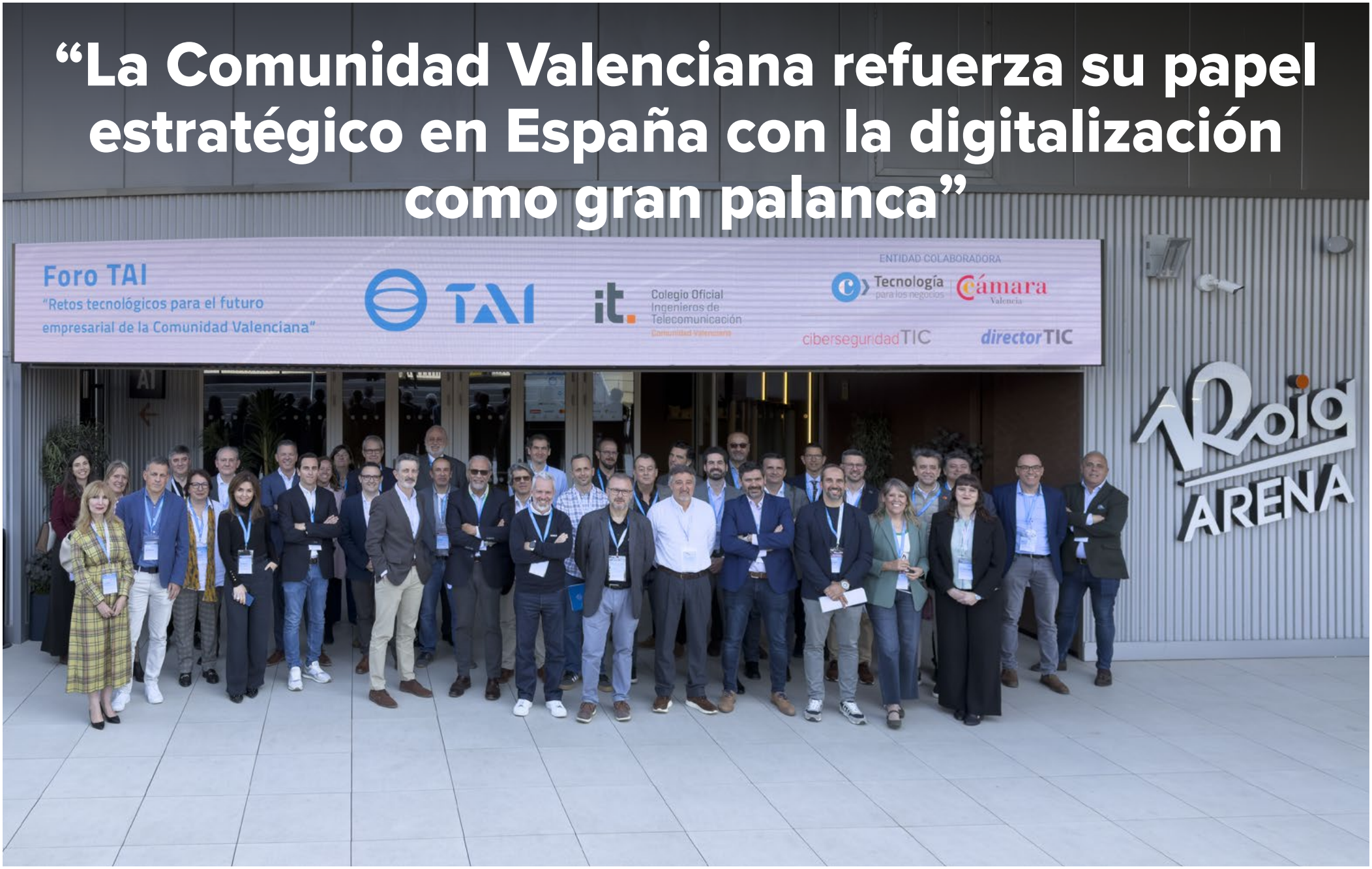
VIRTUAL CABLE

ciberseguridadTIC

directorTIC Información de valor para la toma de decisiones

IR A PÁGINA SIGUIENTE

“La Comunidad Valenciana refuerza su papel estratégico en España con la digitalización como gran palanca”



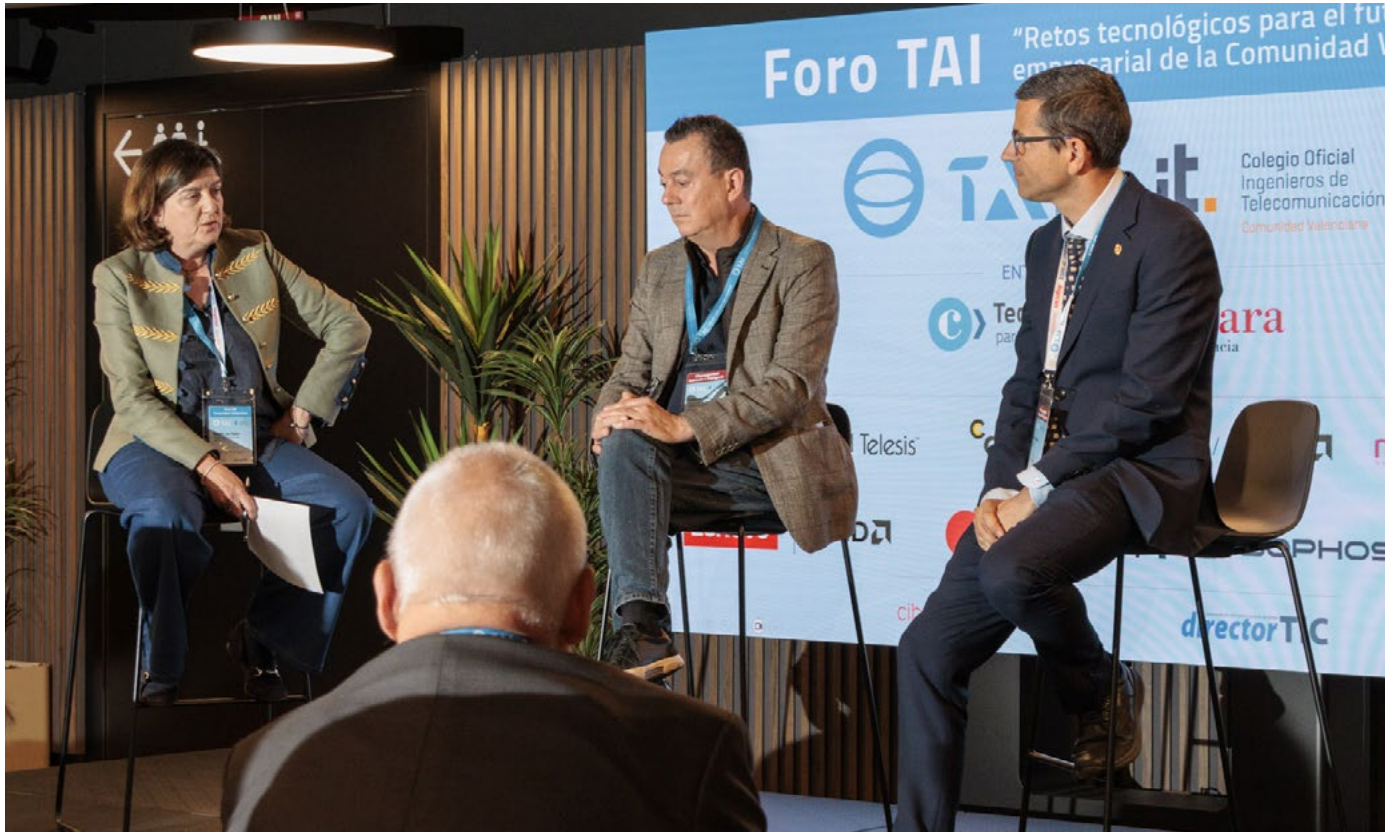
Foro TAI Valencia

IR A: Apertura | Debate CIO | Debate CISO | Entrevista Cámara de Comercio | Vídeos |

La ciudad de Valencia acogió una nueva edición de los foros tecnológicos que organiza el Grupo Tai, a través de sus publicaciones DirectorTIC y CiberseguridadTIC, centrado, una vez más, en analizar el grado de implantación de las Tecnologías de la Información y la Comunicación (TIC) en el tejido empresarial valenciano. Un foro que reunió a CIO y CISO de las principales empresas e instituciones públicas de la Comunidad Valenciana y que puso de relieve tanto los avances como los desafíos pendientes en materia de transformación digital. Grupo TAI contó con la colaboración del Colegio Oficial de Ingenieros de Telecomunicación (COIT) de la Comunidad Valenciana y la Cámara de Comercio de Valencia. El evento estuvo patrocinado por Allied Telesis, Cipher, HP-AMD-NUNSYS, Lenovo-AMD, Mastercard, Pexip, Sophos y Virtual Cable.

Marilés de Pedro

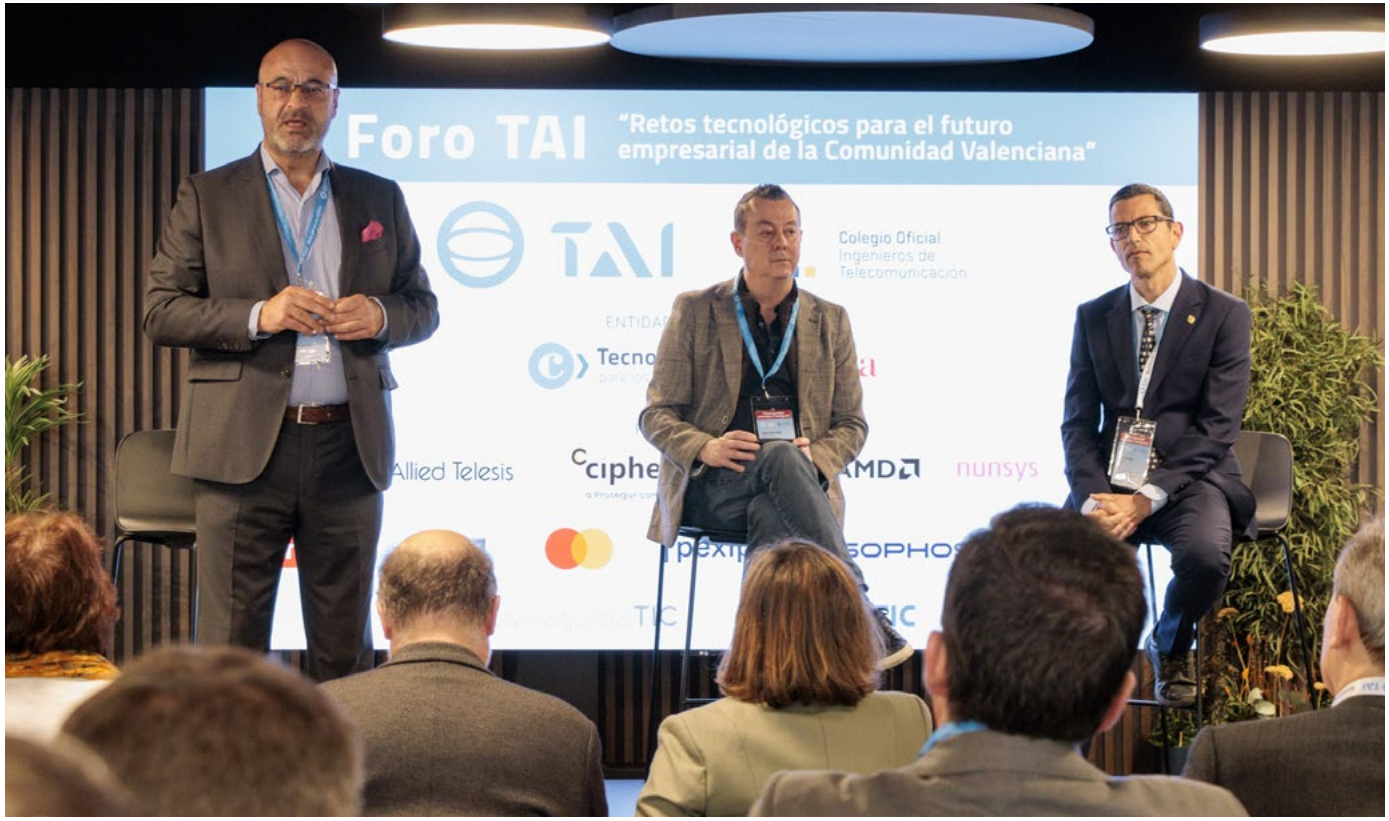
En la inauguración del evento participaron César Morillas, vicedecano del Colegio Oficial de Ingenieros de Telecomunicación (COIT) de la Comunidad Valenciana, y Carlos de Cózar, director del área TIC de la Cámara de Comercio de Valencia, quienes coincidieron en señalar la relevancia creciente de la Comunidad Valenciana en el contexto económico nacional.



Una economía clave en España

La Comunidad Valenciana se consolida como la cuarta economía del país, al generar el 9,3 % del Producto Interior Bruto nacional. Su modelo destaca por una diversificación equilibrada entre industria, exportaciones y turismo. En 2024, el PIB regional creció en torno al 3,3 %,

> “Hay que integrar la inteligencia artificial de forma inteligente en el núcleo de las empresas”
>
> (César Morillas)



ligeramente por debajo del conjunto de España (3,5 %). En 2025 el PIB nacional creció un 3,2 % y las previsiones para la región valenciana apuntan a un crecimiento sostenido de entre el 3,2 % y el 3,6 %, según la Autoridad Independiente de Responsabilidad Fiscal (AIReF) o las estimaciones que hace el BBVA, respectivamente.

Lejos del estereotipo turístico, la comunidad cuenta con un potencial industrial: el 14,5 % de su PIB procede de las manufacturas. A ello se suma una fuerte vocación exterior, con exportaciones que representan el 27 % del PIB regional y el 9,6 % del total nacional. Incluso sectores con menor peso relativo, como la agricultura (2 % del PIB), mantienen una gran importancia estratégica por su capacidad exportadora. El gran reto ya no es crecer, sino crecer en valor y productividad; lo que concede a la digitalización y la ciberseguridad un papel decisivo.

Un tejido empresarial dominado por micropymes

El ecosistema empresarial valenciano está fuertemente atomizado. Con un ecosistema empresarial formado por 350.000 compañías, alrededor del 90 % son pymes, muchas de ellas micropymes de menos de diez empleados y, en gran medida, de carácter familiar. “Es nuestro gran tejido empresarial, pero también nuestro gran desafío a la hora de digitalizar”, apuntó César Morillas.

A nivel territorial, la especialización es clara: la cerámica en Castellón, el juguete y el textil en

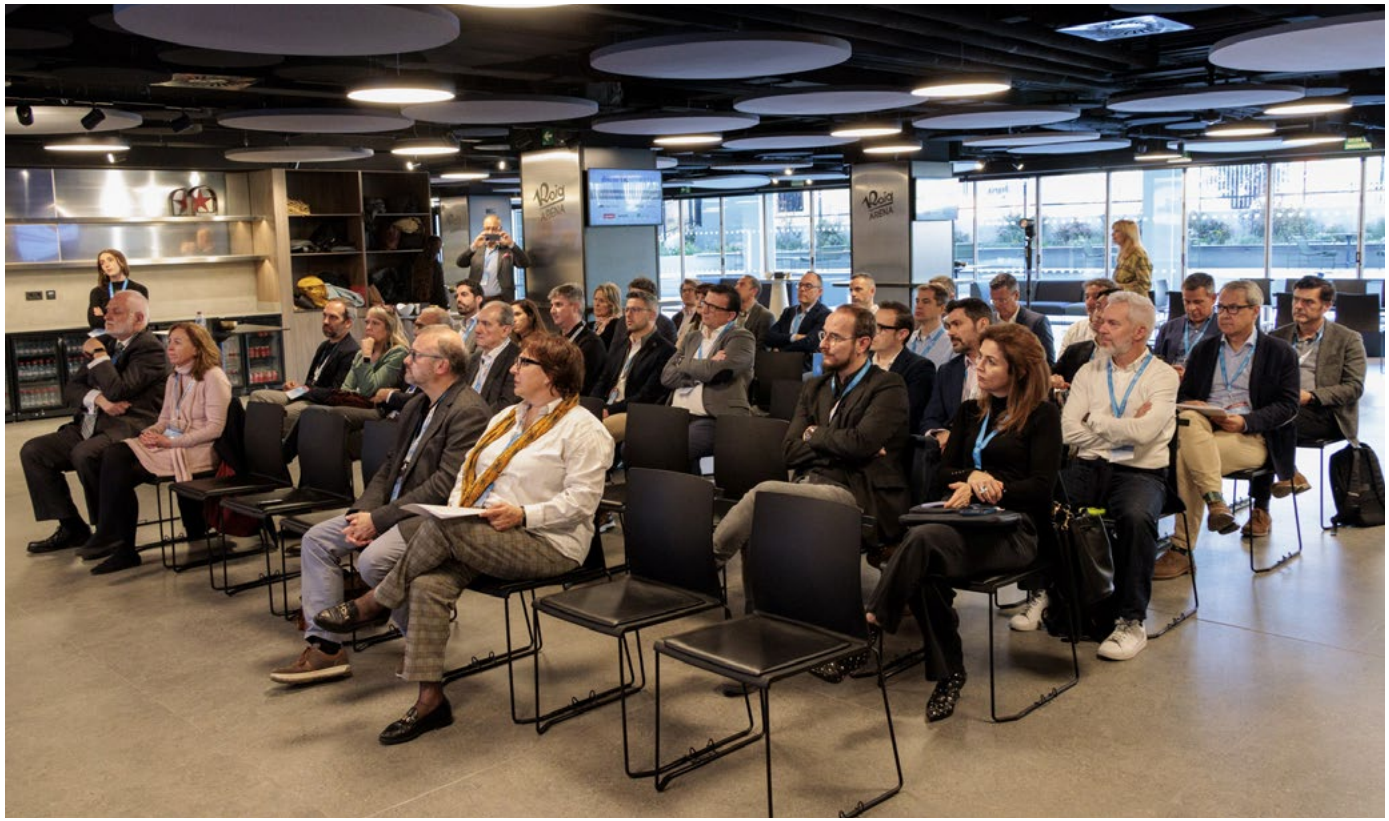
Alicante, y un potente polo logístico e innovador en Valencia, impulsado por su puerto. Aunque las empresas tecnológicas representan en torno al 3 % del PIB, la economía digital alcanza ya el 18 %, reflejando su creciente peso.

Dos velocidades en la adopción tecnológica

El diagnóstico sobre la implantación de las TIC es, en palabras de Morillas, “agridulce”. Por un lado, las infraestructuras digitales están bien desarrolladas, con amplia cobertura de banda ancha y más del 90 % de cobertura 5G. Muchas empresas han alcanzado lo que denomina “supervivencia digital”: presencia web, correo electrónico y facturación electrónica.

Sin embargo, persiste una brecha significativa. “Tenemos dos velocidades muy claras: grandes empresas tractoras y un amplio tejido de micropymes que apenas ha superado ese nivel básico”, explicó. La mayoría de estas pequeñas empresas carece de herramientas clave como CRM, ERP, soluciones *cloud* o inteligencia artificial.

Para avanzar en el proceso de transformación digital, Morillas señaló tres prioridades: la ciberseguridad, los servicios en la nube y la inteligencia artificial. La seguridad, en particular, se ha convertido en un elemento innegociable. “Es una marca de reputación y de prestigio; una obligación en toda la cadena de negocio”, afirmó Morillas. En paralelo, defendió la necesidad de impulsar modelos SaaS y de integrar la inteligencia artificial “de forma inteligente” en el núcleo de las empresas.



Con un tejido empresarial compuesto, en su mayoría, por pymes, Carlos de Cózar también insistió en que la protección es uno de los puntos más críticos. Cerca del 75 % de los ataques se dirigen a este tipo de empresas que cuentan con menos recursos para defenderse. “Las pymes son el eslabón más débil y el más atacado”, alertó. Los principales riesgos incluyen *ransomware*, *phishing*, ingeniería social y ataques a sistemas web.

El gran reto: el talento

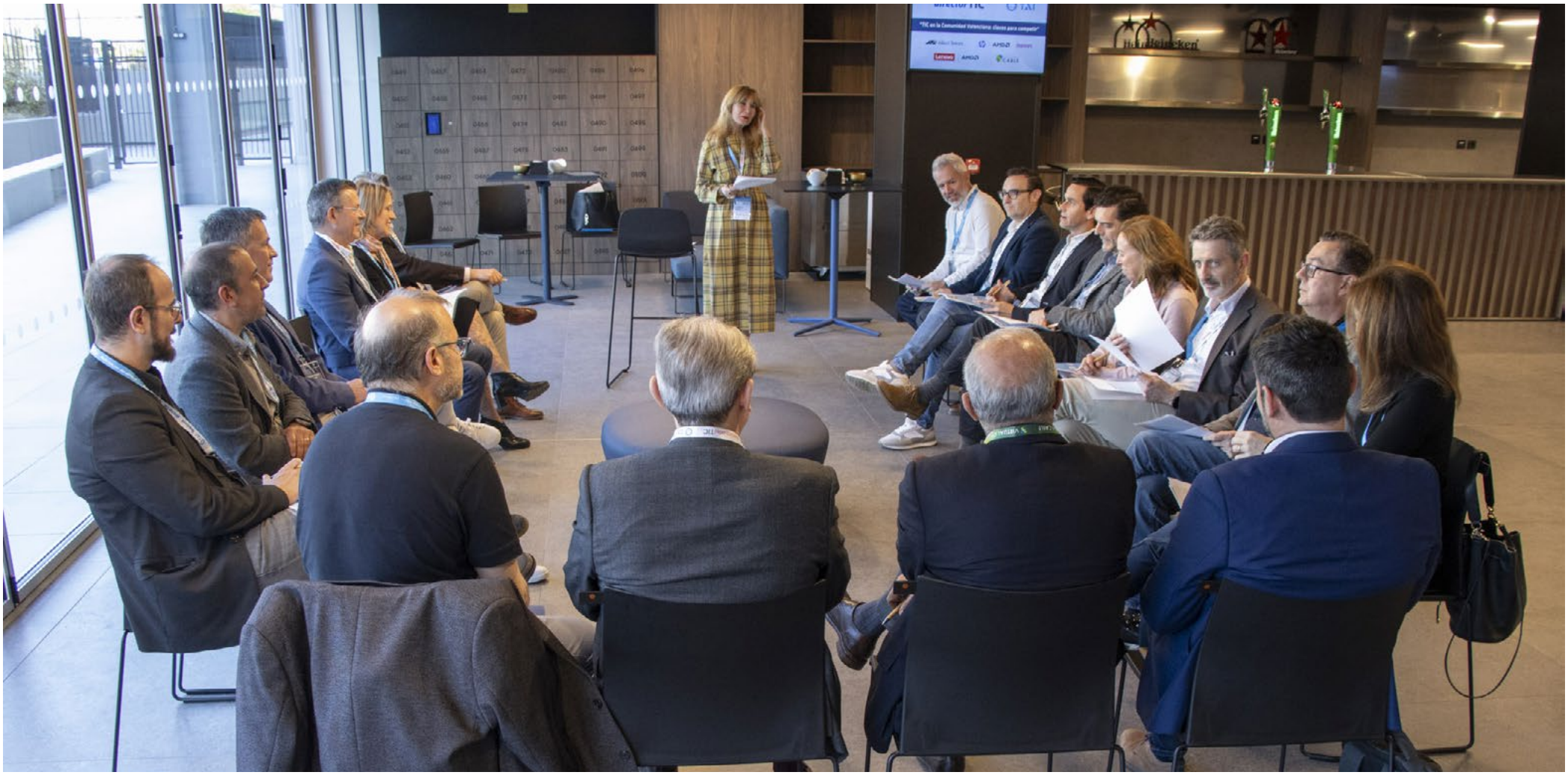
Uno de los principales retos identificados es la escasez de profesionales cualificados en TIC. En España se estima un déficit de unos 120.000 especialistas, lo que se traduce en cerca de 10.000 vacantes en la Comunidad Valenciana. “Es esencial que no solo haya personal especializado en esta materia, sino retenerlo”, remarcó Morillas. Un reto que “no es solo tecnológico; también humano”, advirtió Carlos de Cózar. “Hay muy pocas empresas con una figura de CIO y aún menos con un profesional que ejerce de CISO”. Es el segmento de la ciberseguridad donde “el déficit de talento es todavía más acusado”.

> “Las pymes son el eslabón más débil y el más atacado”
>
> (Carlos de Cózar)

Digitalización desigual y retos en Europa

De Cózar explicó que, en términos de conectividad, la Comunidad Valenciana se sitúa en línea con España y Europa. Sin embargo, reconoció que “en *cloud* y teletrabajo estamos por debajo de la media, especialmente en determinados sectores”. A nivel sectorial, los servicios lideran la digitalización, mientras que la construcción muestra mayores carencias. En cuanto a la inteligencia artificial, el 20 % de las empresas valencianas de más de diez empleados ya la utiliza, principalmente en marketing y gestión empresarial.

Los CIO de las empresas valencianas, entre el reto de medir el valor real de la IA y la reducción de costes



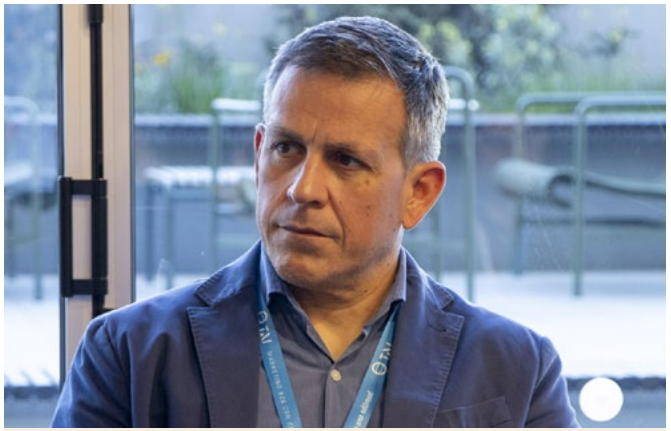
Foro TAI Valencia

La Comunidad Valenciana se consolida como un referente en crecimiento económico, impulsado por la digitalización, con un tejido empresarial donde el puesto de trabajo digital, la conectividad y la gestión del dato se convierten en ejes estratégicos. En este contexto Cámara de Valencia, la Generalitat de Valencia, Nealis, FERMAX, Ysabel Mora, Istobal, AR Hotels&Resorts, Veolia y DCM SISTEMES, junto a Virtual Cable, Allied Telesis, HP-AMD-NUNSYS y AMD-Lenovo, coinciden en señalar en el foro TI, retos como la seguridad, la complejidad tecnológica y el control de costes. La virtualización, la automatización y la inteligencia artificial emergen como palancas claves, aunque también introducen nuevos desafíos, especialmente en la falta de inversión y la gestión del dato en el ámbito de la IA. La conectividad, por su parte, pasa de ser un recurso básico a un elemento crítico. Todo ello en un entorno donde sostenibilidad, eficiencia y gobernanza tecnológica marcan la hoja de ruta.

Inma Elizalde

Diferentes informes de consultoras y organismos posicionan a la Comunidad Valenciana como un referente en crecimiento, impulsado por la tecnología. El BBVA Research la señala como la región líder en crecimiento económico en España en 2026 y el Instituto Valenciano de Investigaciones Económicas (Ivie) destaca que la transformación digital es su principal factor diferenciador para algo más del 81 % del empleo regional, concentrado en empresas digitalizadas.

En torno al puesto de trabajo digital, la Confederación Empresarial de la Comunidad Valenciana (CEV) indica que el modelo híbrido se ha consolidado, con un enfoque en la experiencia del empleado (DEX) y una tendencia, en 2026, a la personalización mediante IA. En cuanto a la virtualización, tras el impulso de los fondos NextGen, las pymes de la comunidad la incorporan con el fin de permitir el acceso seguro desde cualquier dispositivo, reduciendo el coste del hardware.

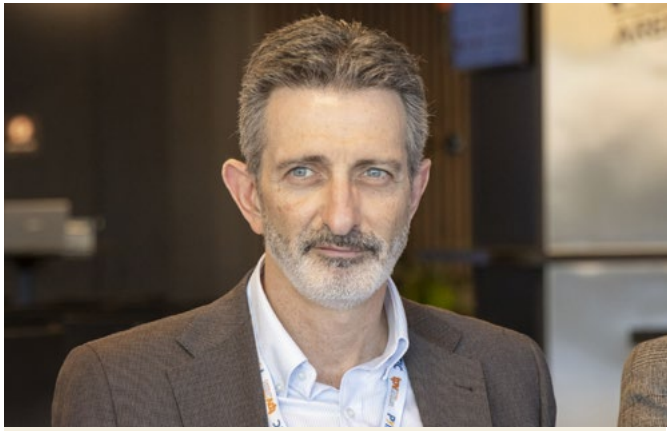


"Nealis cuenta con proyectos de inteligencia artificial en producción, aplicados a casos como licitaciones"

Miguel Ángel Royo, CIO de **Nealis**

Un puesto de trabajo digital que, en el caso de empresas como Nealis, (especializada en agua y medioambiente, instalaciones y servicios, infraestructuras y *hospitality*) presenta retos como la homogeneización de cada uno de los sistemas y su evolución. Así lo destaca Miguel Ángel

Royo, CIO de la compañía. Algo en lo que coincide Francisco Alapont, director de estrategia de FERMAX (fabricante de sistemas de portero, videoportero, control de accesos y soluciones de conectividad para el hogar) una organización que ha dado el paso de compañía familiar a una empresa corporativa en el último lustro. ¿Qué buscan en este momento? Compaginar flexibilidad con seguridad en el puesto de trabajo para sus trabajadores en movilidad y para los que están en un entorno fabril, cubriendo el espectro de fabricación de producción, *delivery* y ventas internacionales con filiales en otros lugares del mundo que van integrando en un proceso de crecimiento inorgánico, avanza Alapont.



"La virtualización del puesto de trabajo optimiza recursos y permite modelos híbridos flexibles y eficientes"

Francisco Alapont,
director de estrategia de **FERMAX**

El valor de la virtualización

En cuanto a la virtualización del puesto de trabajo no todas las empresas la contemplan. Este es el caso de Nealis. Otras como la firma de lencería Ysabel Mora, aunque de momento no se han adentrado en la misma al no sentir esta necesidad, su CIO, Néstor Flórez, reconoce que la empresa cuenta con un equipo informático no estándar que dificulta industrializar soluciones de gestión y administración remota, obteniendo una homogeneidad. En el caso de FERMAX, se lo han planteado en áreas con perfiles de uso más "estáticos" como administración, sin llegar por el momento a dar el paso hacia la virtualización.

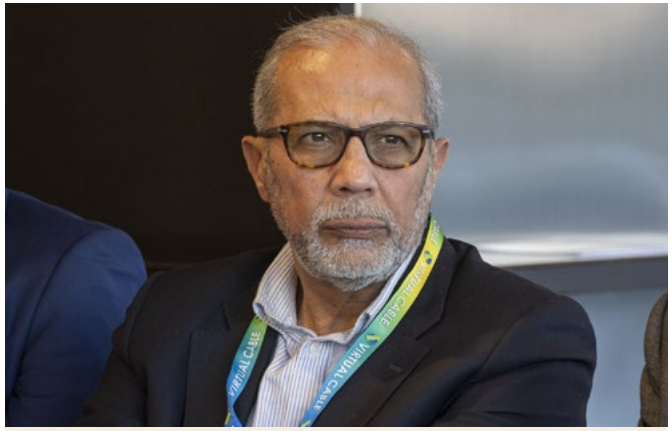
"Los modelos híbridos generan nuevos retos en el control y organización del gasto"

Néstor Flórez,
CIO de **Ysabel Mora**

Fernando Feliu, *executive managing director* de Virtual Cable, (desarrollador español de software especializado en virtualización del puesto de trabajo y acceso seguro a aplicaciones y datos corporativos) pone en valor la virtualización ante los problemas de *ransomware* y agentes de IA o el *compliance* con las normativas existentes,

la soberanía del dato y la soberanía digital. “La virtualización ofrece perfiles reales para cada usuario. Incluso cuando se adquieren otras compañías y hay que seguir utilizando herramientas diferentes, en función de cada uno de los datos, brinda la ventaja de hacer que la entrada de *ransomware* disminuya a casi el 90 %”, confirma. Una virtualización que también optimiza los recursos, ajustando el consumo de las aplicaciones según las necesidades de cada puesto de trabajo y focalizando la evolución tecnológica en aquellos perfiles, como los de desarrollo, que realmente lo requieren.

Feliu enfatiza la oportunidad que ofrece de reutilizar el parque instalado usando las últimas tecnologías. “Además de la seguridad o de los grandes volúmenes de usuarios, también presenta la posibilidad de tener una parte en la nube y otra *on-premise*. Puedes levantar automáticamente máquinas o servidores en función de las necesidades, hacer desbordamientos automáticos a nubes públicas o privadas, sistemas híbridos, todo tipo de hipervisores, autenticación multifactor, políticas *zero trust*...”, añade.

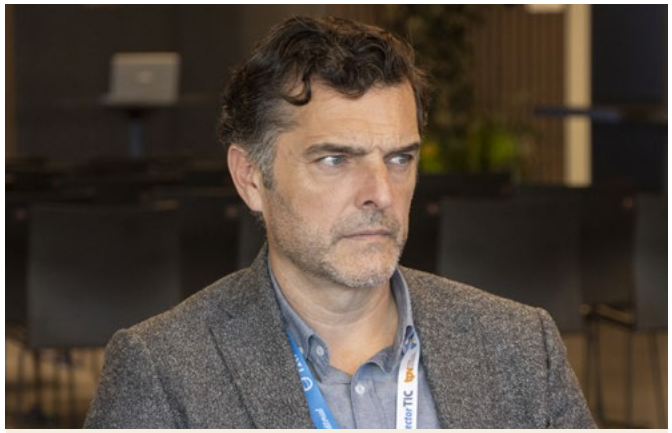


> “La virtualización optimiza recursos y permite modelos híbridos flexibles y eficientes”
>
> **Fernando Feliu,**
> *executive managing director* de **Virtual Cable**

Seguridad en el puesto de trabajo

La seguridad es una constante preocupación para las empresas. Así lo manifiestan Willy Piquer, experto TIC, José Blanco, CIO de Istobal y Lucía Martínez, CIO de AR Hotels&Resorts. Willy Piquer recuerda que las pymes son las principales organizaciones que reciben ataques continuamente, sobre todo en sectores como el sanitario en el que la naturaleza de la información que manejan es más crítica y en la que los facultativos comienzan a integrar herramientas de IA y colaborativas que, en muchas ocasiones, no se sabe de dónde vienen, abriendo mundos difíciles de resolver, observa. La preocupación para José Blanco viene de la mano del empleado y de cómo usa los medios. En el caso del grupo multinacional español Istobal, dedicado al diseño, fabricación y comercialización de soluciones innovadoras para el lavado y cuidado de vehículos, confiesa que el puesto de trabajo no ha sido el punto de entrada de ataques sino los sistemas. “En este momento nuestra preocupación pasa por que los sistemas centrales estén lo más actualizados posible”, comenta. Y si hablamos del sector hotelero, epicentro de un gran número de ciberataques, la falta de inversión suele venir dada por la falta de visualización de esa inversión que repercute en el negocio, declara Lucía Martínez. En el caso de AR Hoteles&Resorts el mayor riesgo pasa por los usuarios que usan el ordenador de manera limitada, la educación y concienciación.

Ante lo expuesto, Sergio Mata, *Iberia Presales Lead* de HP, pone el foco en la importancia de poner al usuario en medio del puesto de trabajo digital, proporcionándole un equipamiento y un entorno seguro desde la fábrica hasta el terminal, que le libere de problemas y le garantice la seguridad que necesita, algo que también ayuda a la retención del talento.



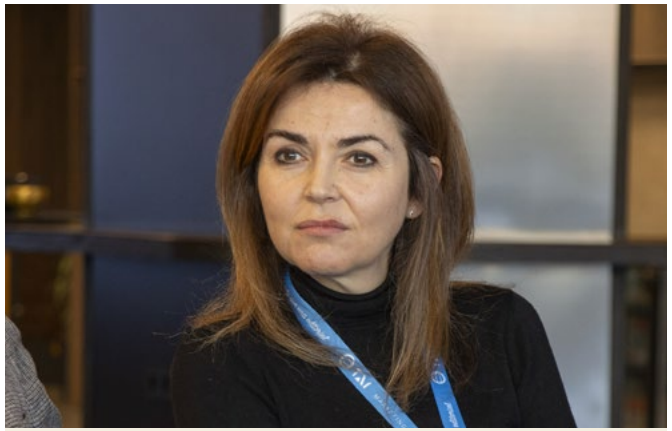
"Muchas organizaciones todavía no valoran adecuadamente la importancia de la conectividad"

José Blanco,
CIO de **Istobal**

Ecosistema completo de trabajo

Más allá del dispositivo, en torno al ecosistema completo del puesto de trabajo, José Raldúa, CIO de DCM SISTEMES, insiste en el usuario como principal problema del ecosistema porque "aun poniendo un gran número de barreras de seguridad, y teniendo la mejor tecnología, éste tiene sus costumbres y el dedo rápido con el ratón", por lo que considera que formar e informar es esencial en los puestos de trabajo.

Por su parte José Luis Martínez, director de sistemas de información de Veolia en la Comunidad Valenciana, apunta a que desde compañías como Veolia (empresa global especializada en soluciones integrales para la gestión optimizada de agua, energía y recursos) cuentan con un *digital workplace* adaptado a cada puesto de trabajo, con perfiles diversos, desde personas operarias en campo, recibiendo y cumplimentando órdenes de trabajo en dispositivos móviles, conectados con planificadores ubicados en sus centros de operación digital *hubgrade*, hasta personal de oficina para atención al cliente, así como personal de oficina técnico y administrativo de las diferentes áreas funcionales. En su opinión, uno de los grandes hándicaps desde el punto de vista de la ciberseguridad son las personas operarias que gestionan plantas consideradas como infraestructuras críticas.



"La concienciación del usuario es clave para evitar riesgos en el entorno hotelero"

Lucía Martínez,
CIO de **AR Hotels&Resorts**

Simón Viñals, director comercial del sector público de AMD para España y Portugal, remarca la idea del empleado como el eslabón más débil de la cadena en cuanto a seguridad, al tiempo que pone el acento en la necesidad de contar con herramientas que permitan implementar soluciones de software como la virtualización, seguridad, que aumenten el rendimiento, la eficiencia energética y de batería o puestos de trabajo con IA que permitan una mayor confidencialidad. “Todo ello se traduce en un mayor rendimiento y productividad del empleado, con la tranquilidad de los departamentos de TI, eliminando agujeros de seguridad y aumentando la confidencialidad de los datos”, subraya.

Conectividad

En el ámbito de la conectividad tanto Carlos de Cózar, director del Área TIC de Cámara de Valencia, como Marta Monleón, subdirectora general de Telecomunicaciones de la Generalitat Valenciana, declaran el gran nivel que existe en la comunidad, sobre todo desde la pandemia. Carlos de Cózar considera que es fundamental tanto a nivel personal como profesional. Marta

“Es complejo gestionar un puesto de trabajo digital adaptado a perfiles muy diversos”

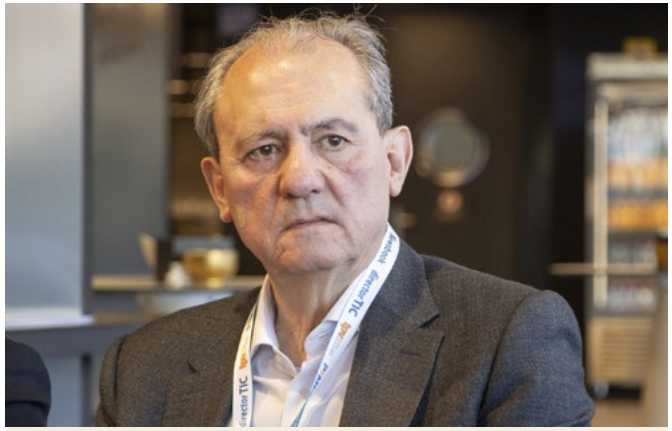
José Luis Martínez, director de sistemas de información de **Veolia en la Comunidad Valenciana**

Monleón describe el mix con el que cuentan en la Generalitat con unas 4.000 sedes diferentes y todo tipo de conectividad, hasta en lugares no habituales. Así como los problemas que han tenido que afrontar en situaciones especiales como la DANA, el apagón o la pandemia, por lo que llevan la conectividad en el ADN. La novedad que avanza es la implementación de satélites en algunas sedes.

José Blanco, sin embargo, opina que todavía existen empresas y organizaciones que no otorgan a la conectividad el valor que requiere, al dar por hecho que va a funcionar por sí sola, por lo que, teniendo en cuenta su importancia, aboga por no esperar a tener un problema para llevar a cabo inversiones en satélites o líneas secundarias. Opinión con la que coincide Luis González, director de Allied Telesis, aunque González considera que, a pesar de que hay compañías que estiman que “cualquier cosa vale”, sostiene que las redes han pasado de ser algo básico a estratégico para la mayoría de las organizaciones. “Hay que intentar facilitar la vida en torno a la red porque los especialistas en OT no suelen ser expertos en la parte de IT. Hay que aplicar soluciones autónomas, seguridad intrínseca en la red, etc”, especifica.

Costes

Los costes ocultos suelen ser una de las principales preocupaciones para empresas y administraciones. Costes ocultos que, en el caso del



"Automatización, visibilidad y redes homogéneas son claves para evitar zonas ciegas en conectividad"

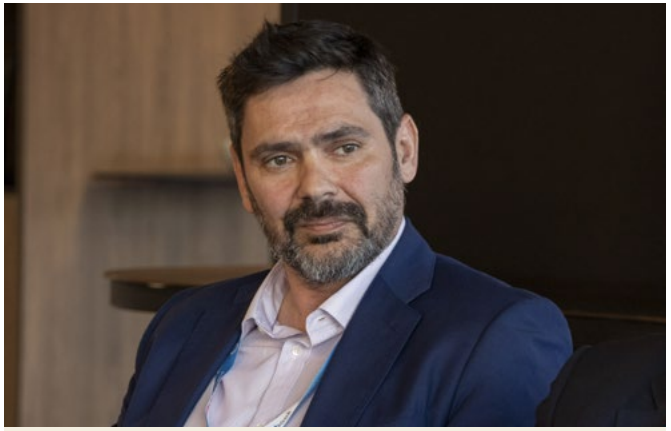
Luis González,
director de **Allied Telesis**

puesto de trabajo digital, fluctúan en función del sector ya que no es lo mismo un puesto de trabajo industrial, de servicios o sanitario, responde Willy Piquer. En su opinión, el sanitario es más caro por la gran diversidad de aplicaciones de negocio que utiliza, hasta 400 diferentes, asegura. "El coste inicial de estas apli-

Alrededor de la IA también surgen preocupaciones relacionadas con los costes

caciones es brutal y la parte de ofimática cada vez está creciendo más", advierte. En el lado de los hoteles, Lucía Martínez menciona los costes del *shadow IT*, aplicaciones que se contratan sin supervisión del departamento de IT, por poner un ejemplo. José Raldúa va más allá al reconocer que, en determinados casos, hay que instalar aplicaciones que no son productivas pero que gustan al usuario y hay que ceder para que esté cómodo en su trabajo. Néstor Flórez explica que, en el caso de Ysabel Mora, su modelo de hibridación ha cambiado en gran medida, viendo fluctuaciones de control de gasto complicadas de gestionar y ordenar, por lo que están llevando a cabo un control más profesionalizado.

La conversación deriva hacia el coste del activo con Sergio Mata señalando a este como otro factor a tener en cuenta, proponiendo



"El pago por uso y el procesamiento local de IA pueden reducir costes"

Sergio Mata,
Iberia Presales Lead de **HP**

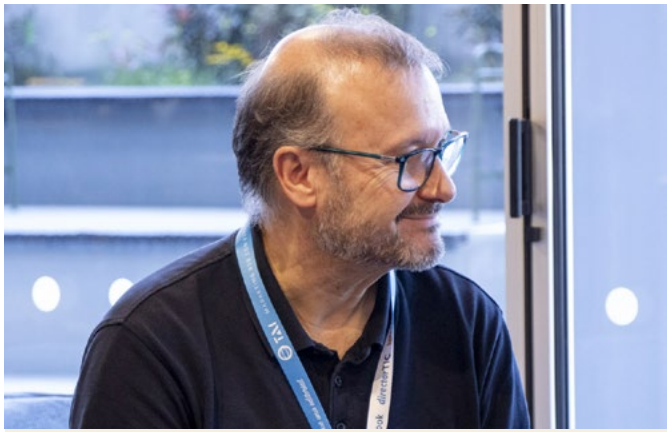
como alternativa el dispositivo como servicio, modelos de pago por uso, etc. porque, tal y como recuerda, "la tendencia va hacia el pago por uso". Y a la virtualización, vuelve a apuntar Fernando Feliu. "Si virtualizas aplicaciones no tienes que comprarlas para cada usuario", recalca.

Y es que tal y como evidencia Feliu, no todo el

mundo tiene que tener el último dispositivo y más en un momento en el que nos vamos a enfrentar de nuevo a la falta de componentes y en el que como solución podemos recurrir al mercado de segunda mano. El directivo también señala otro punto importante, el cambio que se está produciendo por parte de algunas organizaciones hacia Linux y el *open source*, dejando a un lado Windows. Sin olvidar el cumplimiento de las diferentes normativas y la ya mencionada seguridad, para la que Virtual Cable ya está inmerso en la seguridad postcuántica y el cifrado postcuántico.

Con el fin de controlar los costes en electricidad Simón Viñals comenta que AMD cuenta con una calculadora web en la que se pueden poner diferentes procesadores de AMD y de la competencia y hacer una comparativa de consumo eléctrico con respecto a la tecnología de otros fabricantes. Sergio Mata, por su parte, confirma que HP cuenta con la huella de carbono cero.

En materia de sostenibilidad Allied Telesis introduce mejoras discretas pero efectivas en el funcionamiento de sus equipos de red, que permanecen operativos las 24 horas del día, señala Luis González. Uno de los elementos claves



"La tecnología mejora el rendimiento, la eficiencia energética y la confidencialidad"

Simón Viñals, director comercial del sector público de **AMD para España y Portugal**

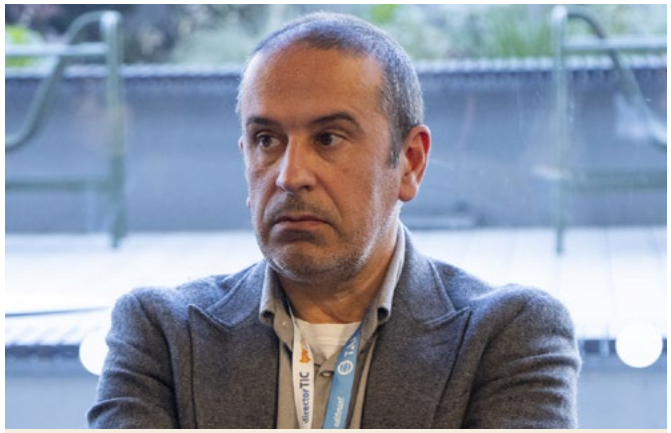
es la incorporación de fuentes de alimentación inteligentes que permiten que cada puerto funcione de manera adaptativa: si un puerto no está en uso, el sistema deja automáticamente de suministrarle energía, reduciendo así el consumo innecesario. Además, el equipo es capaz de medir la longitud del cable conectado y ajustar la potencia en consecuencia. Este mismo principio de eficiencia se aplica en situaciones cotidianas, como durante la noche. Cuando los dispositivos conectados se apagan, los puertos pasan a un estado inactivo, lo que permite a la fuente de alimentación reducir automáticamente la energía suministrada. Este ajuste continuo repercute directamente en una disminución del consumo eléctrico y, a largo plazo, en un ahorro económico significativo.

"La virtualización ajusta el consumo de las aplicaciones según las necesidades de cada puesto de trabajo"

A estas medidas se suman otros ajustes menores, como la posibilidad de desactivar indicadores luminosos LED, que, aunque pequeños en apariencia, contribuyen de forma acumulativa a una reducción considerable del consumo energético.

IA

Alrededor de la inteligencia artificial también surgen preocupaciones relacionadas con los costes. Carlos de Cózar señala que están apareciendo numerosas herramientas que provocan un aumento significativo del gasto, especialmente por el mantenimiento de aplicaciones en la nube y de sistemas, una partida que no deja de crecer en un contexto donde la IA y la automatización se combinan.

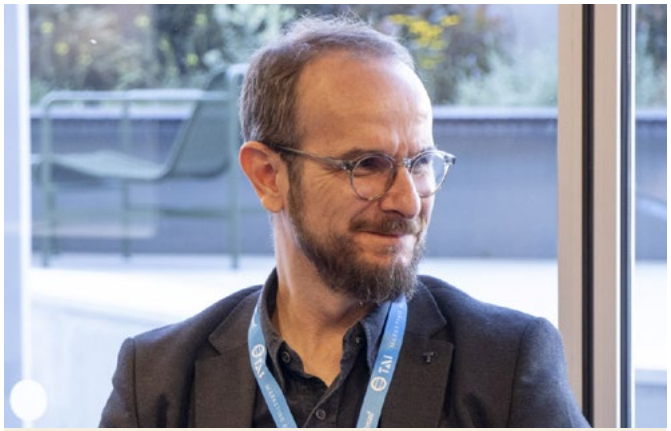


"Es complejo trabajar con IA debido a problemas como las alucinaciones"

José Raldúa,
CIO de **DCM SISTEMES**

Por su parte, Néstor Flórez destaca que los modelos de costes están cambiando de forma considerable. En este escenario, el principal reto es medir el beneficio, que puede derivarse tanto de la reducción de costes como de la mejora del servicio y todo lo que ello implica. A partir de estos factores, explica, es posible establecer métricas.

En este contexto, Marta Monleón plantea la pregunta clave: ¿cómo calcular qué va a suponer un proyecto llevado a cabo con inteligencia artificial? A lo que Sergio Mata responde que hay que partir de una primera cuestión clave: si se cuenta o no con desarrolladores propios y si el proceso se aborda desde cero. Así, es importante diferenciar entre la adopción de soluciones ya preparadas y el desarrollo de inteligencia artificial como tal. Este desarrollo puede abordarse de dos maneras. Por un lado, mediante el uso de entornos *cloud*, donde los desarrolladores comparten recursos como GPU, especialmente en fases de prueba o en entornos no productivos. Un enfoque, sin embargo, que se ve condicionado por aspectos regulatorios, que pueden complicar su aplicación, especialmente en entornos públicos o en sectores como el sanitario. Por otro lado, una vez que los modelos han sido probados, es necesario llevar esa inteligencia artificial a entornos locales. En este punto, HP está desarrollando, con AMD, una es-



"Los costes ocultos, en el caso del puesto de trabajo digital, fluctúan en función del sector"

Willy Piquer,
experto TIC

> Para evitar zonas ciegas en torno a la conectividad hay que apostar por la automatización y la simplificación de la gestión para reducir tareas rutinarias y minimizar errores

trategia que se centra en estaciones de trabajo con capacidad de procesamiento de IA en local, capaces de ejecutar modelos ya entrenados y gestionar cargas de trabajo directamente en el propio entorno. Este enfoque permite un mayor control, elimina problemas de latencia y reduce costes, limitándose estos al dispositivo y su mantenimiento. Además, facilita el cumplimiento de las regulaciones, siempre que los datos no salgan del entorno controlado.

El soporte y la actualización de estas soluciones se apoyan en *partners* tecnológicos, especialmente a nivel local. Por su parte, el coste asociado al mantenimiento y evolución de los gastos abre la puerta a diferentes enfoques:

> "Están apareciendo numerosas herramientas que provocan un aumento significativo del gasto"

Carlos de Cózar,
director del Área TIC de **Cámara de Valencia**

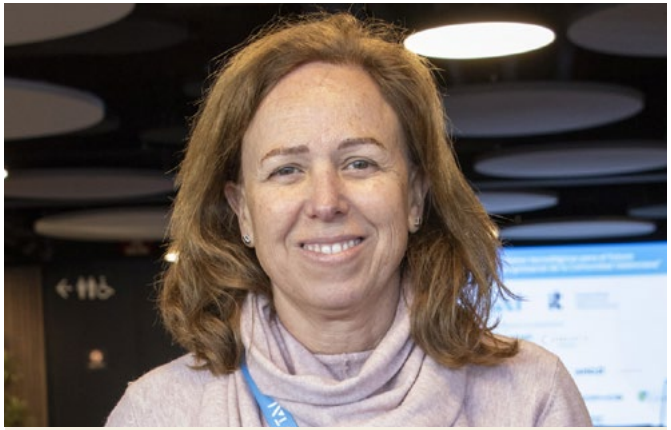
desde contar con desarrolladores propios hasta recurrir a subvenciones o modelos de servicio, aspectos que deben ser evaluados en cada caso, explica.

Más allá de los costes, Simón Viñals plantea otro reto: definir las políticas de uso de la IA, ante lo que Willy Piquer aconseja, a las empresas de menor tamaño, acometer proyectos en los que sepan qué van a hacer. Fernando Feliu avanza que la solución de *digital workplace* de Virtual Cable, UDS Enterprise, permite gestionar y proteger el acceso y uso de los agentes de IA por parte de los usuarios, asegurando entornos controlados y alineados con las políticas de la organización. Y Miguel Ángel Royo confirma que en Nealis ya cuentan con 30 proyectos en producción, entre ellos una aplicación para licitaciones.

Gestión del dato

Gestionar el dato en la era de la IA es otra de las complejidades que tienen que afrontar los CIO. José Raldúa avanza que en DCM SISTEMES están empezando a hacer pruebas con una IA propia, con empleados formateando datos que pasan a la inteligencia artificial. Raldúa reconoce que el proceso no es sencillo por las alucinaciones que sufre la IA.

José Luis Martínez expone los dos proyectos que están llevando a cabo en el ámbito del dato y la IA: su *DataHub*, que une diferentes dominios de conocimiento de Veolia en un úni-



¿Cómo calcular qué va a suponer un proyecto llevado a cabo con inteligencia artificial?

Marta Monleón, subdirectora general de Telecomunicaciones de la **Generalitat Valenciana**

co *datawarehouse* en la nube de Veolia. Por otro lado, un "*Talk to my plant*" sobre IA generativa, es decir, que las personas que operan puedan preguntar con lenguaje natural datos operativos a la planta.

En Ysabel Mora, Néstor Flórez señala también proyectos internos con un modelo de BI analítico con el que dan soporte a los comerciales. Modelo que quieren migrar a una tecnología diferente con el fin de identificar casos de uso.

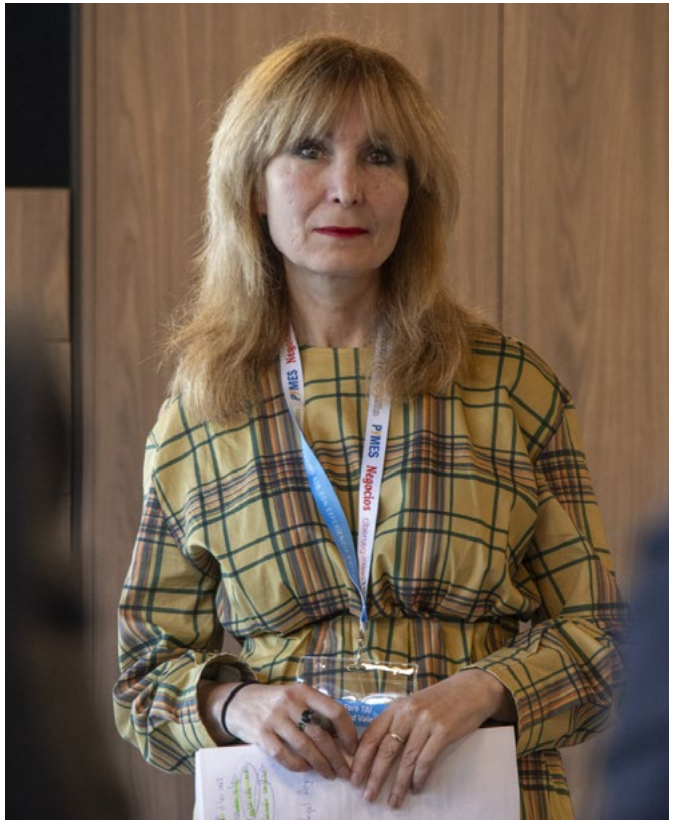
Y en el caso de AR Hotels&Resorts, Lucía Martínez reconoce que desde hace cuatro años están llevando a cabo un *datalake* sobre el que actualmente están construyendo algunas soluciones de IA con un agente conversacional.

Ante todo ello Simón Viñals hace referencia a la importancia de la transparencia algorítmica, desde el punto de vista legal.

¿Cómo evitar zonas ciegas en torno a la conectividad?

Ante la pregunta sobre cómo evitar zonas ciegas en la conectividad, Luis González explica que el principal reto está en la creciente complejidad de las redes y en el cambio del tráfico, cada vez más exigente, lo que puede provocar fallos como la pérdida de paquetes si la infraestructura no está preparada.

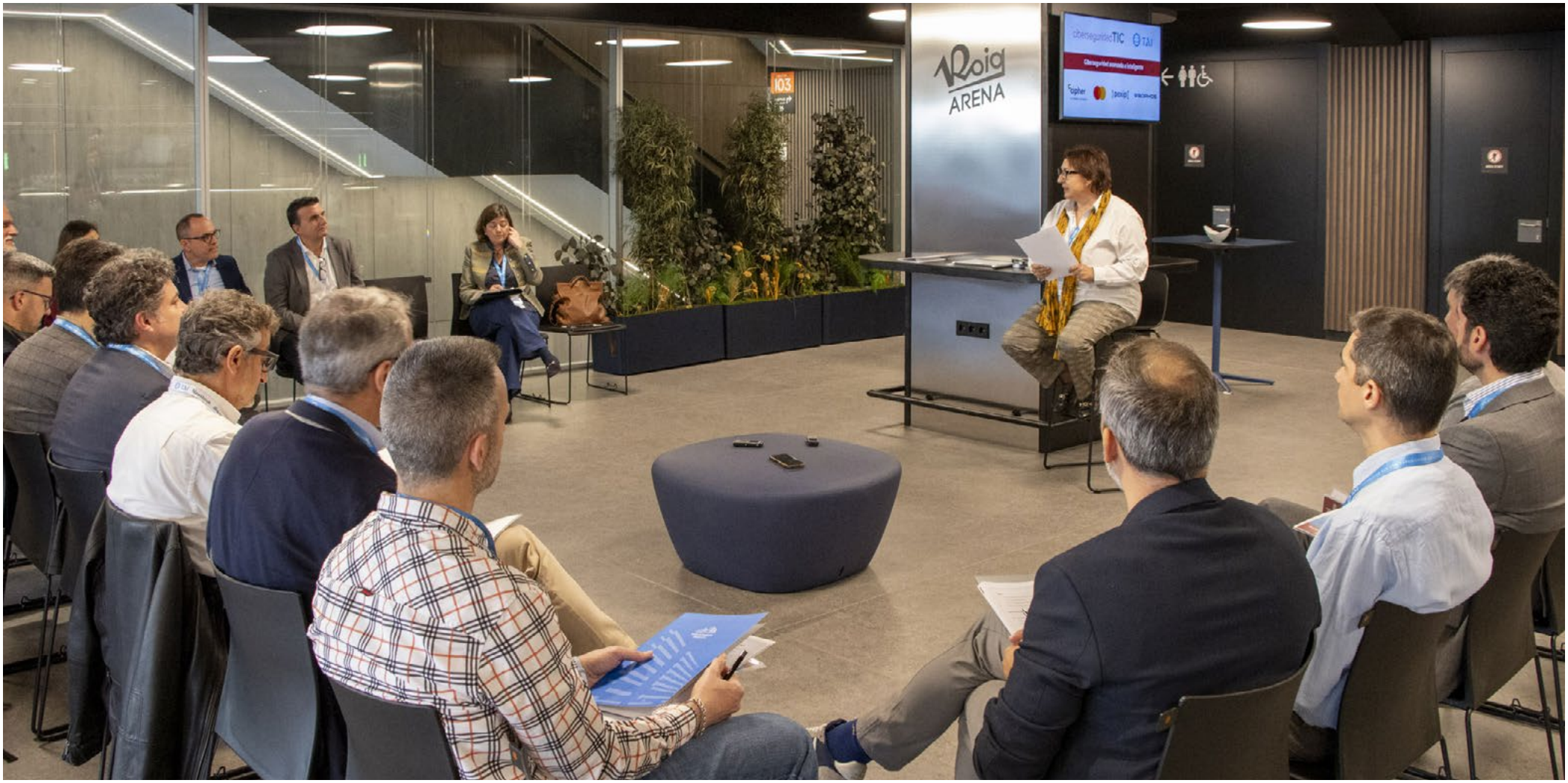
Como consejo destaca apostar por la automatización y la simplificación de la gestión para reducir tareas rutinarias y minimizar errores. También subraya la importancia de contar con



redes homogéneas que integren correctamente entornos IT y OT, evitando puntos débiles.

Además, recomienda mejorar la visibilidad y el control de la red mediante herramientas avanzadas, incluida la inteligencia artificial, que permitan anticiparse a problemas y detectar vulnerabilidades, especialmente ante dispositivos conectados que pueden convertirse en puertas de entrada.

De la visibilidad a la decisión: la ciberseguridad busca su verdadero punto de control



La ciberseguridad atraviesa un momento de transición marcado por la aceleración tecnológica, la presión regulatoria y una creciente complejidad operativa. La irrupción de la inteligencia artificial, la consolidación del *cloud* y la interconexión de entornos digitales han ampliado la superficie de ataque y elevado el nivel de exigencia para las organizaciones. A esto se suma la dificultad para gestionar grandes volúmenes de alertas, la escasez de talento y una dependencia cada vez mayor de terceros, que obligan a replantear cómo se diseñan, operan y gobiernan las estrategias de seguridad.

Rosalía Arroyo

En este contexto, avanzar hacia modelos más resilientes ya no depende solo de incorporar nuevas herramientas, sino de mejorar la capacidad de detección y respuesta, integrar inteligencia de amenazas y gestionar el riesgo en ecosistemas cada vez más complejos. Al mismo tiempo, cuestiones como la protección del dato en entornos de colaboración, el control de las comunicaciones o la soberanía digital empiezan a situarse en el centro del debate, no solo desde una perspectiva técnica, sino también estratégica y de negocio.

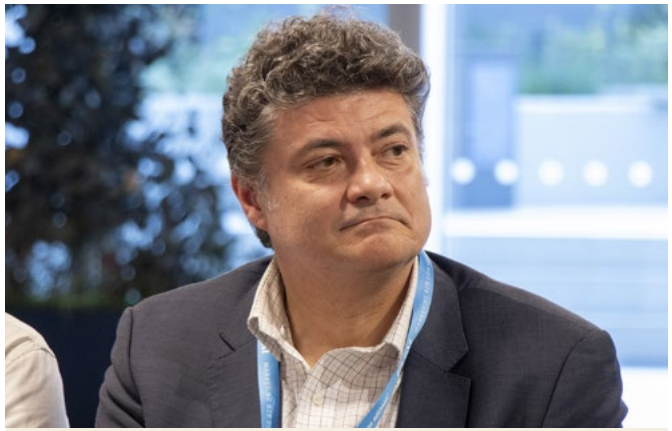
Ese fue el punto de partida del Foro TAI Valencia, Retos tecnológicos para el futuro empresarial, organizado por Grupo TAI junto al COITCV y con la colaboración de Cámara de Valencia, donde responsables de innovación, seguridad y tecnología compartieron cómo están abordando este escenario. A lo largo del encuentro, quedó claro que el reto ya no es solo ver más, sino decidir mejor: ordenar el uso de la tecnología, priorizar riesgos y asumir que la ciberseguridad es, cada vez más, una responsabilidad transversal que afecta a toda la organización.

> La automatización y la IA se perfilan como aliadas imprescindibles para operar en entornos con alta presión de alertas

La visibilidad como punto de partida

La apertura del debate, centrada en visibilidad, detección y respuesta dentro de la ciberresiliencia, dejó una primera conclusión compartida: las tres dimensiones son inseparables, pero la visibilidad sigue siendo el punto de partida.

Adolfo Albaladejo, Jefe de Servicio de Ciberseguridad Industrial de la Generalitat Valenciana, lo situó con claridad al explicar que, en un entorno tan amplio y heterogéneo como el de la Generalitat Valenciana, el reto inmediato pasa por "alimentar el SIEM con suficientes fuentes de información" para tener una visión real de lo que ocurre. Ese esfuerzo, añadía, ya no se limita al ámbito IT tradicional, sino que se está extendiendo también a entornos industriales con el fin de correlacionar mejor la información y reducir puntos ciegos. Mª Ángeles Arqueros, Jefa del Área Seguridad de la Información de Consum S. Coop. V, reforzó esa idea con una frase que resumió bien el consenso inicial: "No puedes proteger lo que no puedes ver". A partir de esa visibilidad,

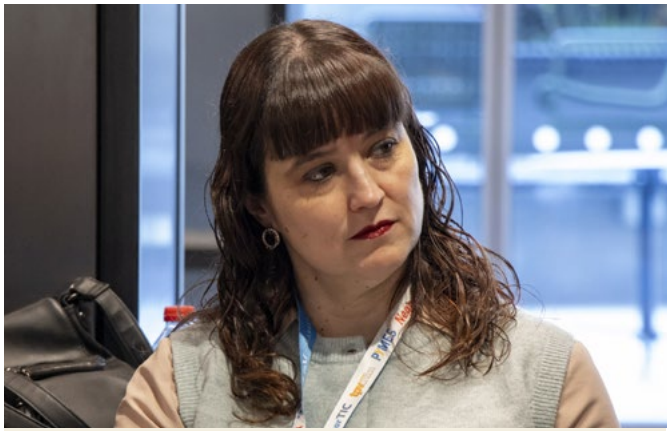


> "La colaboración entre SOC y la federación con el CCN son fundamentales para que la inteligencia de amenazas llegue a tiempo y pueda convertirse en capacidad real de respuesta"

Adolfo Albaladejo Blázquez, jefe de servicio de ciberseguridad industrial, **Generalitat Valenciana**

advertía, empiezan a emerger realidades que muchas organizaciones todavía no controlan del todo, desde el *shadow IT* hasta el *shadow AI*: "Cuando te pones a tirar del hilo, siempre aparecen cosas que necesitas gobernar".

Javier Ripoll, Responsable de la Seguridad de la Información del Instituto de Investigación Sanitaria La Fe, incidió en que la visibilidad no es un fin en sí mismo, sino la base que permite entender el alcance de un incidente. "Si tienes visibilidad de qué sistemas están siendo atacados, puedes ver las dependencias y los datos que pueden verse afectados", explicaba. Desde el lado del patrocinador, Joana Caetano, Regional Sales Manager de CIPHER, coincidía en que la visibilidad es "el cimiento de todo", porque "alimenta la detección y la detección es lo que permite una respuesta rápida y quirúrgica", aunque introdujo un matiz relevante: más que la ausencia de visibilidad, el gran problema actual es su fragmentación. Lo ilustró con una imagen muy clara: muchas organizaciones funcionan "como una casa en la que hay un vigilante en cada habitación, pero que no se hablan entre ellos". En entornos donde convergen *cloud*, OT, IoT e infraestructuras distribuidas, esa falta de conexión entre piezas dificulta una respuesta coordinada.



> "Lo que no ves no lo puedes proteger; la visibilidad es la base para poder detectar, gobernar y responder"

Mª Ángeles Arqueros Moltó, jefa del Área Seguridad de la Información, **Consum S. Coop. V**

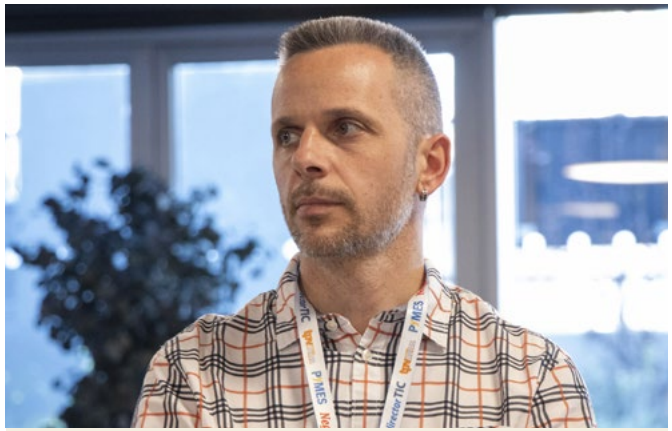
De ver a actuar: la importancia de la respuesta

A partir de ahí, el debate se desplazó hacia la capacidad real de reacción. Iván Mateos, *Sales Engineer* de Sophos, reconocía que "sin visibilidad no tienes por dónde empezar", pero ad-

vertía de que eso, por sí solo, no protege. “Por mucha visibilidad que tengas, si tienes un panel lleno de alertas, eso no te defiende de nada”, resumía. En su opinión, la diferencia está en la rapidez con la que una organización es capaz de detectar y responder, porque “no tiene nada que ver responder en 20 minutos, en horas o en semanas”.

Mastercard amplió el foco al recordar que la ciberresiliencia ya no puede analizarse solo desde la infraestructura propia. “La superficie de ataque, ha cambiado radicalmente con el *cloud*, el teletrabajo y la creciente dependencia de terceros. El 57% de los profesionales especializados en fraude no son conscientes de las brechas cibernéticas hasta que las pérdidas ya se han materializado”, apuntó la compañía, introduciendo una idea que reaparecería después: la necesidad de pasar de un enfoque reactivo a uno más proactivo y de entender la ciberresiliencia como una responsabilidad de toda la organización, “incluyendo al CEO y a cualquier área de la compañía”.

Leopoldo Salinas, tesorero del COIT de la Comunidad Valencioana, remató esa reflexión al introducir una “cuarta pata”: el negocio. A su juicio, “no puede ser el CISO el que decida qué hay que proteger”, porque esa decisión debe formar parte de una estrategia global de empresa.



> “Tenemos que pasar de ser una organización fácilmente atacable a ser una organización fácilmente defendible”

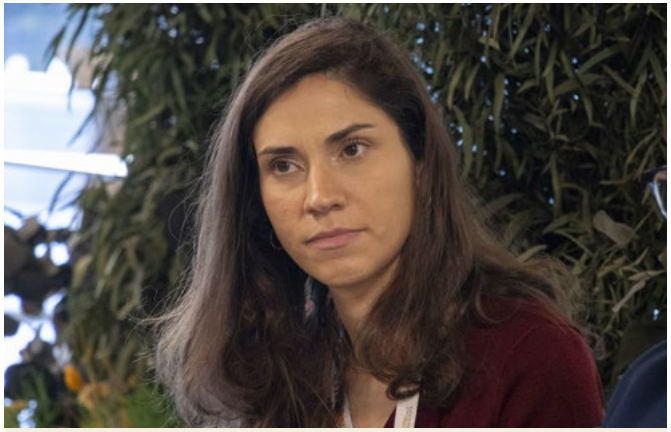
Javier Ripoll Esteve, Responsable de la Seguridad de la Información del**Instituto de Investigación Sanitaria La Fe**

> La soberanía digital gana protagonismo como elemento estratégico

Inteligencia de amenazas: del dato a la decisión

La conversación avanzó así hacia la inteligencia de amenazas y su papel real en la toma de decisiones. Aquí emergió una idea bastante clara: las organizaciones están avanzando hacia modelos más proactivos, pero todavía conviven con dinámicas reactivas difíciles de eliminar.

Javier Ripoll lo explicaba de forma muy directa al reconocer que, en su caso, la aproximación es “algo mixta entre ser proactivo y el día que venga la amenaza”. Es decir, se intenta anticipar, pero la operación diaria sigue obligando a reaccionar ante incidentes que no siempre se pueden prever. Aun así, describió una evolución progresiva hacia ese enfoque más proactivo, apoyada en la mejora de la monitorización, la correlación de eventos y la vigilancia tecnológica, así como en pruebas de seguridad sobre nuevas aplicaciones antes de su despliegue.



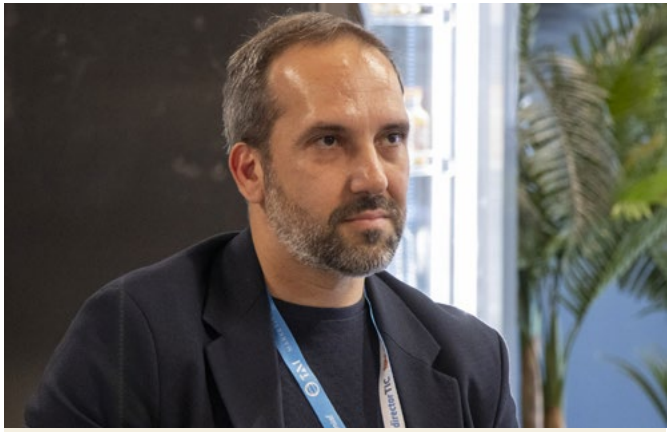
"Ninguna empresa puede externalizarlo absolutamente todo: hace falta un modelo de corresponsabilidad entre el conocimiento interno y la capacidad operativa externa"

Joana Caetano,
Regional Sales Manager, **CIPHER, a Prosegur company**

Este tipo de prácticas, apuntaba, les permite ganar visibilidad sobre su exposición —incluyendo información que puede estar circulando fuera de la organización— y entender mejor por dónde pueden materializarse los riesgos.

Antonio Orduña, jefe del área de seguridad y calidad de los sistemas de información del Hospital La Fe, coincidió en que la inteligencia de amenazas se ha vuelto clave, más aún en un momento en el que "los atacantes ya usan inteligencia artificial" y las organizaciones necesitan automatizar parte de su defensa. En su caso, puso en valor el ecosistema público valenciano y la colaboración entre la DGTIC, el CSIRT-CV y los recursos de la propia Conselleria. Pero quiso subrayar algo más: anticipar está bien, pero tan importante como eso es saber cómo responder. Por eso defendió que "es fundamental tener un *checklist* para no tomar decisiones improvisadas" y entrenar esa respuesta mediante ejercicios de ciberresiliencia.

Ramón Onrubia, director máster ciberseguridad de CIPFP Mislata - Conselleria d'Educació, aportó una perspectiva especialmente interesante desde el ámbito formativo. Explicó que en el máster de ciberseguridad trabajan con un entorno simulado que replica la lógica de un SOC



"Por mucha visibilidad que tengas, si tienes un panel lleno de alertas, eso no te defiende de nada"

Iván Mateos,
Sales Engineer de **Sophos**

real, alimentado con fuentes de inteligencia y plataformas como MISP (Malware Information Sharing Platform & Threat Sharing) para que el alumnado aprenda a operar con escenarios cercanos a los que encontrará después en una empresa. Desde su punto de vista, la inteligencia de amenazas "es fundamental", no sólo por

el uso de *feeds* o indicadores de compromiso, sino porque obliga a entender la seguridad como un ejercicio de colaboración. Esa dimensión colaborativa la reforzó también Adolfo Albaladejo al recordar que el primer CSIRT autonómico de España nació precisamente en la Comunidad Valenciana en 2007 y que muchas veces la inteligencia no se genera dentro, sino que "te llega gracias a esa federación de SOC" impulsada a través del CCN y de la red nacional. Esa visión contrastó con la realidad de organizaciones de menor tamaño. José García de la Guía, CIO de la Autoridad Portuaria de Castellón, advertía de que todo este despliegue resulta "maravilloso" cuando se habla de grandes estructuras, pero mucho más difícil de sostener con recursos limitados. En esos casos, defendía, no queda otra que apoyarse en estructuras superiores o en servicios externos. Mª Ángeles Arqueros lo resumía en términos muy prácticos: en muchas organizaciones el SOC está externalizado porque "es muy difícil tener personal suficiente" y, en muchos casos, "no tiene sentido" intentar asumir internamente una especialización tan exigente.

Desde Mastercard se aprovechó este bloque para conectar la inteligencia de amenazas con la propuesta de la compañía. Se recordó que la compra de Recorded Future respondía precisamente a ese valor estratégico, al tiempo que se

"Herramientas hay; el problema es gobernarlas, configurarlas bien y ser capaz de ejecutar de verdad las reglas que te has dado"

José García de la Guía,
CIO, **Autoridad Portuaria de Castellón**

subrayó que Mastercard no solo ofrece soluciones de inteligencia, sino que la aplica de forma masiva en sus propias operaciones. "Cuando analizamos las transacciones detectamos en tiempo real y realizamos rechazos proactivos de transacciones de prueba fraudulentas", explicaba, mostrando cómo esa inteligencia se traduce en protección activa frente al fraude. "Sin inteligencia de amenazas sería inviable", añadía.

Gobernanza, IA y control del dato

El debate entró después en un plano más estratégico al abordar qué debería ser hoy prioritario para los responsables de tecnología y ciberseguridad en un contexto marcado por la IA, el *cloud* y la regulación. Aquí la idea más repetida fue que, antes de hablar de herramientas, hace falta gobernanza. José García de la Guía lo resumió en dos palabras: "Racionalidad y gobernanza". Para ilustrarlo, apuntó a un uso cada vez más extendido de herramientas de IA generativa en el entorno profesional sin un marco claro de control. En su opinión, muchos usuarios trabajan con este tipo de soluciones sin ser plenamente conscientes de las implicaciones que puede tener el uso

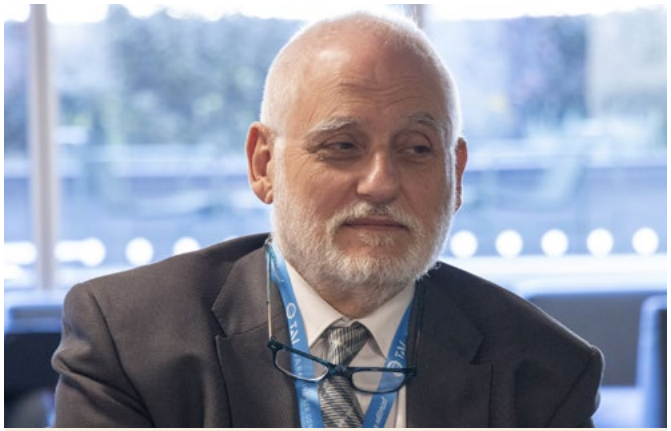
> “La inteligencia solo tiene valor si es accionable: si no sabes cómo te afecta una amenaza y qué tienes que hacer, no te sirve de nada”
>
> **Mastercard**

de información sensible en plataformas externas. “El 95 % de los usuarios no tienen ni idea de las consecuencias que tiene hacer lo que hace”, advertía. Por eso defendió que la gobernanza y la educación deben situarse ya como “paso cero”.

Leopoldo Salinas insistió en que esta supervisión no puede recaer solo en seguridad, sino que exige una visión global desde la dirección, porque “lo que no se supervisa no ocurre más que por la conducta personal”. Mª Ángeles Arqueros coincidió en que la seguridad ha ganado visibilidad interna, pero de forma todavía superficial. Se la reconoce más, sí, pero muchas veces sigue siendo el área de “los que dicen que no”. Y eso provoca que algunos usuarios ni siquiera consulten. Antonio Broseta, *Corporate IT Manager* de CSPSpain, amplió esta idea al señalar que la gobernanza ya no puede mantenerse en los marcos anteriores. La llegada de la IA, del *cloud* y de normativas como NIS2 o CER obliga, a su juicio, a reformularla desde arriba: primero reglas, luego políticas, después procedimientos y, finalmente, tecnología. Todo ello está empujando, además, a revisar estructuras internas y a plantear una mayor separación entre IT y ciberseguridad.

La conversación aterrizó entonces en las herramientas de colaboración y en el impacto de la IA sobre ellas. Joana Caetano reconoció que, muchas veces, la tecnología entra antes por el usuario que por el departamento de IT. “La IA llegó antes a los hogares que a las empresas”, resumía, lo que obliga a reaccionar deprisa, regular y ordenar después su adopción. Puso como ejemplo los resúmenes automáticos en Teams y el desconcierto que se produce cuando se explica que ese dato “se ha quedado fuera”, que ha salido del perímetro corporativo y puede haber sido procesado por terceros. De ahí su defensa de una IA “sí, pero regulada, gobernada”.

Fue precisamente ahí donde Valentín Martín, director de canal de Pexip, introdujo uno de los conceptos más sólidos del encuentro: la sobera-



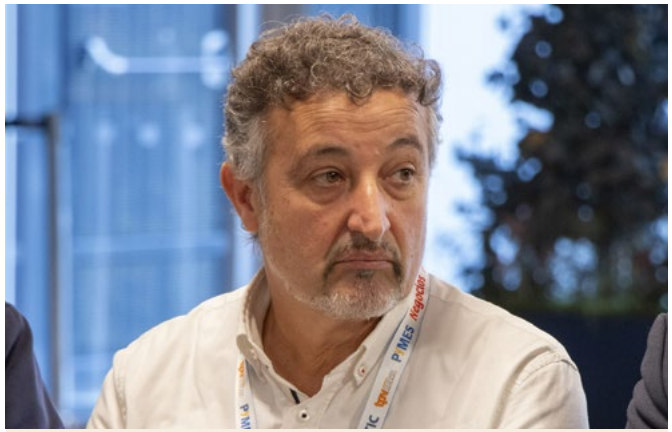
> “No puede ser el CISO el que decida en solitario qué hay que proteger; esa es una decisión empresarial completa”
>
> **Leopoldo Salinas,** Tesorero, **COIT CV**

nía del dato. En su opinión, muchos de los temas que habían aparecido —visibilidad, gobernanza, cumplimiento— se podían resumir en eso: "Saber dónde tenemos el dato, controlarlo". Recordó que en una sesión de Teams, Zoom o Webex no solo se intercambia voz o vídeo, sino también un gran volumen de metadatos —protocolos, puertos, IP, dispositivos o registros de sesión— que, si quedan fuera de control, pueden convertirse en información útil para un atacante. Además, vinculó directamente esta cuestión con NIS2, no sólo por las obligaciones de gobernanza, sino también por el componente sancionador que muchas organizaciones aún no han terminado de interiorizar. Antonio Orduña coincidió en que este marco regulatorio, aunque "genera trabajo" y obliga a salir de la zona de confort, también puede convertirse en una palanca para alinear a la dirección y hacer visible que la seguridad exige estructura, inversión y acreditación.

Capacidades internas vs. servicios externos

Otro de los grandes ejes del debate fue el equilibrio entre capacidades internas y apoyo externo en áreas como SOC, *threat hunting* o respuesta ante incidentes. Aquí el consenso fue amplio: para muchas organizaciones, especialmente públicas o medianas, una cobertura completamente interna no es realista. José García de la Guía lo expresó sin rodeos: con recursos propios "sería imposible". Adolfo Albaladejo explicó que la Generalitat sí ha reforzado claramente su estructura, apoyándose en un SOC que ha ido creciendo y en una apuesta por ampliar cobertura en sectores críticos. Javier Ripoll, por su parte, describió un escenario más ajustado, en el que el equipo combina funciones de ciberseguridad y sistemas mientras intenta trasladar a la dirección la necesidad de externalizar determinadas capacidades.

Ramón Onrubia llevó esta reflexión al tejido empresarial más pequeño con una imagen muy sencilla: "Zapatero a tus zapatos". Una empresa que no vive de la ciberseguridad, sostenía, no puede aspirar a tener dentro todos los perfiles necesarios. De ahí que defendiera fórmulas como el CISO virtual o los servicios profesionales compartidos, aunque matizando que siempre debe existir dentro una figura capaz de hablar con ese SOC externo y tomar decisiones. Joana Caetano habló, en este sentido, de un "modelo de corresponsabilidad". Se puede



"Los atacantes ya usan inteligencia artificial, así que nosotros tenemos que automatizar y apoyarnos en inteligencia de amenazas para adelantarnos"

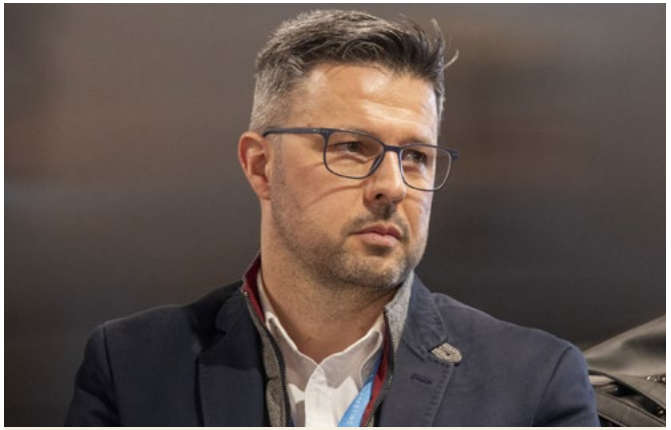
Antonio Orduña Galán, Jefe del área de seguridad y calidad de los sistemas de información, **Hospital La Fe**

> "No basta con esperar a los indicadores de compromiso; hay que fijarse también en los indicadores de ataque y en los comportamientos anómalos"
>
> **Ramón Onrubia Pérez,** Director máster ciberseguridad, **CIPFP Mislata - Conselleria d'Educació**

externalizar mucho, pero hay un conocimiento del negocio que solo existe dentro. "Esa inteligencia de negocio solo va a tenerla quien está dentro", recordaba. José García y Leopoldo Salinas reforzaron esa idea desde otro ángulo: se pueden delegar tareas, pero no la responsabilidad. Tener proveedores "no exime de la responsabilidad de ser clientes".

Del IOC al comportamiento: detectar antes de que ocurra

A partir de ahí, la conversación volvió a la inteligencia de amenazas, pero ya desde otra perspectiva: no tanto la disponibilidad de datos como su verdadero valor. Álvaro Fides, Investigador Desarrollador Senior en SABIEN - Instituto ITACA, abrió este bloque recordando que anticipación y protección activa forman parte de una misma secuencia: "No es tanto que una tenga precedencia sobre la otra, sino que una viene antes que la otra". Javier Ripoll recuperó entonces una idea atribuida a Javier Candau: el reto es pasar de ser una organización "fácilmente atacable" a una "fácilmente defendible". Ramón Onrubia desarrolló esta idea con más detalle al insistir en que hay que ir más allá de los IOC y poner el foco también en los IOA, es decir, en indicios de comportamiento anómalo



> "La clave es convertir la seguridad en un hábito, en algo casi instintivo dentro de la organización"
>
> **Antonio Broseta,** Corporate IT Manager **CSPSpain**

que apuntan a que algo está ocurriendo o está a punto de ocurrir; "No es que te anticipes del todo, es que estás detectando que ya te están atacando o están a punto de hacerlo", resumía. Joana Caetano conectó esa idea con la necesidad de cruzar comportamiento interno e inteligencia contextual externa, mientras que

Mª Ángeles Arqueros aportó el contrapunto operativo: la anticipación implica también lidiar con “la cantidad de falsos positivos que tienes que gestionar”. Desde Mastercard se sintetizó bien el punto central del bloque al defender que la inteligencia solo tiene valor si es accionable. Acumular direcciones IP, indicadores o señales no basta si no se sabe qué hacer con ellos, cómo afectan al negocio o qué prioridad merecen. De ahí la importancia de perfilar amenazas según el tipo de organización, su sector, su tamaño o su geografía.

Colaboración, herramientas y límites del control

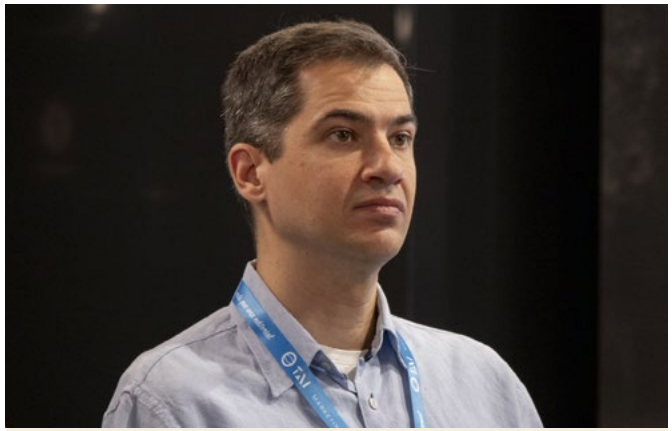
En la recta final, el debate se centró en las herramientas de colaboración y en las limitaciones que presentan cuando se comparte información sensible. José García de la Guía fue claro al señalar que el problema no está en la ausencia de tecnología, sino en la dificultad de “gobernarla y configurarla” bien. Se pueden bloquear p*endrives* y desplegar controles, pero si luego el usuario utiliza OneDrive, Google Drive o funciones de IA integradas en esos entornos sin un marco claro, el riesgo se desplaza y se multiplica. Antonio Orduña coincidió en que no existe una forma de limitarlo todo sin afectar a la operativa. Se pueden cerrar puertos USB o restringir descargas en Teams, sí, pero siempre existirá una foto al monitor o un método alternativo. De ahí que la seguridad dependa también de la formación y del compromiso del empleado.

“Muchos de los conceptos que hemos comentado se pueden resumir en uno: soberanía del dato”

Valentín Martín, director de canal, **PEXIP**

Valentín Martín introdujo aquí otro de los elementos diferenciales de la jornada: la interoperabilidad y, de nuevo, la soberanía. Recordó que muchas organizaciones conviven con entornos dispares —Teams, Zoom, Webex, Google Meet— y que esa falta de interoperabilidad es una limitación práctica muy real. Pero fue más allá cuando habló del impacto de la IA sobre las reuniones. Si una herramienta supuestamente segura externaliza la transcripción, el resumen o la traducción a una *cloud* externa, la pregunta clave es evidente: “¿Dónde se ha quedado toda esa información?”. Frente a ello, explicó la apuesta de Pexip por motores de inteligencia privada desplegados en nubes dedicadas para que la información no salga del perímetro ni alimente modelos ajenos.

El cierre volvió a un problema muy concreto: la presión operativa diaria de los equipos de seguridad. Aquí, de nuevo, las respuestas combinaron automatización, externalización e integración. Javier Ripoll explicó que están intentando reducir complejidad, integrar consolas y automatizar



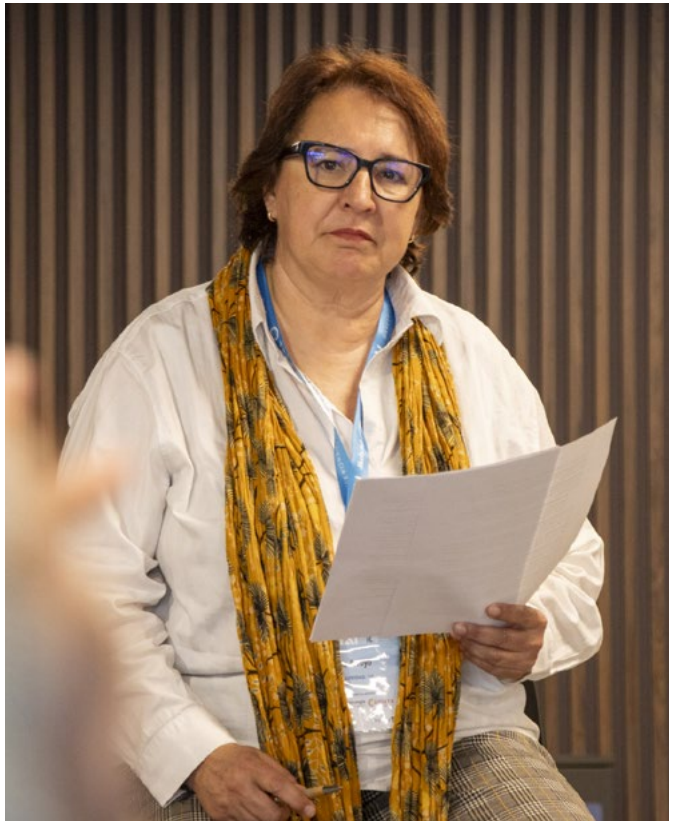
> "La primera medida para mitigar riesgos es identificar dónde están los datos, quién accede a ellos y con qué permisos"

Álvaro Fides Valero, Investigador Desarrollador Senior, **SABIEN - Instituto ITACA**

procesos, pero sin renunciar a tareas manuales esenciales apoyadas en guías y tickets automatizados para que "esas cosas no se nos pasen". Adolfo Albaladejo describió un entorno más maduro en automatización, con reglas preaprobadas que permiten responder a ciertos ataques sin necesidad de levantar al CISO a las tres de la mañana. Iván Mateos, desde Sophos, aportó una doble lectura: por una parte, automatización e inteligencia artificial son imprescindibles para operar a escala; por otra, los fabricantes deben asumir más responsabilidad y aplicar de verdad el *security by design*. "El fabricante no puede formar parte del problema", advertía.

> La evolución de las amenazas impulsa a las organizaciones a pasar a modelos cada vez más proactivos

Ramón Onrubia reforzó el valor de la automatización como herramienta para liberar a los analistas de tareas repetitivas y reservar su tiempo para incidentes que realmente exigen criterio. Y ya en los últimos minutos emergió un último gran tema: la soberanía digital. Valentín Martín citó el caso de Francia y su decisión de avanzar hacia una nube soberana tras comprobar hasta qué punto la dependencia tecnológica puede convertirse en un problema estratégico. Joana Caetano añadió que, en un contexto geopolítico cambiante, no es descartable que Europa y España empiecen a apostar con más fuerza por tecnología propia. La conclusión de fondo era evidente: la ciberseguridad ya no se juega solo en la tecnología, sino también en quién la controla, dónde reside el dato y bajo qué jurisdicción opera.



“La Comunidad no solo aporta PIB, también un modelo productivo basado en la industria, la exportación y el emprendimiento”

Competitividad, diversidad y vocación internacional. El tejido productivo de la Comunidad Valenciana atesora un enorme valor y exhibe un estable crecimiento, lo que le permite a Carlos de Cózar, director del área TIC de la Cámara de Comercio de Valencia, defender su importante papel como motor de la economía española. Un tejido en el que la digitalización es materia obligatoria para acelerar su productividad y competitividad.

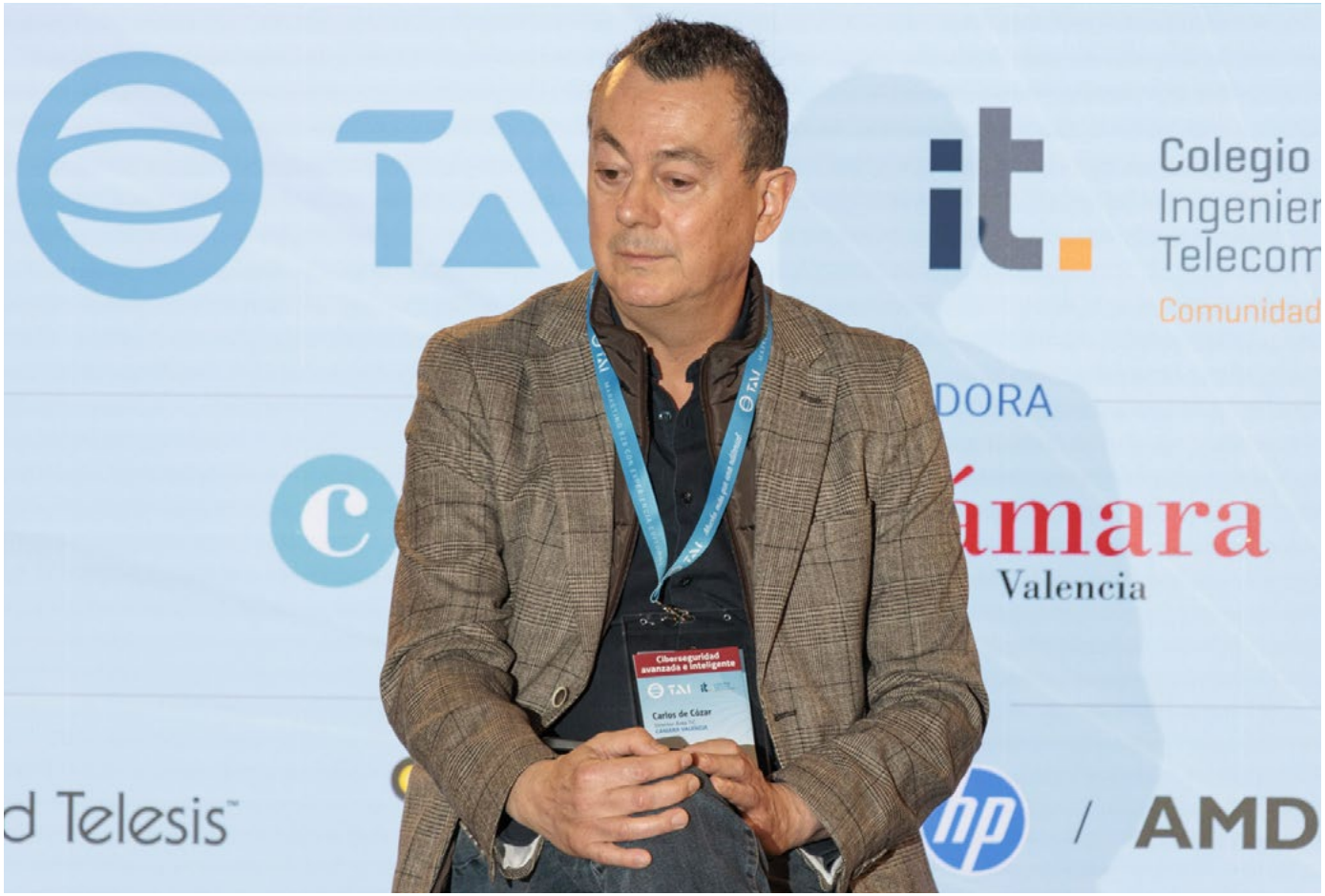
Marilés de Pedro

La Comunidad Valenciana es el cuarto motor de la economía española con un peso en torno al 10 % en el PIB español. ¿Qué valor aporta a la riqueza económica española? ¿Qué rasgos la hacen diferente?

La Comunidad Valenciana aporta un valor económico muy relevante por la diversidad y equilibrio de su tejido productivo, que combina sectores tradicionales altamente competitivos —como la agroalimentación, el calzado, la cerámica o el mueble— con sectores industriales y de servicios avanzados con un alto potencial de crecimiento. Esta combinación le permite ser resiliente ante los cambios de ciclo y actuar como un motor estable dentro de la economía española.

Uno de sus rasgos diferenciales es su vocación claramente internacional, apoyada en una sólida red logística, portuaria y empresarial, así como en una cultura históricamente orientada

> “La digitalización es hoy un factor crítico para competir fuera”



a los mercados exteriores. A ello se suma un ecosistema de pymes muy dinámico, con capacidad de adaptación, y una creciente conexión con el conocimiento, la innovación y el talento que generan las universidades, centros tecnológicos y parques científicos de la región.

Desde el punto de vista económico, la Comunidad no solo aporta PIB, sino también un modelo productivo basado en la industria, la exportación y el emprendimiento, que resulta clave para la competitividad del conjunto del país.

Se trata de una región con un perfil claramente exportador. Las exportaciones suponen el 27 % del PIB regional, representando el 9,6 % de las ventas de España. ¿Cómo valoraría el grado de digitalización de las empresas valencianas exportadoras? ¿Qué importancia concede a la digitalización para competir en los mercados internacionales?

El grado de digitalización de las empresas valencianas exportadoras es desigual, aunque presenta una evolución claramente positiva en los últimos años. Existen compañías muy avanzadas, especialmente aquellas que han integrado la tecnología en su estrategia de negocio y no solo en los procesos operativos. Estas empresas están utilizando sistemas de gestión integrados, analítica de datos, automatización, comercio digital o herramientas colaborativas para mejorar su competitividad en los mercados internacionales.

En paralelo, aún hay pymes exportadoras que se encuentran en fases más iniciales de este proceso. Precisamente para acompañarlas resulta clave el papel de la Cámara Valencia, a través de iniciativas como la Oficina de Transformación Digital Acelera Pyme, que ofrece asesoramiento especializado, diagnóstico digital y acompañamiento práctico para abordar la transformación con visión y realismo.

La digitalización es hoy un factor crítico para competir fuera: permite ganar eficiencia, reducir costes, mejorar la trazabilidad, cumplir requisitos normativos internacionales y responder con mayor rapidez a las demandas del mercado. En un entorno global cada vez más exigente, competir no es solo una cuestión de producto, sino de capacidad tecnológica, gestión de la información y agilidad, y en ese contexto la transformación digital se convierte en un elemento imprescindible para la internacionalización.

¿Qué debería mejorar en la colaboración entre instituciones, universidades y empresas para acelerar la digitalización del tejido productivo valenciano?

> "Para acelerar la digitalización del tejido productivo valenciano es fundamental reforzar la colaboración real y continua entre instituciones, universidades y empresas"

Para acelerar la digitalización del tejido productivo valenciano es fundamental reforzar la colaboración real y continua entre instituciones, universidades y empresas, evolucionando desde iniciativas puntuales hacia ecosistemas estables orientados a resultados.

Es clave mejorar la transferencia efectiva de conocimiento, facilitando que la innovación, la tecnología y el talento que se generan en universidades y centros de investigación lleguen de forma práctica y accesible a las empresas, especialmente a las pymes. En este ámbito, espacios como el Ecosistema Tecnología para los Negocios de Cámara Valencia permiten conectar oferta tecnológica y necesidades empresariales, favoreciendo proyectos concretos y aplicables.

Las instituciones, por su parte, deben seguir actuando como elemento tractor, alineando políticas, programas y recursos, y ofreciendo a las empresas referentes claros. Iniciativas de divulgación y sensibilización como el Congreso GoDigital ayudan a generar cultura digital, compartir casos de éxito y acercar la transformación digital desde una perspectiva práctica y comprensible para el empresariado.

En definitiva, la digitalización no es solo una cuestión tecnológica, sino de personas, cultura y colaboración. Cuando empresa, academia e instituciones trabajan de forma coordinada, la capacidad de impacto se multiplica. La Comunidad Valenciana dispone de un ecosistema muy sólido para avanzar con rapidez en este proceso.

“Las redes tienen que ser totalmente seguras y autónomas”

En plena aceleración de la transformación digital, la red ha dejado de ser una infraestructura técnica para convertirse en un pilar estratégico de la competitividad empresarial. Así lo señala Luis González, director de Allied Telesis, quien resume esta evolución afirmando que “se ha pasado de no significar nada a que una empresa no funcione si no está conectada”. En la actualidad, cualquier proceso dentro de una organización depende de la conectividad, lo que obliga a reforzar su estabilidad, disponibilidad y seguridad. Este nuevo escenario plantea retos importantes, especialmente la creciente complejidad de las infraestructuras y la falta de talento cualificado. “El talento es escaso y a las empresas les cuesta encontrar personas capacitadas”, advierte Luis González, que defiende la automatización como vía para simplificar la gestión sin depender de perfiles altamente especializados. En este contexto, las redes autónomas cobran protagonismo y permiten liberar a los CIO para un rol más estratégico.

Luis González, director de **Allied Telesis**

Allied Telesis™

Cipher: “El problema no es la falta de herramientas, es no darles contexto para tomar decisiones”

La ciberseguridad ha dejado de centrarse solo en la prevención para convertirse en un ejercicio continuo de detección, respuesta y adaptación. Así lo explica Francisco de Asís Quintero, arquitecto de preventa de Cipher, al señalar que “ser ciberresiliente es, lo primero, asumir que te van a atacar”.

En este contexto, uno de los principales problemas sigue siendo la falta de visibilidad. “No conocemos lo que tenemos, no conocemos el nivel de riesgo”, advierte, a lo que se suma la fragmentación de herramientas y el exceso de alertas sin contexto. “Si la alerta viene sin contexto, no vamos a ser capaces de identificar un riesgo”.

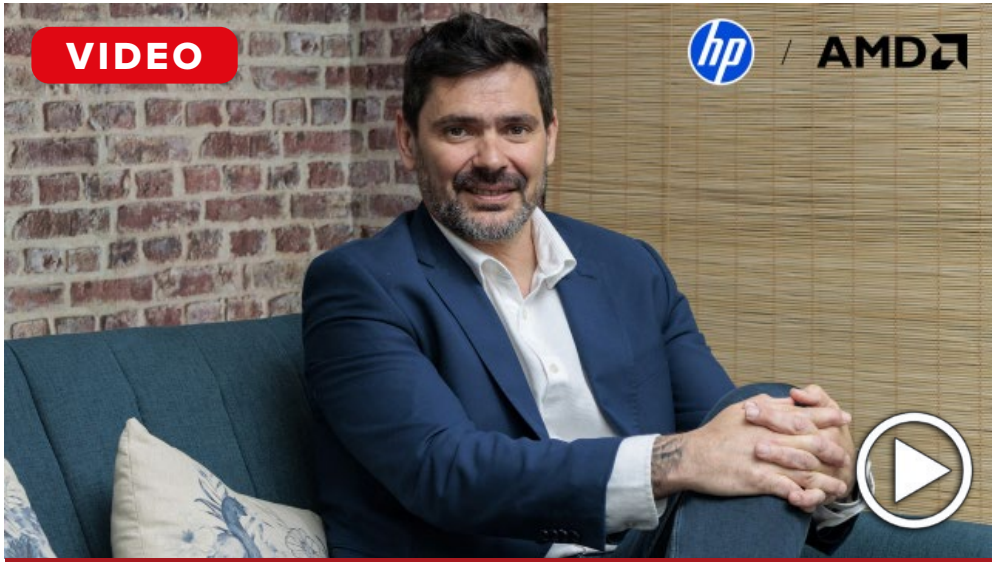
Para afrontarlo, defiende integrar tecnología, inteligencia y automatización para correlacionar información y facilitar la toma de decisiones.

Francisco de Asís Quintero, arquitecto de preventa de **Cipher**

cipher
a Prosegur company

Tecnología, experiencia de usuario, IA y seguridad: pilares de HP en el puesto de trabajo

Ser reconocida como la empresa del trabajo: ese es el reto que va a marcar la estrategia de HP en los próximos años. Con una propuesta que, según explica Sergio Mata, responsable del equipo de preventa de la compañía, va mucho más allá del dispositivo, está redefiniendo el puesto de trabajo a través de un enfoque integral que combina la experiencia de usuario, una seguridad avanzada y el impulso de la inteligencia artificial, especialmente en el *edge*. Su plataforma Workforce Experience Platform se sitúa en el centro, permitiendo optimizar la experiencia digital de los empleados y facilitando la labor de los administradores.

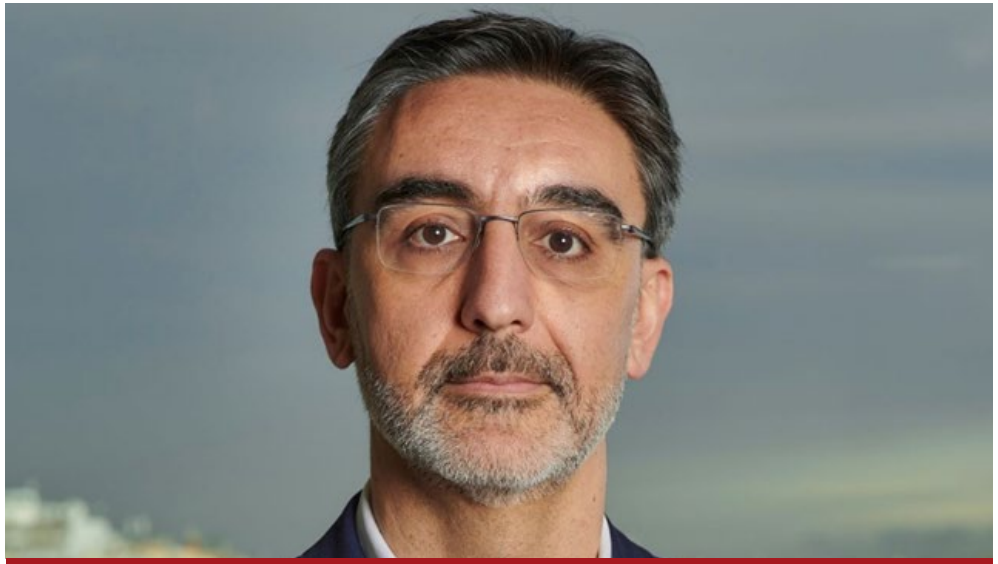


Sergio Mata, responsable del equipo de preventa de **HP**

La nueva frontera de la confianza digital: por qué el comercio a través de agentes exige una seguridad verificable

La seguridad ha dejado de ser un coste para convertirse en la base de la confianza digital. En un contexto donde el cibercrimen no deja de crecer, ya no basta con proteger, sino que es necesario anticipar, resistir y adaptarse. Los ataques se dirigen cada vez más a las personas, con la ingeniería social como vector principal, y muchos fraudes comienzan antes del propio pago.

Ante este escenario, el enfoque pasa por combinar inteligencia artificial, análisis en tiempo real y modelos de protección multicapa que permitan actuar antes, durante y después del ataque. Al mismo tiempo, la irrupción de agentes de IA en el comercio introduce nuevos retos, donde la confianza debe ser verificable. Convertir datos en decisiones y adelantarse al riesgo será clave en esta nueva etapa.



Alberto López, vicepresidente y responsable de Fraude y Crimen Financiero, **Mastercard**

Nunsys sitúa el puesto de trabajo en el centro de la transformación digital

El puesto de trabajo atraviesa la mayor transformación de los últimos 20 años, impulsada por la digitalización, el trabajo híbrido y la inteligencia artificial. Así lo explica Esteban Rueda, gerente de negocio de *Workplace* de Nunsys, en este vídeo. El directivo destaca que el entorno laboral ha dejado de ser físico para convertirse en un ecosistema conectado y seguro. La ciberseguridad, basada en identidad, *Zero Trust* y la automatización se consolidan como un pilar clave frente a amenazas crecientes, confirma, mientras la IA promete un salto de productividad, siempre que esté respaldada por una sólida gobernanza del dato. En este escenario, Grupo Nunsys despliega proyectos integrales que combinan modernización, automatización, IA generativa y seguridad avanzada, posicionando el puesto de trabajo como eje estratégico de la transformación digital empresarial.

Esteban Rueda, gerente de negocio de *Workplace* de **Nunsys**

nunsys
Tu socio tecnológico ®

Pexip: “Las herramientas de videoconferencia dejan una huella digital en cada llamada”

“No tiene mucho sentido mantener una infraestructura securizada y luego apoyarnos en servicios compartidos para procesar ese contenido”. Con esta reflexión, Valentín Martín, Director de Canal Iberia & LATAM de Pexip, plantea uno de los retos clave de la videocolaboración: el control del dato en entornos cada vez más digitales y apoyados en inteligencia artificial.

Las herramientas de colaboración son ya críticas en la operativa diaria, impulsadas por el trabajo híbrido y la digitalización, lo que sitúa la seguridad en primer plano, especialmente en sectores regulados.

Advierte también Valentín Martín de que el riesgo no está solo en lo que se comparte, sino en lo que se genera alrededor. “Las herramientas de videoconferencia dejan una huella digital en cada llamada”, explica, en referencia a metadatos que pueden facilitar la detección de vulnerabilidades si no se protegen adecuadamente.

Valentín Martín, Director de Canal Iberia & LATAM de **Pexip**

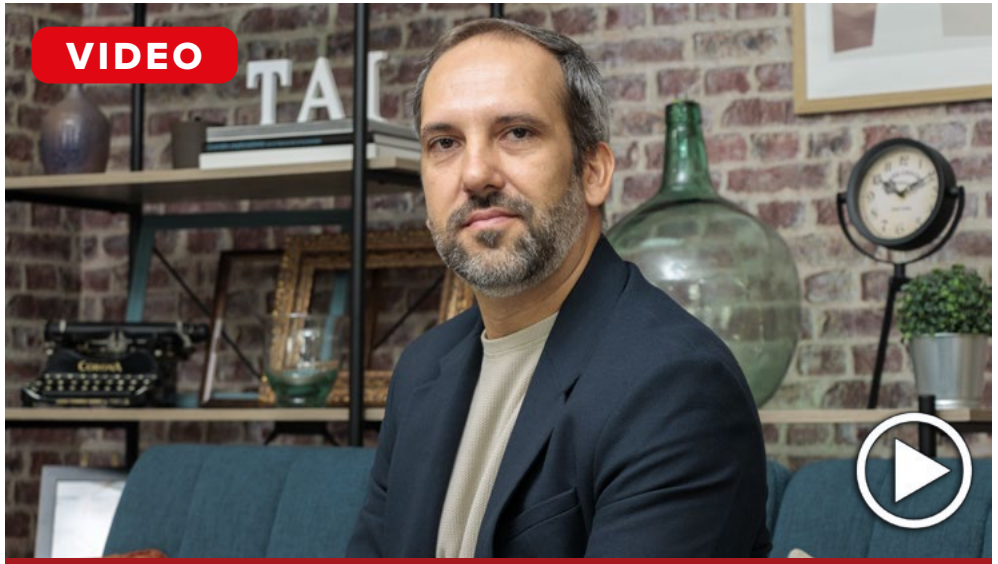
] pexip [

Sophos: “Ante un ciberataque no puedes improvisar: necesitas experiencia y capacidad de respuesta inmediata”

La ciberseguridad afronta el reto de mejorar la detección y respuesta sin aumentar la complejidad. Iván Mateos, Sales Engineer de Sophos Iberia, advierte de que muchas empresas operan con un “Frankenstein de seguridad”, con múltiples herramientas desconectadas que generan más trabajo que valor. Frente a ello, defiende un modelo de plataforma que integre tecnología, inteligencia y servicios gestionados.

Los servicios MDR permiten a las organizaciones responder con rapidez apoyándose en equipos expertos: “ante un ciberataque no puedes improvisar”. La inteligencia artificial está ayudando a agilizar la detección y el análisis, aunque siempre bajo supervisión humana.

De cara al futuro, el foco estará en el control del dato. “Hay que poner gobernanza sobre la información”, señala, para evitar fugas en entornos cada vez más abiertos y automatizados.



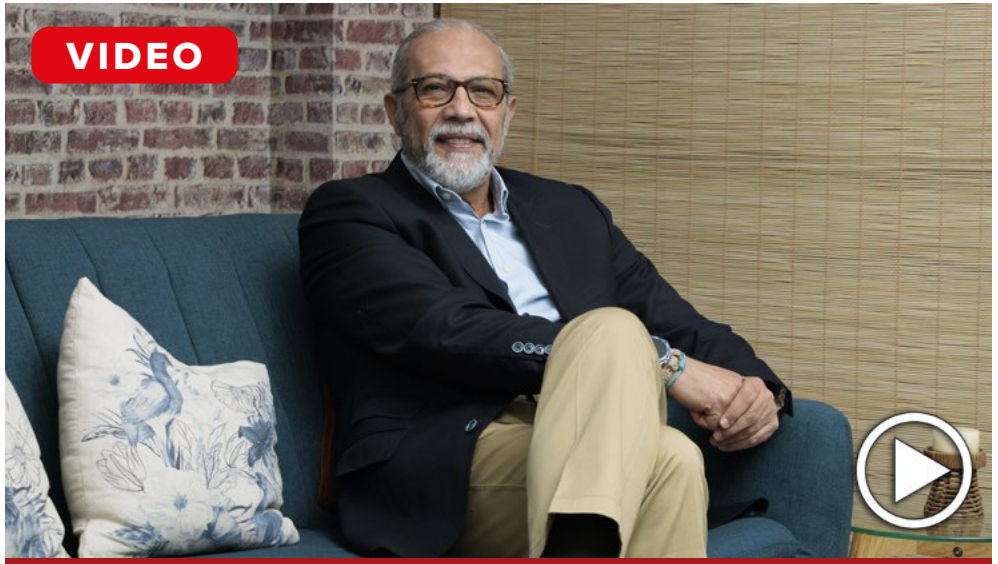
Iván Mateos, Sales Engineer, **Sophos Iberia**

SOPHOS

“UDS Enterprise nace y se desarrolla escuchando a los clientes”

La virtualización es una de las soluciones para mejorar la gestión del puesto de trabajo que tiene que ajustarse a las necesidades de las compañías en un escenario en el que hay que tener en cuenta numerosos factores como la normativa, la ciberseguridad o la inteligencia artificial. Fernando Feliu, *executive managing director* de Virtual Cable, aconseja a los CIO estudiar “cuáles son las necesidades reales que cada compañía tiene”.

Tras este primer paso se podrá elegir la solución a implantar, destacando aquellas que forman parte de un ecosistema como UDS Enterprise, la solución que permite virtualizar el puesto de trabajo, cumpliendo con el esquema nacional de seguridad y garantizando la soberanía digital. Feliu recalca que USD Enterprise “nace y se desarrolla escuchando a los clientes finales, a los *resellers*, escuchando cuáles son las necesidades que se están planteando y las situaciones geopolíticas que se están creando actualmente y en el futuro”.



Fernando Feliu, *executive managing director* de **Virtual Cable**

VIRTUAL CABLE