Foro TAI Galicia

Retos tecnológicos para el futuro de la empresa gallega

ENTIDADES COLABORADORAS

Colexio Oficial Enxeñeiros de Telecomunicación Galicia

Asociación de Enxeñeiros de Telecomunicación de Galicia

Allied Telesis · Commvault · kaspersky · NTT DATA · SOPHOS · tp-link · VARONIS

TAI · ciberseguridadTIC · directorTIC

IR A PÁGINA SIGUIENTE

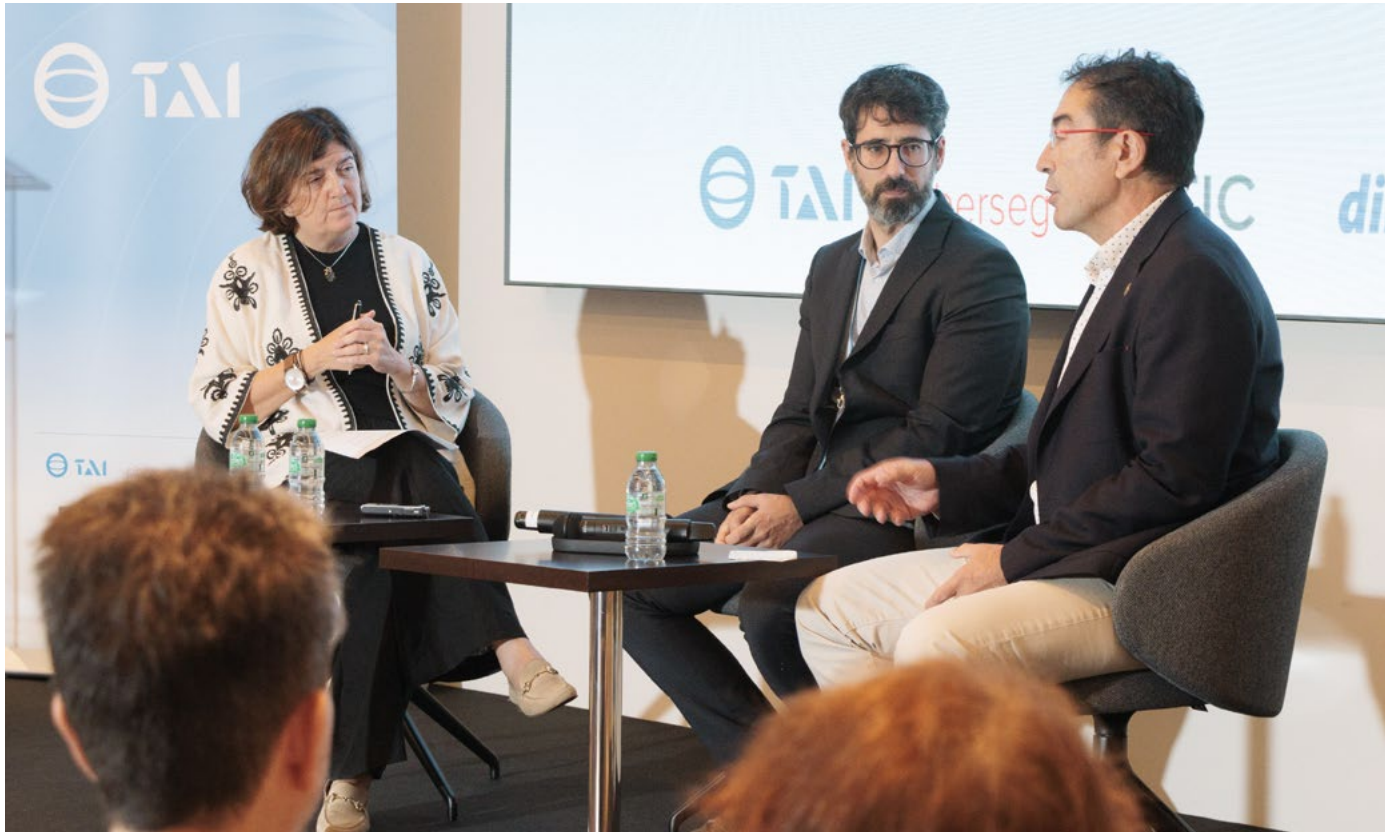
Galicia: el reto de la "*calidade*" tecnológica

Foro TAI Galicia

Con la colaboración del Colexio Oficial de Enxeñeiros de Telecomunicación (COIT) y la Asociacion de Enxeñeiros de Telecomunicación de Galicia, el Grupo TAI, a través de sus publicaciones DirectorTIC y CiberseguridadTIC, ha organizado el "Foro TAI Galicia: retos tecnológicos para el futuro empresarial", en el Club Cámara Noroeste, en La Coruña. Un evento en el que contó con el patrocinio de Allied Telesis, Commvault, Kaspersky, Mastercard, NTT DATA Inc, Sophos, TP-Link y Varonis; y en el que participaron representantes de sectores como la banca, los medios de comunicación, la industria, la Administración pública o la educación, para debatir sobre los desafíos, las oportunidades y las prioridades estratégicas en materias como la digitalización, la internacionalización y la innovación tecnológica en la comunidad gallega.

Marilés de Pedro

Desde hace muchos años Galicia trabaja por exhibir su etiqueta de "*Calidade*". Y no solo por el valor que tiene su patrimonio cultural y artístico, su riqueza gastronómica y su belleza paisajística; la comunidad trabaja por elevar la calidad de su ecosistema económico y acelerar su desarrollo tecnológico.

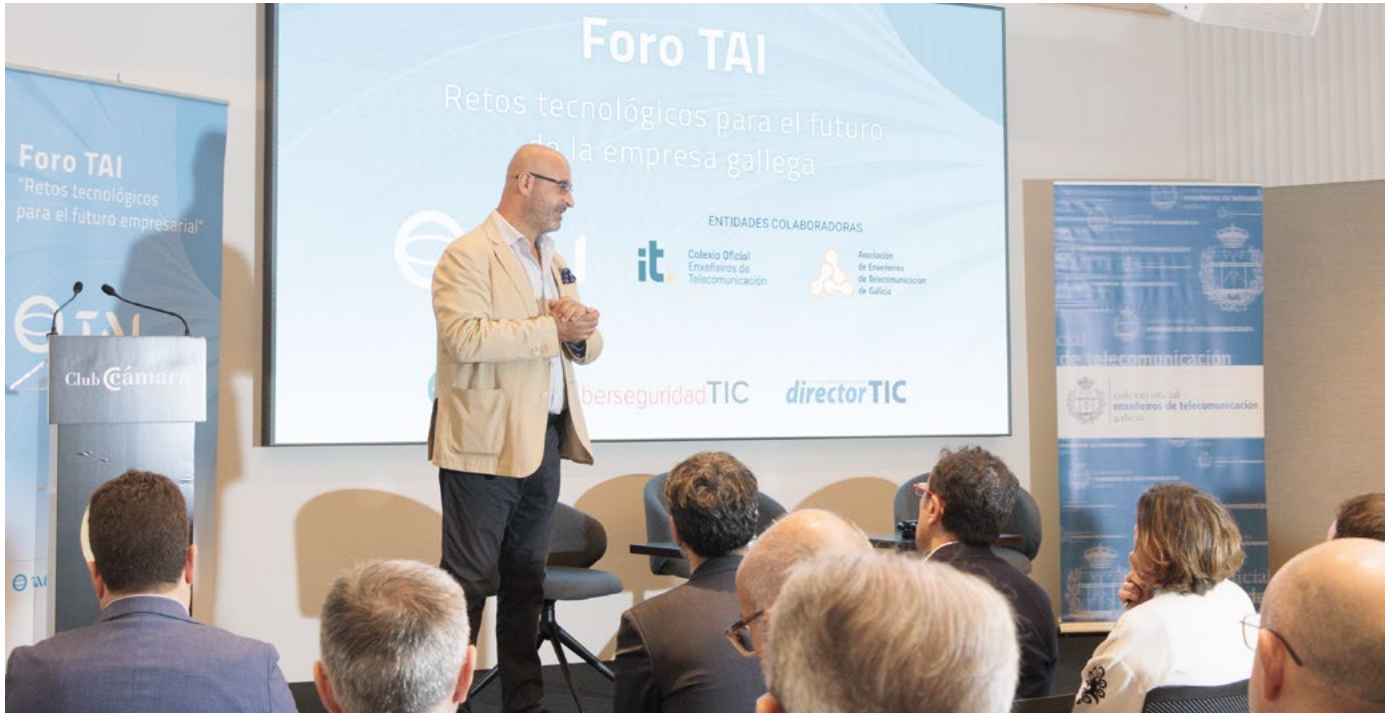


En el último cuatrimestre del pasado año la economía gallega tuvo un crecimiento del PIB del 3,7 %; un baremo por encima de la media nacional. En términos de internacionalización, las exportaciones gallegas también experimentaron un crecimiento mucho mayor que el registrado a nivel nacional (3,3 % frente al 0,2 %) según el Instituto Galego de Estadística.

En la inauguración de la jornada, Julio Sánchez

Foro TAI Galicia

> “Para acelerar la transformación digital de las empresas gallegas, la inversión en formar y retener el talento es esencial”



Agrelo, decano del COIT en Galicia, pintó la realidad empresarial gallega, marcada por la atomización de su población: 30.454 núcleos de población en menos de 30.000 kilómetros cuadrados, en los que se ubican 230.000 empresas, de las cuales más del 95 % son pymes y micropymes. Una realidad, insistió, que afecta a la economía y a la digitalización, y que tiene su reflejo en el sector TIC ya que alrededor de 3.000 empresas tienen la ingente misión de “ayudar a la transformación tecnológica de ese enorme ecosistema empresarial”. Sin embargo, para el decano, se dispone de la infraestructura y la tecnología “suficientes para romper la brecha que existe”.

A su juicio, para acelerar la transformación digital de las empresas gallegas, la inversión en formar y retener el talento es esencial. Para ello, y entre otros núcleos formativos, Galicia cuenta con la Escuela Técnica Superior de Ingeniería de Telecomunicación, en Vigo; o las de Ingeniería Informática en La Coruña, Santiago y Orense. La inversión en torno a la ciberseguridad y la concienciación acerca de la confianza en el uso de las tecnologías son otras áreas claves. “Cuanto más crece la digitalización, más vulnerable es la empresa”, alerta. “Por tanto, invertir en soluciones para diseñar una adecuada protección se hace indispensable”. También se refirió a la innovación aplicada. “Todas las tecnologías, como es el caso de la inteligencia artificial, la nube, las soluciones vinculadas con la gestión y la protección del dato o la ciberseguridad son esenciales, pero hay que conseguir que no solamente estén presentes en las grandes empresas; hay que ser capaces de trasladarlas a las pymes y micropymes”.

Foro TAI Galicia

Uno de los grandes valores tecnológicos que se encuentran en Galicia es el Centro de Supercomputación de Galicia (CESGA), fundado en 1993, ubicado en Santiago, y que cuenta, entre otras joyas tecnológicas, con el superordenador Finisterrae. Un centro que busca transferir innovación al tejido empresarial, facilitando el acceso a tecnologías innovadoras, mejorando la competitividad y la productividad del tejido empresarial gallego. Lois Orosa, director del CESGA, que participó en la inauguración del foro, aseguró que, por el auge en torno a la IA, la supercomputación y el análisis de los datos, en constante crecimiento, centros como el CESGA son cada vez son más estratégicos para el desarrollo de las regiones, de los países y de los continentes. “Tanto la Xunta de Galicia como el Estado español, y también Europa, están invirtiendo en áreas claves vinculadas con la supercomputación y la inteligencia artificial”.

Orosa puso en valor las importantes labores que desarrollan desde el centro, entre ellas, ayudar a las empresas a incrementar su productividad y competitividad. “Como centro de investigación, nuestra contribución a la empresa es, siempre o casi siempre, en la fase de preproducción de las soluciones y los productos, vinculada, por tanto, con la innovación y la investigación”, especificó. Una labor que cuenta con diversos casos de éxito. Es el caso de la colaboración, que ya supera los siete años, con la empresa maderera Finsa, vinculada con la aplicación de la inteligencia artificial para optimizar sus procesos de producción. Una alianza que permite al CESGA la financiación de profesionales que investigan alrededor de esta tecnología.

El centro apoya a numerosas pymes, siempre en la fase de preproducción, en el entrenamiento de modelos alrededor de la inteligencia artificial gracias al concurso de la computación. “Hay muchas empresas que no cuentan con la capacidad de cómputo suficiente para entrenar sus modelos”, explica. También establecen colaboraciones para ayudar a las empresas, “con expertos, a ejecutar una idea que han diseñado”.

Por último, el centro absorbe a jóvenes titulados, que participan en los diferentes proyectos

> “Tanto la Xunta de Galicia como el Estado español, y también desde Europa, se está invirtiendo en supercomputación e inteligencia artificial”

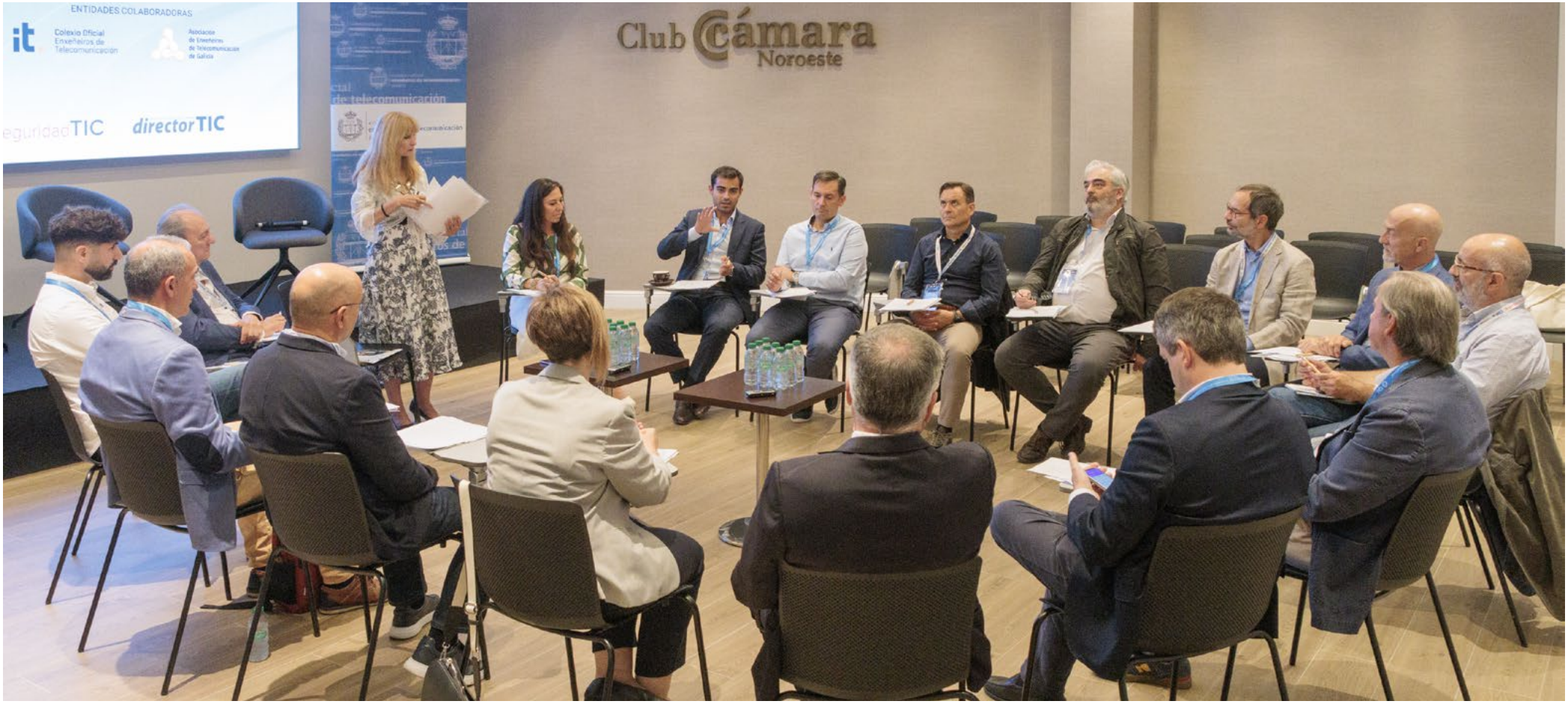
tecnológicos europeos, y que posteriormente se unen al mundo empresarial. “El talento es el área más importante y nuestro mayor reto en los próximos años”.

Las capacidades en supercomputación empiezan en 2007 con la creación del Finisterrae, un superordenador que va a alcanzar el próximo año la cuarta versión, Finisterrae IV, orientado a la IA, que multiplicará por siete la capacidad de cálculo actual del CESGA. Una máquina que se ubicará en la nueva sede del Centro, actualmente en construcción, que estará operativa el año que viene en Santiago y que cuenta con una inversión de 56 millones de euros. Orosa explicó que, para el diseño del supercomputador, se consultó con el ecosistema, diverso, del CESGA, en el que están incluidos las universidades o el Consejo Superior de Investigaciones Científicas (CSIC), para analizar cuáles eran los grandes proyectos estratégicos que se iban a desarrollar y que el supercomputador estuviera en línea con ellos. “El denominador común era, prácticamente en todos los casos, la inteligencia artificial”.

Uno de los objetivos es dotar al centro de una proyección europea y lograr ubicar un supercomputador europeo. “Aspiramos a contar con infraestructura europea y no solo dar servicio a pymes y empresas gallegas y españolas; también europeas”. Junto a ello, otro objetivo es ampliar su oferta de servicios.

Además de estas infraestructuras de computación cuántica, el centro cuenta con un ordenador de 45 Qbits considerado el más potente del sur de Europa; una máquina con un componente “mucho más experimental y que requiere una etapa de investigación; por tanto, solo las empresas más atrevidas ingresarán en este mundo”, especificó.

El dulce momento tecnológico que viven las empresas gallegas contrasta con su preocupación sobre su futuro ante la escasez de talento



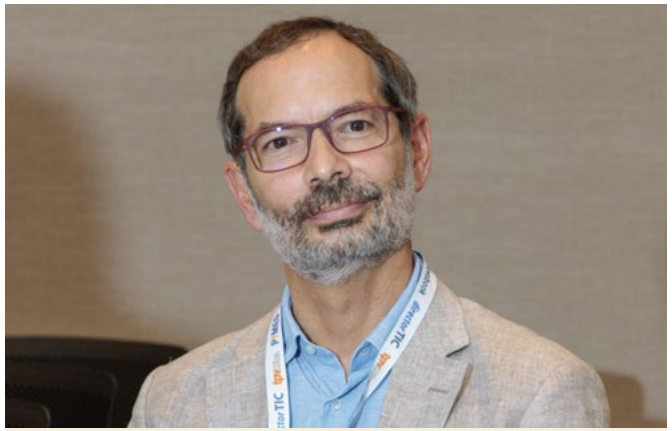
Foro TAI Galicia

El sector tecnológico gallego se posiciona entre los más dinámicos de España. DirectorTIC, junto a Allied Telesis, NTT DATA Inc y TP-Link, ha querido pulsar, de la mano de directivos de empresas como Aluman, Autoridad Portuaria de La Coruña, B100/ABANCA, Estrella Galicia, Cabeiroa, Grupo Plásticos Ferros, La Voz de Galicia, Universidade de Santiago de Compostela o Russula SAU, por poner algunos ejemplos, la realidad tecnológica de la comunidad.

Inma Elizalde

Galicia cuenta con 3.140 empresas TIC, casi el 5 % del total nacional, superando los 23.000 empleados. Y, según datos de la Xunta, la inteligencia artificial está implantada en más del 38,3 % de las empresas, desarrollando un 38 % de las empresas tecnológicas actividades de I+D+i en los últimos tres años. Por su parte, el Clúster TIC Galicia ha crecido un 40 % en su número de asociados en los últimos tres años, agrupando a 148 organizaciones. Por ciudades, Vigo, La Coruña y Santiago actúan como motores, concentrando más de la mitad de las empresas. En cuanto a los sectores que lideran esta escalada figuran el biotecnológico, el del software, el *foodtech, ehealth* y *agrotech* Pero ¿cómo ven y viven las empresas tecnológicas gallegas el momento actual?

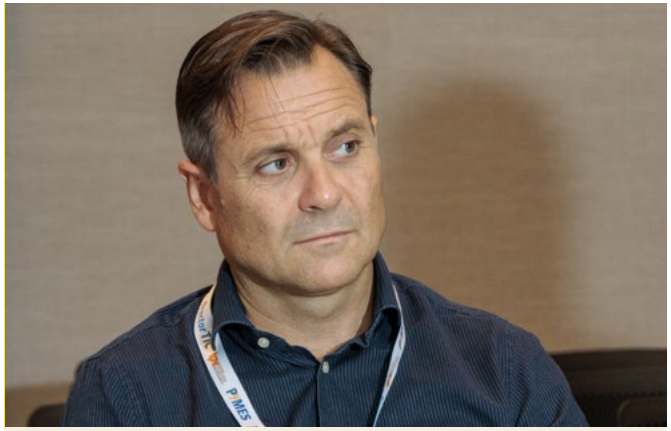
José Antonio Fernández, CIO de Grupo Plásticos Ferros, considera que el ecosistema tecnológico gallego vive un dulce momento, contando con proveedores importantes a nivel mundial tanto en productos como en servicios. Manuel Diaz, *head of technology* de B100/ABANCA, resalta que, aunque el sistema tecnológico es bueno, habría que avanzar a la hora de comprender la tecnología, cultivando el conocimiento, la cultura y creación del ecosistema digital. “El ecosistema local es óptimo, pero hay que poner más cuidado en la modernización del ecosistema de la propia empresa porque hay compañías que tienen tecnología que no han cambiado en años. Ese es un problema típico de nuestra comunidad”, se queja. A lo que José Manuel Velo, director del área TIC de Universidade de Santiago de Compostela, responde que en la universidad cuentan con centralitas instaladas en 1994 que siguen funcionando. “Si ahora migramos a cualquier tecnología moderna va a durar unos cinco años, por lo que no es fácil convencer a los gerentes de que si antes



> “El ecosistema tecnológico gallego vive un dulce momento, contando con proveedores importantes a nivel mundial”
>
> **José Antonio Fernández,**
> CIO de Grupo **Plásticos Ferros**

una tecnología sobrevivía tres décadas ahora dura un lustro. O a los usuarios de que hay que gestionar el cambio", reivindica.

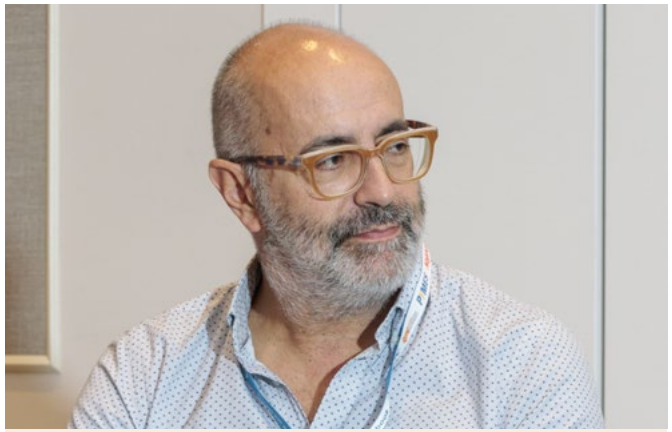
Miguel Silva, director de sistemas de La Voz de Galicia, se muestra escéptico en términos



"El ecosistema local es óptimo, pero hay que poner más cuidado en la modernización del ecosistema de la propia empresa"

Manuel Diaz,
head of technology de **B100/ABANCA**

tecnológicos con una IA de la que dice que muy pocas empresas tienen idea de en qué van a aplicarla. "Se habla mucho de ChatGPT, de Copilot, de los procesos administrativos en los que en lugar de utilizar la palabra digitalización deberíamos usar transformación", dice. "Hay que cambiar la manera de trabajar para poder aplicar la IA o generar recursos". Como ejemplo pone el sector periodístico en el que el número de lectores en papel que compran un periódico es cada día más bajo, por lo que tienen que buscar esa transformación porque lo digital no suple el *business plan* de una gran empresa. "Todo ello sin olvidar la regulación europea que obliga a las editoriales a dar contenido incluso a las personas que no quieren pagar por la publicidad". José Manuel Velo, director del área TIC de Universidade de Santiago de Compostela, coincide en su escepticismo hacia la inteligencia artificial en un momento en el que los CISO tienen que explicar a sus superiores cómo utilizarla. Desde su punto de vista hay muchas carencias y desconocimiento en torno a conceptos básicos de informática y los riesgos asociados a la misma.



"Me preocupa si la comunidad gallega tendrá la capacidad de contar con suficientes RR.HH. en cinco años para dar respuesta a las necesidades tecnológicas"

José Manuel Velo, , director del área TIC de
Universidad de Santiago de Compostela

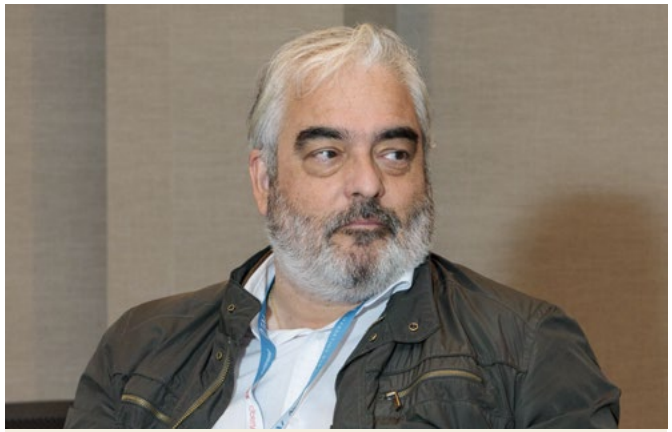
Manuel Doval, consultor de gestión TIC, organización y gestión de clientes, recuerda que la inteligencia artificial no va a resolver problemas. "Saber cómo preguntar a la misma es esencial

para que nos responda correctamente. Esto nos falta". También escasea, en su opinión, el valor que tienen que dar las empresas al papel de TI, "que sigue siendo a veces bastante complicado", apunta.

Por su parte Carlos Figueiras, interin CIO, señala la descoordinación a la hora de adquirir tecnología en un entorno en el qué predominan las pequeñas empresas que no cuentan con un director de TI que sepa que se necesita en materia tecnológica. "Adquieren productos y servicios más por impulso que por necesidad", comenta.

cambiar por José Ramón González, *industrial IT director* de Russula señala como problemático encontrar información sobre soluciones. "En Internet sólo se ofrecen presentaciones llamativas, descripciones muy generales y contenido que no detalla qué hacen y cómo funcionan los productos ofrecidos", argumenta.

En cuanto a la segmentación empresarial, José Antonio Fernández reconoce que las pequeñas y grandes empresas juegan en ligas distintas, por lo que cada una tiene que adaptarse a sus recursos, aunque, en su opinión, tener referentes en



"A la nube le falta un punto para decir que en el pago por uso puedo ajustarme y transformar también mis procesos para disminuir los costes"

Miguel Silva,
director de sistemas de **La Voz de Galicia**

los que reflejarse es conveniente, comprobando qué tecnología aplican y cómo funciona.

En el ámbito más humano, José Manuel Velo alude a la falta de relevo generacional como un problema con jóvenes que no quieren adaptarse si no hay tecnología de última generación en las organizaciones.

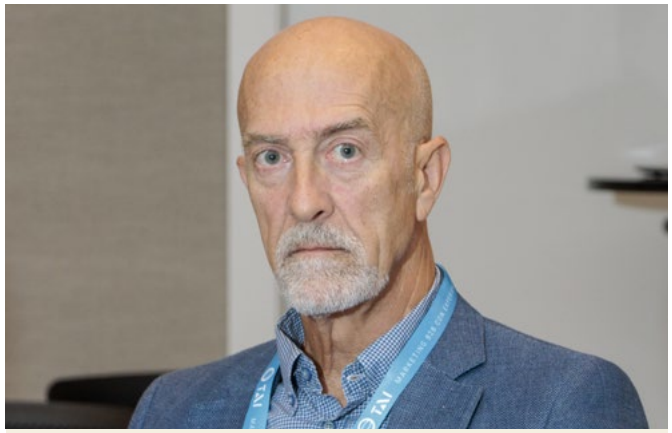
En el apartado de la internacionalización Manuel Doval reconoce que no es lo mismo vender un producto en el exterior que internacionalizar, por lo que ante la primera opción sería más estratégico contar con un óptimo *marketplace* que montar una infraestructura.

Rocío Vázquez, directora TIC de Aluman, avanza que como compañía necesitan, tanto en la parte de internacionalización como en la local, tecnología robusta y escalable que asegure la trazabilidad al final de la cadena de producción. Todo ello junto a ciberseguridad, "porque todo tiene que ser seguro". En cuanto a la tecnología que Aluman utiliza, pone ejemplos como el ERP, aplicable a las normativas de todos los países, BI para tomar decisiones a partir de los datos...

José Luis Suárez, jefe de Transformación Digital de la Autoridad Portuaria de La Coruña, confirma que su organización tiene problemas muy parecidos a los comentados, a pesar de pertenecer a la Administración: recursos escasos, falta de talento, dificultad a la hora de que lleguen los mensajes sobre la importancia de la tecnología...

La voz de los expertos

Javier Sánchez de la Poza, GTM Practice Solutions Specialist de NTT DATA Inc, advierte que para que la IA sea una herramienta de transformación y pueda solucionar problemas tiene que estar alineada con un proceso de consultoría que comience desde la estrategia de verificación, *milestones*, tener claras las expectativas... En definitiva, "planificar con tecnología todo lo que se pretende, de principio a fin, porque la IA es una herramienta que hay que usar para resolver situaciones problemáticas".



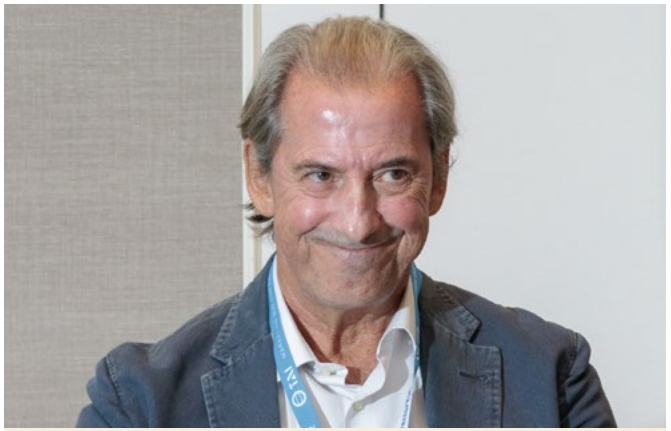
"La IA no va a resolver problemas y saber cómo preguntarle es esencial para que nos responda correctamente"

Manuel Doval,
consultor de gestión TIC, organización y gestión de clientes

Beatriz Pérez, *key client manager* de NTT Data, por su parte, alude a la necesidad de, además de disponer de tecnología, de contar con buenos proveedores que ayuden a llegar a la misma porque "no toda la tecnología vale para todo ni para todos los sectores ni para todas las compañías". Por lo tanto, aconseja analizar qué tecnología es buena para nosotros y si es válida, hasta qué punto.

Siguiendo la estela de Beatriz Pérez, Luis González, director de Allied Telesis, anima a las empresas a tomar las decisiones correctas a la hora de comprar la tecnología que necesitan, en función de los presupuestos de los que disponen en ese momento. "Deben averiguar qué necesitan de los proveedores y fabricantes. Nosotros vamos a apoyarles para que no tomen decisiones precipitadas. Pueden ir eligiendo lo que más les guste de cada proveedor", enfatiza.

Óscar León, B2B *business development manager* de TP-Link, agrega que "tecnologías estratégicas pueden ser aquellas que garanticen continuidad y eficiencia como la IA, la nube o la red, el peso sobre la que se apoya el resto", porque, tal y como reconoce, "sin ella no tendríamos nada". En cuanto a la internacionaliza-



"Las pymes adquieren productos y servicios más por impulso que por necesidad"

Carlos Figueiras,
interin CIO

ción destaca la relevancia de plataformas que pueden permitir escalar de manera más sencilla. En cuanto a Iago Cotelo, responsable del departamento técnico de EMTEL del Nororeste, comenta que el problema de los proveedores es tratar con la persona que ha asumido el departamento de informática, que en muchas ocasiones cumplen ese cometido porque es a quien mejor se le da dentro de la compañía, sin tener la preparación suficiente para ello. En los casos en los que la compañía tiene un total desconocimiento, delega en un operador para que le lleve todos los servicios, pero, en su opinión, "mucha de la atención que pueden dar los operadores es prácticamente nula". Aunque también señala que muchas veces quien firma la solución no es quien la despliega. "Y por ahí también vienen los problemas", certifica.

El entorno de la red

La importancia de la red en las organizaciones es una realidad en un mundo tecnológico que avanza a gran velocidad. Con los nuevos tiempos, y las nuevas maneras de trabajar, la conectividad *wifi* confiable y segura se ha convertido

"Tengo la suerte de que la CEO de la empresa cree en la tecnología y nos apoya"

José Ramón González,
industrial IT director de **Russula**

en un valor añadido para los trabajadores que han hecho de cualquier espacio, y en cualquier lugar, su oficina. Si hasta hace unos días hablábamos de *wifi* 6, ya son varias las organizaciones, como TP-Link o Allied Telesis, que han presentado soluciones para *wifi* 7, mientras el mercado ya habla de *wifi* 8... NTT DATA Inc, además, acompaña a las compañías a la hora de mostrar cómo se utiliza esa red. "Tenemos proyectos donde, a través de la automatización y con proyectos propios, conseguimos optimizar esa red", explica Beatriz Pérez.

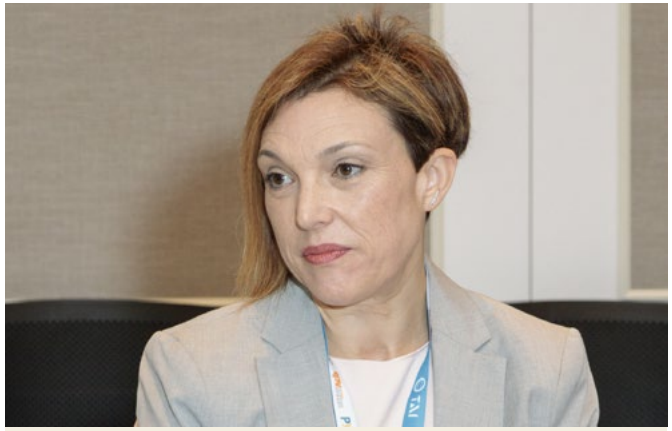
Óscar León señala que en este momento hay una coexistencia entre el *wifi* 6 y el 7. "Por un lado se adoptan proyectos que soportan perfectamente tecnología *wifi* 6, sin embargo, hay sectores que optan más por *wifi* 7 por adaptarse a entornos de futuro. Más usuarios conectados, con mayores velocidades y menores latencias en situaciones críticas como, por ejemplo, en el sector sanitario", explica.

En este sentido José Manuel Velo apunta a que un claro síntoma que tienen los usuarios de que la *wifi* va mal es cómo están diseñados los edificios y las zonas de alta densidad, por lo que considera importante llevar a cabo una buena planificación de los puntos de acceso.

Aluman ha realizado un plan de cambio relacionado con la *wifi* porque querían modernizar su infraestructura, confiesa Rocío Vázquez. "Cambiamos todos los dispositivos e hicimos un estudio de cobertura. Las soluciones que ahora

tenemos desplegadas son acordes a nuestras necesidades actuales. Todo ello con la seguridad correspondiente".

Para facilitar las cosas Luis González avanza que Allied Telesis permite a una empresa que quiere cambiar de *wifi,* y tiene que renovar toda su infraestructura al mismo tiempo, contar con un controlador universal para que vaya cambiando automáticamente a otra nueva tecnología sin cambiar toda la tecnología, actualizando sólo el software. Y esto también conlleva un ahorro, confirma.



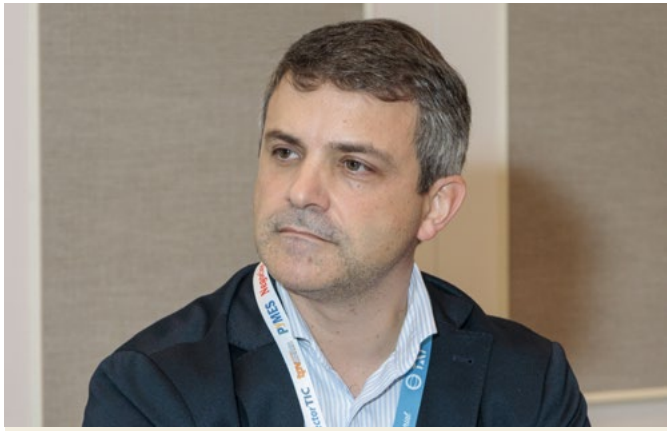
"Necesitamos que la tecnología que utilizamos sea robusta y escalable para asegurar la trazabilidad al final de la cadena de producción"

Rocío Vázquez, directora TIC de **Aluman**

En el ámbito de la nube las experiencias son muy diferentes

En cuanto a las ventajas que se observan en la adopción de soluciones SD-WAN frente a los modelos tradicionales para garantizar la continuidad y flexibilidad en las organizaciones, Óscar León expone que la tecnología SD-WAN ha supuesto un salto significativo frente a soluciones tradicionales. "Se trata de una arquitectura de software que conecta a usuarios y aplicaciones en la nube o aplicaciones críticas. Tienen muchos puntos a favor, gestión centralizada, visibilidad de un único panel", dice.

Iván Casto, CTO global Informatica de Hijos de Rivera, Estrella Galicia, Cabeiroa, manifiesta que, al trabajar los empleados desde cualquier parte de la geografía, necesitan satisfacer esa conectividad y ciberseguridad en las conexiones, por lo que tienen un proyecto de plataforma SASE que garantice ambas.



"Hemos sido y seguimos siendo muy CAPEX, aunque vamos subiendo cosas a la nube privada y algunas a la pública"

José Luis Suárez, jefe de Transformación Digital de **Autoridad Portuaria de La Coruña**

Para Carlos Figueiras es fundamental tener plataformas colaborativas con seguridad detrás de las mismas.

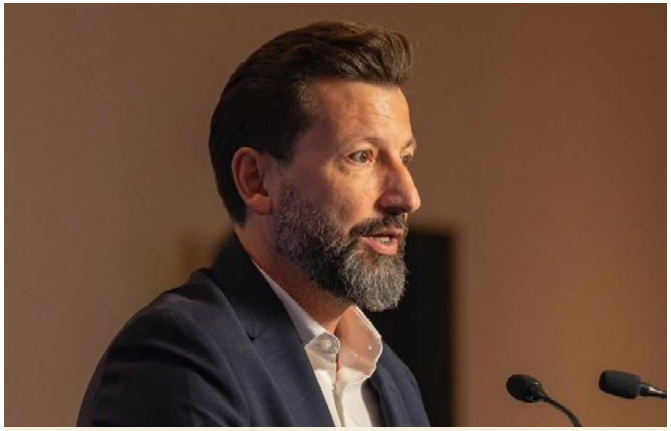
El universo nube

En cuanto a la nube, las experiencias son muy diferentes. En el caso de un periódico, Miguel Silva expone que tienen en la misma casi todos sus planes, pero también necesitan recursos de red local. Aún así destaca ventajas como el cambio de Capex a Opex "pero me falta un puntito más para decir que en el pago por uso puedo ajustarme y transformar también mis procesos para disminuir los costes porque, sino la nube, en principio, es más cara que la infraestructura *onprem*", reivindica.

Desde la banca digital Manuel Díaz confirma trabajar en la nube pública y estar encantado en la misma por su alto nivel de observabilidad, de velocidad de despliegue, de integración con terceros... Todo ello unido a la gran seguridad que aporta, y por un precio muy razonable, en su opinión.

La experiencia de José Ramón González en el sector industrial pasa por la necesidad de mantener el software de desarrollo de ingeniería en local, mientras que los procesos más ofimáticos los están moviendo progresivamente a la nube de Microsoft.

Desde el puerto, al tener un componente de Administración se complican un poco las cosas en este sentido, admite José Luis Suárez. "Hemos sido y seguimos siendo muy Capex, aunque vamos subiendo a la nube privada y algunas a la pública".



"Somos una región en la que se vive bien y contamos con empresas que pueden desarrollar talento para que los trabajadores se queden"

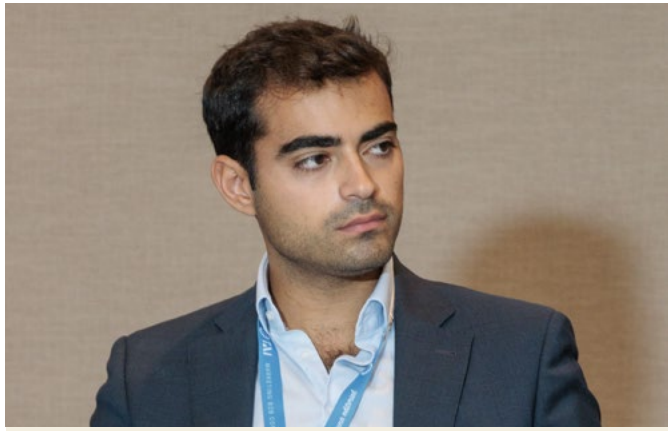
Iván Casto, CTO global Informatica de **Hijos de Rivera, Estrella Galicia, Cabeiroao**

En cuanto al sector universitario, José Manuel Velo reconoce que en 2016 decidieron migrar su estructura de correo electrónico a Microsoft 365. Desde 2018 optan por contratar todo lo que pueden como servicio. Todo lo relacionado con los servicios que prestan a los alumnos lo tienen en Azure, aunque admite contar con muchas partes *on-premise*, como todo lo relacionado con la gestión académica, por ejemplo, al tiempo que lanza una queja: la poca predicibilidad de los costes.

En el lado del proveedor, Javier Sánchez de la Poza considera lógico utilizar determinadas herramientas en la nube por la velocidad de implementación, escalabilidad, uso... Mientras otras es fundamental mantenerlas en *on-premis* por el coste y la protección de los datos. "Si yo fuera el CEO de una empresa, seguramente apostaría casi siempre por arquitecturas híbridas. Las más delicadas las dejaría en *on-premise*", explica.

Difícil elección

¿Y si sólo pudieran invertir en dos tecnologías, cuáles elegirían? Hay dos claramente ganadoras: la ciberseguridad y la inteligencia artificial. Iván Castro rompe el fuego al elegirlas, entendiendo por IA todo lo que hay por debajo: gestión del dato, gestión de la nube... apostilla. Una IA fundamental para Abanca. “Nosotros siempre vamos a invertir en colocar funcionalidades diferenciales y disruptivas para el cliente final”, admite Manuel Díaz.



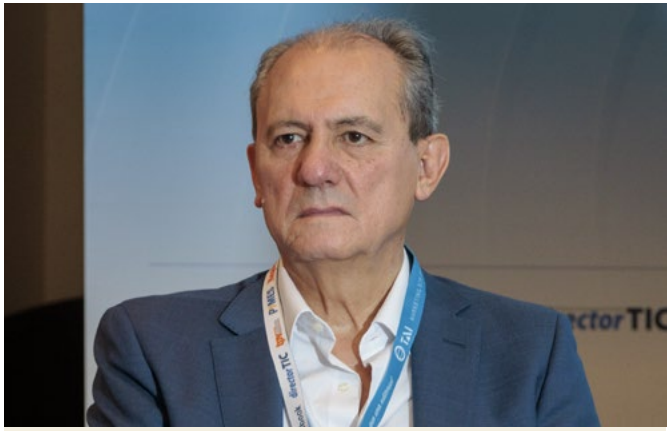
“Para que la IA sea una herramienta de transformación y pueda solucionar problemas, hay que planificar todo lo que se pretende”

Javier Sánchez de la Poza,
GTM practice solutions specialist de **NTT DATA Inc**

Carlos Figueiras suma a la ciberseguridad la automatización, al igual que Manuel Doval quien añade que hay que invertir en nuevas aplicaciones enfocadas al cliente. A este grupo también se une José Antonio Fernández. “Yo sigo pensando que viene un gran potencial a nivel muy básico de diferentes puestos de simplificación de documentación, despliegue de contratos...”, reflexiona. Una automatización e integración de todos los sistemas que, según Rocío Vázquez, es fundamental en Aluman, donde el trabajo de un departamento debe ser el punto de partida del siguiente. “Ahí es donde hay que mejorar y donde entra en juego mucha parte de automatización”, subraya.

José Ramón González reconoce estar embarcados en ciberseguridad al tiempo que tienen que ahondar en la parte de servicios para los diferentes departamentos porque “cada departamento es una isla. Hay que intentar integrar y coordinar todo”.

En el caso de José Manuel Velo optaría por la infraestructura, con la ciberseguridad en la que incluye al *endpoint*. Mientras Miguel Silva elegi-



“Las empresas tienen que detectar qué es lo que necesitan de los proveedores porque estamos aquí para apoyarlas”

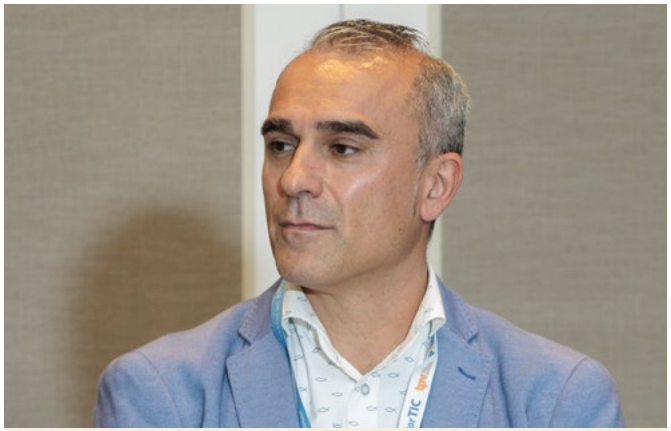
Luis González,
director de **Allied Telesis**

> La ciberseguridad y la inteligencia artificial, las dos tecnologías en las que las empresas invertirían

ría invertir en personal en un momento en el que pone el acento en la tendencia a reducir los equipos de IT cuando, en su opinión, esto es un error. Óscar León recuerda que nada sería posible sin la red, “el sistema nervioso de las organizaciones”. Luis González refuerza este mensaje apuntando que donde más dinero se pierde es cuando la línea de producción se cae. Para ello cuentan con soluciones seguras con aplicaciones ciber por encima.

Cambios deseados

¿Qué cambios esperan ver en el panorama tecnológico gallego en los próximos cinco años? José Ramón González reconoce que tiene dudas sobre cómo será la estructura laboral de las compañías con los cambios que llegan. Al igual



> “Tecnologías estratégicas pueden ser aquellas que garanticen continuidad y eficiencia como la IA, la nube o la red”
>
> **Óscar León,**
> B2B business development manager de **TP-Link**

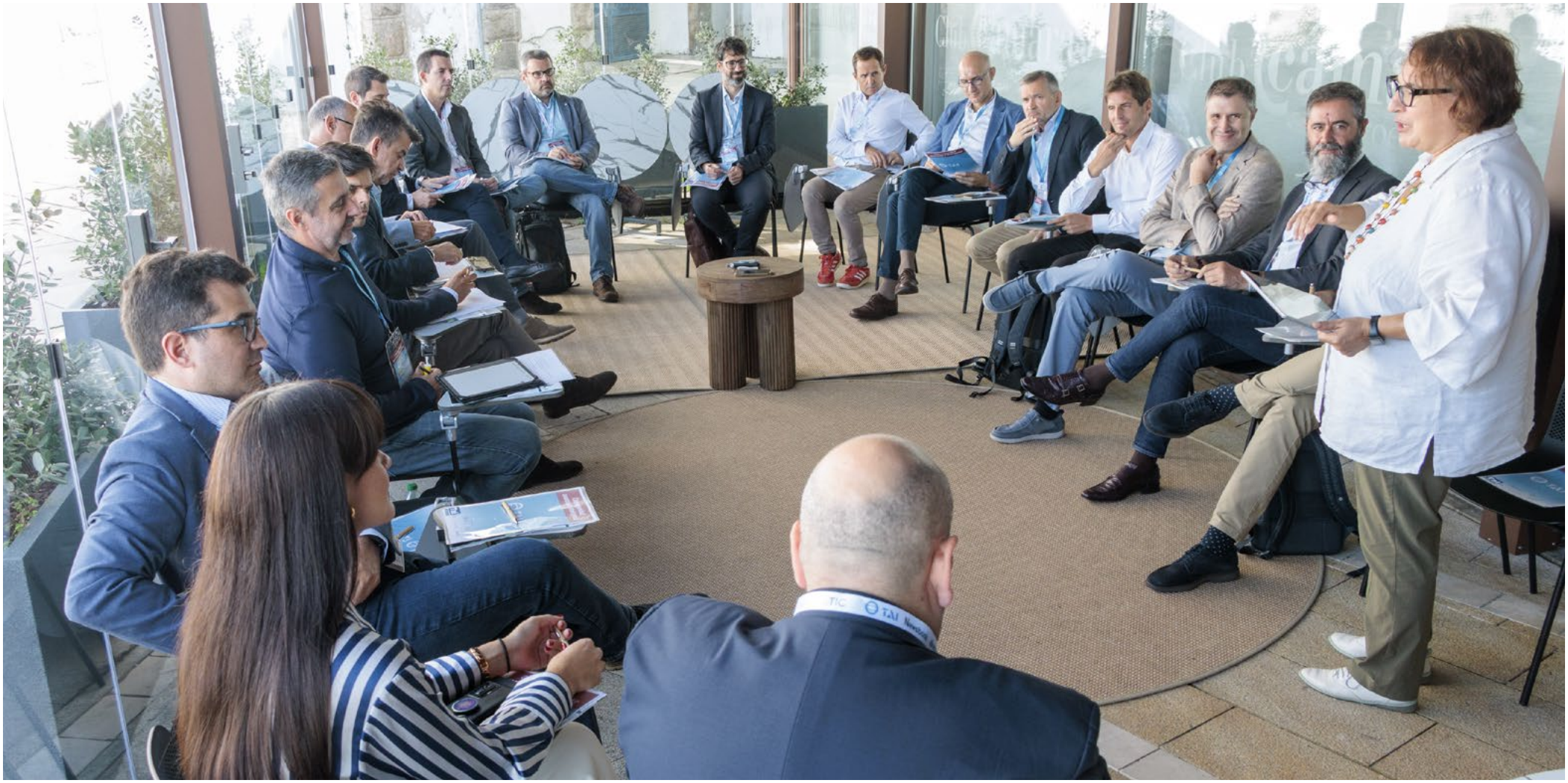
que Miguel Silva, aunque señala en una dirección: la computación donde espera que Galicia sea puntera.

Mientras José Manuel Velo se muestra muy escéptico sobre posibles cambios tecnológicos sí reconoce que le preocupa si la comunidad gallega tendrá la capacidad de contar con suficientes recursos humanos para dar respuesta a las necesidades tecnológicas. “Hay que invertir para que las personas quieran trabajar aquí”, demanda. Inquietud con la que coincide de José Luis Suárez. “Ojalá que en cinco años haya talento suficiente en número y capacitación que viva y se desarrolle aquí”, desea. E Iván Castro: “Somos una región en la que se vive bien y contamos con empresas que pueden desarrollar ese talento para que los trabajadores se queden”. A lo que Manuel Doval responde que hay que hacer que se vea la tecnología como un valor estratégico “ya que esto permitirá mayores inversiones y el talento querrá quedarse”.

Rocío Vázquez pediría una mayor igualdad en la infraestructura entre empresas de todos los tamaños y una óptima disponibilidad de red. Algo en lo que la secunda José Antonio Fernández, mientras Carlos Figueiras apuesta por la tendencia del todo como servicio.

Manuel Díaz suscribe todo lo comentado, incidiendo en que espera que el empresario gallego quiera tener la mejor tecnología, la comprenda y la aplique lo mejor posible.

La resiliencia digital en Galicia pasa por identidad, IA y regulación



Foro TAI Galicia

Celebrado a finales de septiembre, el Foro TAI Galicia se convirtió en un punto de encuentro clave para analizar cómo las organizaciones gallegas afrontan los nuevos desafíos de la ciberseguridad. En una comunidad con un tejido empresarial dominado por pymes y sectores estratégicos como la energía, la agroalimentación o los medios de comunicación, la protección digital no es sólo una cuestión tecnológica, sino un factor de competitividad y resiliencia. El debate giró en torno a cuestiones que marcan la agenda en toda Europa —de la implantación de NIS2 a los riesgos de la inteligencia artificial— y permitió constatar hasta qué punto la madurez, la identidad y la gestión de la cadena de suministro se han convertido en ejes prioritarios.

Rosalía Arroyo

La mesa reunió a David González, CISO de Coren; Pablo Iglesias, CISO de Luckia; José Antonio Pizarro, director de seguridad de la información de la Universidad de la Coruña; Santiago Ramón Paz, jefe de infraestructura TIC y Ciberseguridad de La Voz de Galicia; Luis Álvarez, CISO de Grupo Itelsis; Jesús M. García, CIO de la Corporación de servicios audivisuais de Galicia, CSAG; Lois Orosa, director del Centro de supercomputación de Galicia (CESGA); Javier Fernández, director técnico de Protese Sistemas de Seguridad; Alfonso Díaz Cobo, Account Manager de Commvault; Pedro Jorge Viana, Head of Presales de Iberia, UK & Irlanda de Kaspersky; Juan Rodríguez, director regional iberia de Mastercard; José Manuel Moreno, Cybersecurity Director de NTT DATA Inc; Álvaro Fernández, Senior Manager, Enterprise Sales, Spain & Portugal de Sophos, y Mónica Banegas, Enterprise Sales Engineer de Varonis, en una conversación que combinó la visión de los responsables de ciberseguridad e IT de usuario final con el enfoque de fabricantes y proveedores de servicios.

Planes de ciberrecuperación frente a planes de recuperación ante desastres

La digitalización ha transformado los planes de recuperación: si antes se centraban en fallos técnicos o desastres, hoy el ransomware obliga a ir más allá. Ya no basta con restaurar sistemas, es imprescindible garantizar que los datos sean íntegros, lo que plantea si la ciberrecuperación debe considerarse una extensión del plan de recuperación de desastres o un enfoque propio.

David González, CISO de Coren, apuntó que, en realidad, ambos planes acaban solapándose porque "la ciberseguridad hoy en día está presente en todas las partes de la empresa". A su juicio, el plan de desastres tiene un enfoque más global, mientras que el de ciberincidentes debería centrarse en la reacción inmediata y en protocolos claros para distintos escenarios, desde un phishing hasta un ransomware.

En esa misma línea, José Antonio Pizarro, de la Universidad de la Coruña, subrayó que la recuperación exige un alto grado de madurez. Recordó que durante la pandemia muchas organizaciones tuvieron que improvisar ante situaciones inéditas, lo que evidenció que un plan de recuperación no puede quedarse solo en lo técnico. "Requieren una mejora continua y una constante reevaluación", afirmó, insistiendo en que son

procesos que nunca se dan por cerrados.

Desde la visión del fabricante, Alfonso Díaz Cobo, Account Manager de Commvault destacó que el cambio más relevante ha sido pasar de recuperaciones motivadas por accidentes a tener que hacer frente a ataques deliberados. Eso obliga a replantearse todo el proceso: no solo hay que restaurar rápido, también hay que asegurarse de que los datos son fiables. “Ya no basta con la alta disponibilidad; ahora es clave asegurarse de que el dato que devuelve esa producción esté limpio”, señaló. Además, puso el foco en la necesidad de definir el “negocio mínimo viable” para resistir tras un ataque y de probar periódicamente los planes para comprobar que realmente funcionan.

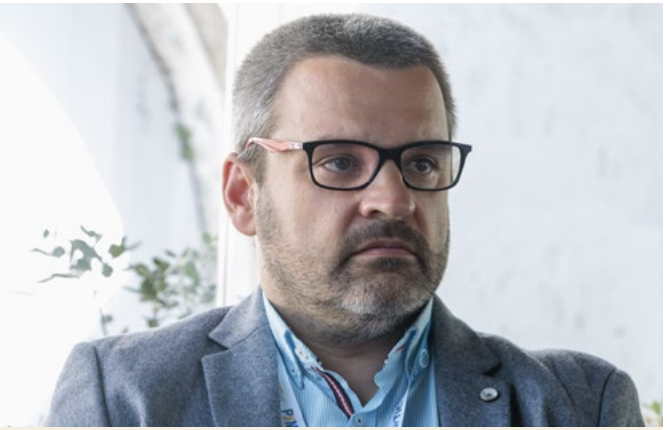
“Puedes tener muchas medidas, pero si un atacante consigue credenciales legítimas, gran parte de esas defensas dejan de ser efectivas”

David González,
CISO, **Coren**

Detección y respuesta: entre la manualidad y la automatización

La detección y respuesta es un indicador clave de madurez, pero muchas empresas siguen dependiendo de procesos manuales. El reto está en avanzar hacia la automatización sin perder control ni disparar costes.

Pablo Iglesias, CISO de Luckia Games, explicó que la mayoría de las compañías siguen en una fase inicial. “Se empieza con herramientas independientes —firewalls, EDR, filtrado del correo y web— y luego se intenta correlacionar todos esos eventos”, señaló. El gran obstáculo, según dijo, está en los costes de integración y en la falta de madurez y complejidad de integración de muchas soluciones, lo que convierte la automatización en “una gran barrera de entrada para muchas compañías”.



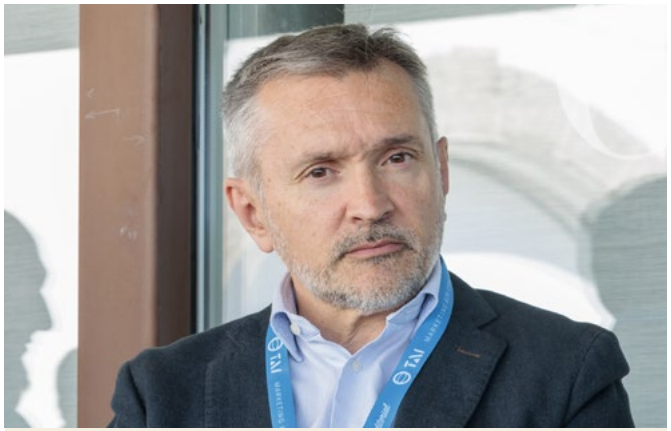
“Los costes de integración siguen siendo una barrera de entrada enorme para avanzar hacia una detección y respuesta realmente automatizadas”

Pablo Iglesias,
CISO, **Luckia Games/Grupo Egasa**

Reconociendo que el tejido empresarial gallego está compuesto en su mayoría por pymes y autónomos, recordó que empiezan a aparecer iniciativas que buscan democratizar estas capacidades a trasvés de grandes proveedores que ofrecen paquetes básicos (as a Service) de EDR, SIEM y monitorización a precios más asequibles para pequeñas empresas.

José Antonio Pizarro defendió abiertamente la automatización como una vía imprescindible para organizaciones sin SOC 24/7, como es el caso de muchas universidades.

Pedro Jorge Viana, Head of Presales de Iberia, UK & Irlanda de Kaspersky, aportó la visión del fabricante, recordando que la estrategia depende del tipo de organización. En un entorno industrial, por ejemplo, no se puede automatizar a ciegas sin evaluar el impacto en la continuidad de negocio. A su juicio, lo fundamental es adaptar la estrategia a la madurez y a los recursos de cada empresa, y apoyarse en servicios gestionados como MDR cuando no es viable montar un SOC propio. “Los dolores son los mismos —afirmó—, lo único que cambia es el equipo”, aseguró.



> “La concienciación es la medida más rentable para ganar en ciberseguridad y sigue siendo un eslabón débil en muchas organizaciones”
>
> **José Antonio Pizarro,**
> director de seguridad de la Información,
> **Universidad de la Coruña**

Proactividad vs. reactividad: concienciación y memoria corta

El debate sobre si la ciberseguridad se gestiona de forma más reactiva que preventiva puso de relieve una realidad compartida: muchas organizaciones sólo actúan cuando ya han sufrido un incidente.

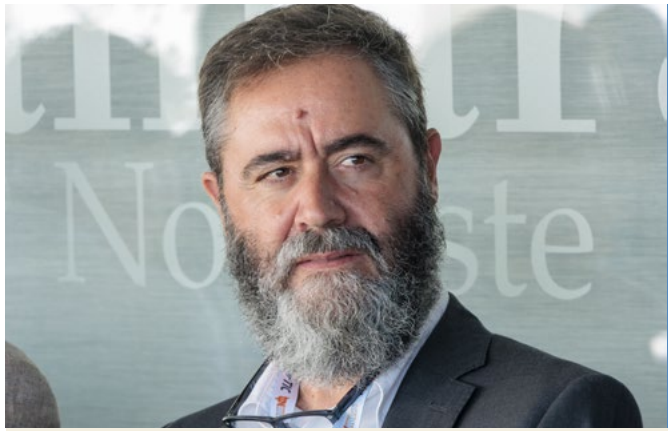
Luis Álvarez, de CISO de Grupo Itelsis, fue claro al señalar que la proactividad está limitada a un grupo reducido de empresas con más recursos y conciencia, mientras que “la gente solo va a actuar el día que pierde la copia de seguridad o cuando un archivo aparece con una extensión rara y no se puede abrir”. Incluso en sectores críticos, como el eléctrico, muchas compañías siguen a la espera de que normativas como NIS2 las fuercen a actuar, a dar el paso.

En el ámbito de los medios, Santiago Ramón Paz, de La Voz de Galicia, señaló que desde sistemas intentan mantener un enfoque preventivo, aunque reconoció que aún existen carencias y que es necesario aprovechar la normativa europea como palanca para implicar a la dirección en nuevas inversiones.

La visión de Juan Rodríguez, director regional de Mastercard, añadió un matiz global. Para él, ser proactivo significa ampliar la mirada más allá de la propia empresa e incluir también a proveedores y socios. Subrayó además la importancia de la concienciación interna como he-

rramienta fundamental para reforzar la cultura de ciberseguridad en cualquier organización."

Pablo Iglesias, de Luckia, se mostró más pesimista al advertir que la sensación de riesgo suele ser cortoplacista salvo que el incidente haya tenido un gran impacto en la organización. Tras un incidente se suelen aprobar inversiones o se implantan nuevos controles, pero al cabo de un tiempo vuelven las dudas sobre si realmente la inversión justifica la mitigación del riesgo. Por eso el reporte a la dirección de métricas e indicadores sobre la efectividad de estos controles es vital en cualquier organización". "La reactividad suele ser de memoria corta", resumió.



"La gestión de identidades es la base para afrontar entornos híbridos con garantías"

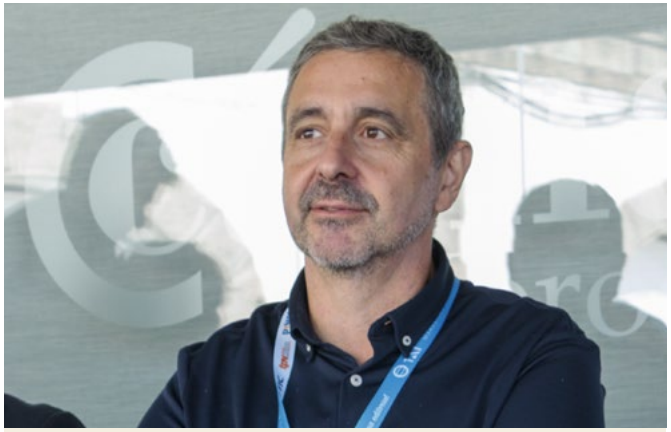
Santiago Ramón Paz,
jefe de infraestructuras TIC y Ciberseguridad/Informática,
La Voz de Galicia

Inteligencia artificial y automatización: entre la oportunidad y el descontrol

La irrupción de la inteligencia artificial en el ámbito de la ciberseguridad abrió un nuevo capítulo en la mesa. La pregunta no fue tanto si se está usando, sino hasta qué punto se está gobernando de manera adecuada.

Javier Fernández, director técnico de Protese Sistemas de Seguridad, reconoció que para muchas empresas de menor tamaño el uso de inteligencia artificial en ciberseguridad sigue siendo un terreno incipiente. El debate, apuntó, está más en analizar su potencial y sus posibles aplicaciones que en su implantación real.

Desde una visión más amplia, José Manuel Moreno, Cybersecurity Director de NTT DATA Inc, defendió que antes de aplicar IA en ciberseguridad es necesario establecer un marco de gobierno. Según explicó, en muchas organizaciones la IA ya se está utilizando de forma dispersa, sin control sobre qué se comparte ni con qué fines. "Antes de utilizarla hay que empezar con el gobierno de la IA dentro de la organiza-



"La parte más débil de la cadena suele ser el cliente, y eso nos obliga a un control exhaustivo de accesos y conexiones"

Luis Álvarez,
CISO/Informática, **Grupo Itelsis**

ción y a partir de ahí ver qué casos de uso se pueden implantar", subrayó, aunque reconoció que las posibilidades son enormes para optimizar procesos y ganar velocidad.

Visibilidad más allá del perímetro

La protección de entornos híbridos exige más visibilidad y control: las herramientas por sí solas no bastan y deben complementarse con servicios y equipos especializados.

Jesús M. García, de la Corporación de Servicios Audiovisuais de Galicia, explicó cómo recientemente se ha acelerado la adopción de medidas más estrictas, desde la implantación de EDR y antivirus hasta la actualización de firewalls y la monitorización con SIEM 24x7. Sin embargo, lanzó una preocupación compartida por muchos: ¿qué ocurre cuando la amenaza ya está dentro? "Tenemos 60 petabytes de vídeos que hay que proteger y la emisión diaria no puede parar. Pero una vez detectas algo internamente, ¿qué pasa después?", se preguntó, mostrando escepticismo sobre si la automatización puede ser la respuesta.

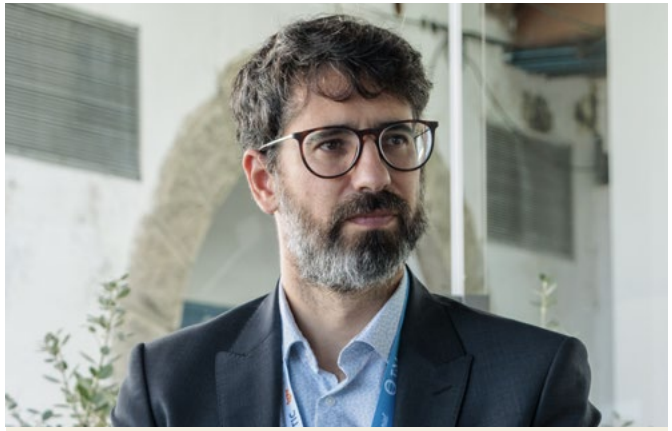
Desde la perspectiva del fabricante, Álvaro Fernández, Senior Manager, Enterprise Sales, Spain & Portugal de Sophos, coincidió en que la clave está en combinar tecnología con capital humano. Señalando que la protección no acaba con desplegar EDR o SIEM sino que hace falta investigar y actuar de forma constante, ya sea con un equipo interno 24x7 o recurriendo a servicios gestionados como MDR, que aportan ese seguimiento continuo. Recordó, además, que las vulnerabilidades siguen siendo la puerta de entrada número uno para el ransomware y que, pese a ser un problema conocido, muchas organizaciones siguen sin abordarlo de forma eficaz.

> "En nuestro sector, la continuidad del servicio es irrenunciable: no se puede permitir que la pantalla se quede en negro"
>
> **Jesús M. García,**
> CIO/Informática, **Corporación de servicios audivisuais de Galicia/csag**

Juan Rodríguez, de Mastercard, enlazó esta reflexión con la necesidad de pasar de la reactividad a la proactividad. Destacó el valor de los servicios de inteligencia de amenazas que permiten anticiparse al comportamiento de los atacantes, detectando, por ejemplo, si un directivo está siendo investigado en la dark web o si circulan credenciales comprometidas. "En vez de esperar a ver qué me pasa, ya sé que me van a hacer algo y puedo preverlo", señaló, insistiendo en que estas capacidades ya no están reservadas solo a los grandes SOC, sino que empiezan a llegar directamente a las empresas.

Seguridad del dato: del inventario al control de accesos

Cuando se habló de los planes directores en materia de protección de datos, quedó claro



"Nuestra prioridad siempre han sido los servicios a los investigadores, pero si queremos avanzar necesitamos reforzar nuestros sistemas de seguridad"

Lois Orosa,
director, **CESGA**

que cada organización lo aborda desde una realidad distinta, pero todas coinciden en que el dato se ha convertido en un activo crítico cuyo valor va mucho más allá de tenerlo almacenado de forma segura.

Lois Orosa, director del CESGA, explicó que, en el caso de su centro de supercomputación, los riesgos hasta ahora eran limitados porque la mayoría de la información es de investigación y está anonimizada. Sin embargo, el escenario cambia con los nuevos proyectos en datos médicos y genómicos, que les obligan a implantar el Esquema Nacional de Seguridad.

Desde una perspectiva más pragmática, Pablo Iglesias, de Luckia, resumió su posición en una sola medida clave: "Por mucho que protejas tus datos, la única solución que tienes para preservarlos es hacer una copia inmutable deslocalizada y tener un buen plan de recuperación". En su opinión, solo esta estrategia garantiza que la información pueda recuperarse tras un ataque.

La intervención de Mónica Banegas, Enterprise Sales Engineer de Varonis, puso el foco en un aspecto a menudo olvidado: la protección interna. "Siempre hablamos de EDR, de SIEM, del perímetro, en lugar de qué pasa si yo llamo y me abren la puerta, o qué pasa si directamente yo ya tengo llave para entrar". Para la directiva, la primera medida de un plan director debería ser identificar dónde están los datos, qué nivel de sensibilidad tienen y quién accede a ellos. Solo así se puede aplicar un control efectivo de permisos y trazar un plan de remediación.

"En muchas empresas pequeñas, el debate sobre la inteligencia artificial está más en analizar su potencial que en implantarla"

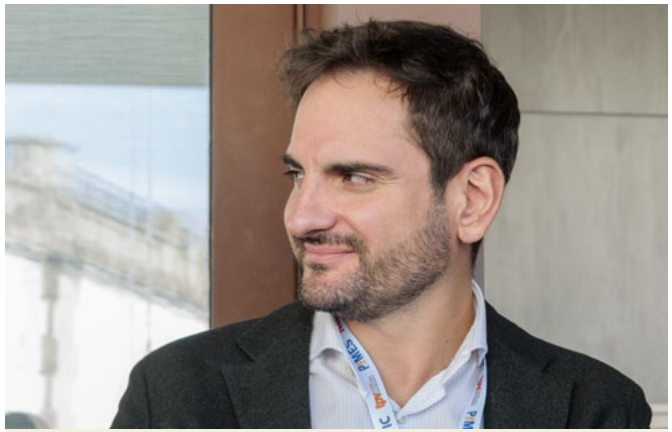
Javier Fernández,
director técnico de **Protese Sistemas de Seguridad**

En esa línea, David González, de Coren, insistió en la importancia de inventariar y catalogar la información, y en aplicar cifrado tanto en tránsito como en reposo. Tener un control de accesos riguroso y usar herramientas y estrategias como DLP, DSPM o DDR También recordó que, frente a los ataques de ransomware actuales, la exfiltración de los datos para extorsionar, es tan crítico como su cifrado.

Para cerrar, desde Varonis se subrayó que incluso con credenciales legítimas es posible detectar comportamientos anómalos si se analizan los patrones de uso. Puso como ejemplo la creación repentina de cientos de cuentas de administrador o accesos desde ubicaciones inusuales, señales que deberían activar las alarmas antes de que el atacante ejecute el ransomware.

Estrategias en entornos híbridos: identidad, automatización y responsabilidad compartida

La transición hacia modelos híbridos —con datos y aplicaciones distribuidos entre infraestructuras on-premise y la nube— obliga a replantear cómo se diseñan las estrategias de prevención,



> “La identidad, junto con el dato, se ha convertido en uno de los activos más importantes que hay que proteger”
>
> **José Manuel Moreno,**
> Cybersecurity Director, **NTT DATA Inc**

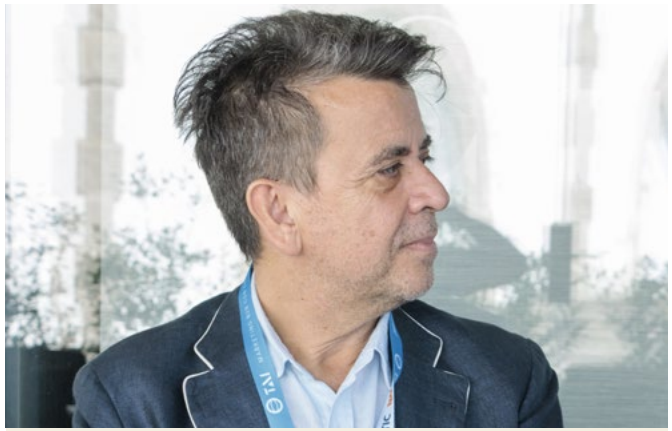
detección y respuesta. La complejidad aumenta, pero los ponentes coincidieron en algunos pilares fundamentales: la gestión de identidades, la automatización y la claridad sobre las responsabilidades en la nube.

Santiago Ramón Paz, directivo de La Voz de Galicia, subrayó que la gestión de identidades es el punto de partida. Explicó que en su organización han apostado por un enfoque zero trust, con control estricto de privilegios y políticas de acceso basadas en roles y en la clasificación de la información. “Cualquier acceso al dato con un cierto nivel de privilegio debe pasar por un mecanismo de gestión de identidades”, apuntó.

Desde la visión de fabricante, Alfonso Díaz Cobo incidió en que la prevención pasa también por la capacidad de las herramientas para correlacionar eventos y trabajar de forma integrada. “Los clientes no quieren soluciones en nicho, sino que sean capaces de hablar entre ellas”, señaló. Además, puso el acento en que la recuperación en la nube no se limita a bases de datos o instancias, sino que incluye también firewalls, balanceadores de carga o gateways. En este sentido, la automatización resulta clave para restaurar de manera eficaz y minimizar tiempos de inactividad.

Otro de los intervinientes recordó la importancia de no perder de vista el modelo de responsabilidad compartida. En cloud, explicó, parte

de la seguridad recae en el proveedor, pero otra parte corresponde al cliente. Tener claras esas fronteras es esencial para definir qué medidas aplicar en cada capa.



"Cada vez más clientes empiezan a evaluar los riesgos de su cadena de suministro con una visión multidimensional, no solo ciber"

Juan Rodríguez,
director regional iberia, **Mastercard**

IT y OT: mundos que empiezan a acercarse

La integración entre la seguridad IT y OT sigue siendo uno de los grandes retos en sectores críticos. Aunque cada vez hay más conciencia de que ambos mundos deben coordinarse, la realidad es que en muchas organizaciones aún funcionan como compartimentos estancos.

Explicó el CISO de Coren durante el encuentro que en su empresa ha intentado que no exista esa separación, ya que él mismo gestiona ambas áreas. Sin embargo, reconoció que "en general siguen siendo mundos bastante separados". Señaló que hay compañías donde el CISO no se responsabiliza de la parte industrial y esta acaba en manos de mantenimiento, lo que complica la coordinación. Para evitarlo, en Coren han fomentado la formación en ciberseguridad de los equipos de OT y creado grupos híbridos de trabajo entre ambas áreas.

Santiago Ramón Paz (La Voz de Galicia), destacó la dificultad de gestionar entornos industriales con equipos heterogéneos, de diferentes fabricantes y con tecnologías que en muchos casos llevan décadas en funcionamiento.

La perspectiva de fabricante corrió a cargo de Pedro Jorge Viana, Head of Presales de Iberia, UK & Irlanda, Kaspersky, quién defendió la necesidad de un enfoque transversal que incluya IT, OT e IoT bajo una misma estrategia de mo-

"Por mucho que automatices, la tecnología por sí sola no basta: necesitas capital humano para interpretar y actuar"

Álvaro Fernández,
Senior Manager, Enterprise Sales, Spain & Portugal, **Sophos**

nitorización y visibilidad. Explicó que la integración avanza más rápido de lo esperado gracias a la concienciación, pero que aún queda mucho por recorrer. “Esa capacidad de visibilidad y trazabilidad es clave, no para reaccionar, sino para detectar movimientos anormales”, afirmó, insistiendo en que allí donde no es posible securizar, al menos debe garantizarse la capacidad de observar lo que está ocurriendo.

Cumplimiento normativo y cadena de suministro: entre la teoría y la práctica

La mesa coincidió en que marcos como NIS2, DORA o GDPR plantean un doble reto: demostrar cumplimiento interno y, al mismo tiempo, monitorizar los riesgos que vienen de la cadena de suministro. Según el perfil de cada organización, el peso recae más en un ámbito u otro.

José Antonio Pizarro, de la UDC reconoció que, en su caso, NIS2 no les aplica directamente, aunque sí deben cumplir con el Esquema Nacional de Seguridad y el RGPD. Explicó que el esfuerzo se centra más en implantar medidas de protección que en demostrar su cumplimiento, aunque las certificaciones suponen un trabajo añadido: “La prioridad es ser seguros, pero cuando quieres certificarte requiere mucho esfuerzo demostrar que lo estás haciendo”.

> “El ransomware ha cambiado las reglas: ya no basta con la alta disponibilidad, hay que asegurarse de que el dato restaurado esté limpio”
>
> **Alfonso Díaz Cobo,**
> Account Manager, **Commvault**

En cambio, Luis Álvarez (Grupo Itelsis) explicó que en su sector —la distribución eléctrica— NIS2 está muy presente, aunque aún genera incertidumbre. Sus clientes esperan a que la directiva marque plazos y obligaciones claras para adaptarse, lo que genera retrasos en la adopción. En su caso, la mayor preocupación está en la cadena de suministro, pero no tanto por los proveedores, sino por los propios clientes, lo que le ha llevado a tener que establecer controles estrictos sobre accesos y monitorización geográfica para evitar riesgos.

Desde la visión de mercado, Juan Rodríguez recordó que la presión regulatoria suele acelerarse con la primera sanción ejemplar, como ya pasó con GDPR. Aun así, defendió que muchas organizaciones que ya cuentan con certificaciones como ISO 27001 o ENS están en buena posición para adaptarse. También destacó un cambio de tendencia: las empresas están ampliando el análisis de riesgos a una visión más global que va más allá de la ciberseguridad. “Ya no solamente ciber, sino también financiero, de protección de datos o incluso criterios ESG”, explicó. Cada proveedor se evalúa en función de su criticidad, con más exigencia para los estratégicos y un análisis más ligero para los secundarios.

Identidad y accesos: el nuevo perímetro de seguridad

La protección de la identidad se ha consolidado como uno de los ejes centrales de la ciberseguridad. Con la nube, el IoT y la inteligencia artificial multiplicando los puntos de entrada, ya no se trata solo de proteger dispositivos o redes, sino de asegurar que cada credencial y cada acceso están bajo control.

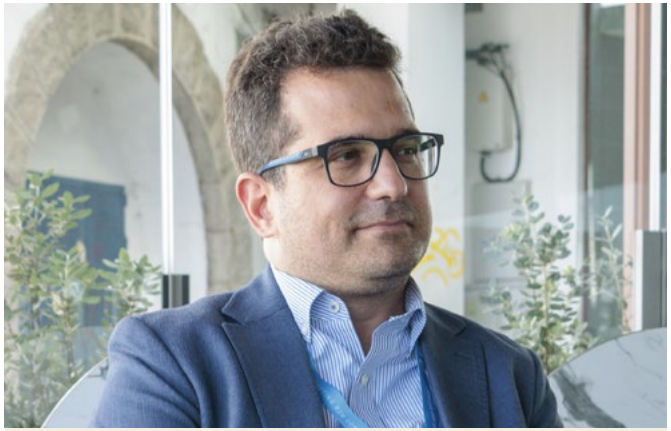
> "La primera medida para mitigar riesgos es identificar dónde están los datos, quién accede a ellos y con qué permisos"

Mónica Banegas,
Enterprise Sales Engineer, **Varonis**

La experiencia de José Antonio Pizarro, de la Universidad de la Coruña ilustró bien el impacto de medidas concretas. Tras la invasión de Ucrania, aceleraron la implantación del MFA en toda la universidad, incluidos los alumnos. El cambio fue inmediato: de unos 300 incidentes anuales de robo de contraseñas, pasaron a apenas unos pocos. "Fue el día y la noche", admitió, añadiendo que, para él, la clave está también en la concienciación, sobre la que asegura que "es la forma más rentable de ganar en ciberseguridad".

José Manuel Moreno, de NTT DATA Inc insistió en que la identidad es ya tan crítica como el propio dato. El reto, señaló, es unificar la autenticación en un solo sistema en lugar de mantener silos en diferentes entornos cloud o entornos u on-premise. En su opinión, el verdadero perímetro de la organización hoy son las credenciales de los usuarios.

Álvaro Fernández, de Sophos, aportó un dato revelador: el 32 % de los incidentes se deben a vulnerabilidades no parcheadas y el 29 % a credenciales comprometidas. "Poner un MFA es básico", afirmó, recordando que aún el 93 % de las compañías no lo tienen implementado.



> "La integración IT y OT avanza más rápido de lo esperado, pero aún queda mucho camino por recorrer"

Pedro Jorge Viana,
Head of Presales de Iberia, UK & Irlanda, **Kaspersky**

IA generativa: entre el bloqueo y la gobernanza

El cierre de la mesa se centró en uno de los temas más actuales: cómo controlar el uso de la inteligencia artificial generativa en las organizaciones para evitar fugas de información o usos indebidos. Las posiciones oscilaron entre medidas restrictivas y planteamientos más estratégicos de gobernanza.

David González explicó que en su compañía ya han tomado medidas concretas: “Monitorizamos y bloqueamos. Hay IAs generativas que están directamente prohibidas y otras que permitimos con filtros”. Añadió que, además, forman y asesoran a los usuarios con recomendaciones específicas para fomentar un uso responsable. Reconoció que no es una solución perfecta, pero sí un primer paso para reducir riesgos.

En el ámbito de los medios de comunicación, Santiago Ramón Paz señaló que, por ahora, la única forma de trabajar con IA generativa es mantenerla completamente fuera de la red corporativa. Una medida drástica, pero que refleja la desconfianza hacia el potencial de fuga de datos.

Desde la perspectiva de fabricante, Mónica Banegas, de Varonis, recalcó que la clave está en implementar la tecnología con controles de seguridad desde el inicio, especialmente en torno a la identidad y al acceso. Puso como ejemplo Copilot de Microsoft, cuyo nivel de exposición depende de los permisos del usuario, lo que hace imprescindible una gestión previa de roles y accesos.

Mónica Banegas también destacó la importancia de mirar más allá de los límites de la empresa: “Tu partner, tu proveedor o tu socio puede estar usando la IA e introduciendo en ella tus datos”. Para ella, la cadena de suministro debe estar incluida en cualquier plan de control, ya que el riesgo no termina en la organización propia.

El Foro TAI Galicia dejó varias conclusiones claras. La primera, que la madurez sigue marcando la diferencia: sin ella, la automatización, la recuperación del dato o la aplicación de normativas se quedan cortas. La segunda, que la identidad se consolida como el nuevo perímetro, con MFA, monitorización y control de accesos como medidas mínimas. La tercera, que la IA abre una oportunidad, pero exige gobernanza y control para evitar que se convierta en una amenaza más.

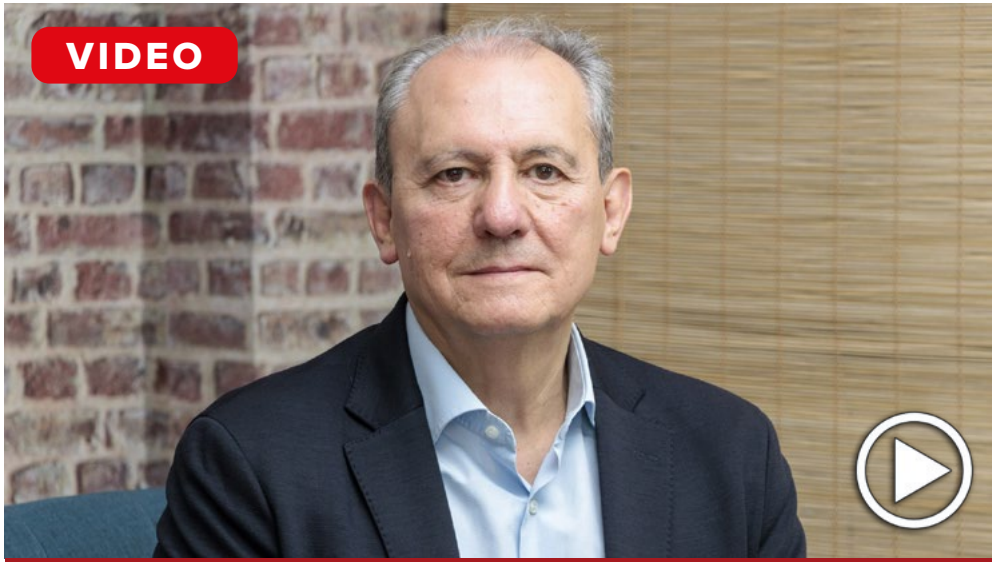
Finalmente, el encuentro reflejó que Galicia comparte los mismos desafíos que el resto de Europa: un tejido de pymes con recursos limitados, sectores críticos en plena transformación y la necesidad de combinar tecnología con servicios y personas para construir una ciberseguridad verdaderamente resiliente.

Allied Telesis o cómo proteger la red

La inteligencia artificial generativa se ha convertido en un elemento esencial para la gestión y optimización de redes. Luis González, director de Allied Telesis señala que la misma se está utilizando para planificar, analizar y mejorar el rendimiento de infraestructuras.

El fabricante japonés, especializado en soluciones de redes inteligentes y conectividad, ofrece a las empresas una integración de los entornos IT-OT, facilitando su seguridad a través de aplicaciones específicas que detectan y controlan amenazas gracias a su interlocución con el firewall, llevando a cabo las acciones necesarias en el resto de la red. También apuestan por una gestión predictiva, monitorizando parámetros como la carga, la memoria o la CPU para anticipar fallos y evitar interrupciones del servicio.

Con este enfoque, Allied Telesis combina automatización, inteligencia artificial y ciberprotección para ofrecer una gestión de red más eficiente, resiliente y preparada ante los desafíos del futuro digital.



Luis González, director de **Allied Telesis**

Allied Telesis™

Commvault: “La ciberresiliencia convierte la continuidad de negocio en negocio continuo”

Durante este vídeo David Sanz, director de Customer Experience para el Sur de Europa de Commvault, explica cómo la compañía redefine la continuidad de negocio bajo el concepto de “negocio continuo”, un estado de preparación y recuperación permanente frente a amenazas constantes. Basado en cuatro pilares —seguridad, preparación, rebalanceo y recuperación continuos—, este modelo integra la ciberresiliencia en el corazón de la estrategia empresarial. La plataforma Commvault Cloud, reconocida por Gartner, unifica la protección y recuperación de datos en cualquier entorno, incorporando innovaciones como Clean Room Recovery, Cloud Rewind o Clumio Backtrack. Sanz destaca además el concepto de compañía mínima viable, que permite seguir operando tras un ataque, y la necesidad de que CIO y CISO trabajen juntos: “No se trata de si nos atacarán, sino de cuándo. Hay que estar preparados.”

David Sanz, director de Customer Experiencia para el Sur de Europa de **Commvault**

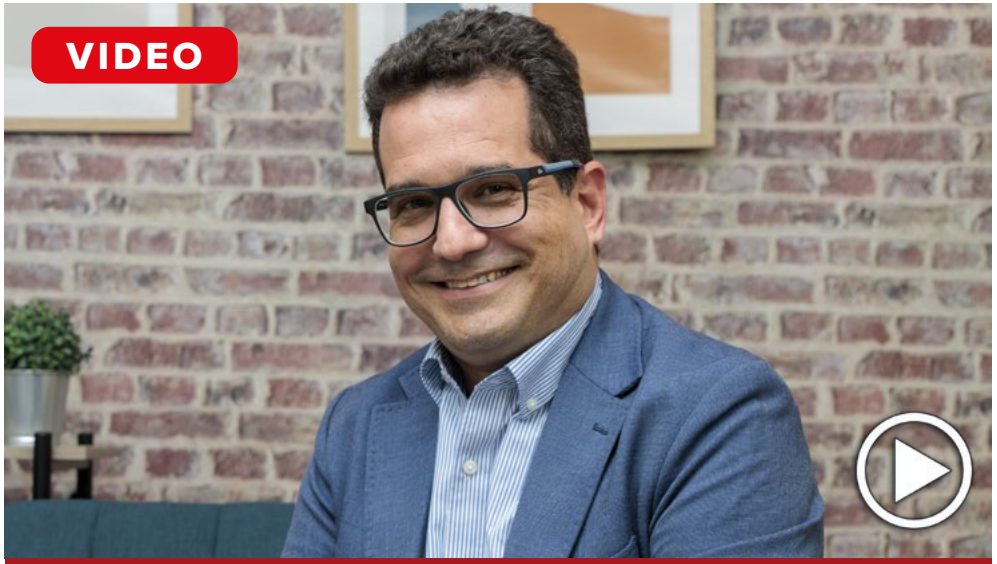
Commvault®

Kaspersky: “La visibilidad y la trazabilidad son esenciales para cumplir con NIS2 y fortalecer la resiliencia”

Pedro Viana, responsable de Preventa de Kaspersky para Iberia, Reino Unido e Irlanda, analiza en esta entrevista en vídeo la evolución de las amenazas y el papel de la visibilidad y la trazabilidad en la ciberresiliencia.

Según explica el directivo, Kaspersky ha bloqueado más de 20 millones de intentos de compromiso en entornos industriales, lo que refleja tanto el aumento de ataques como la eficacia de las defensas. “Cuantos menos puntos ciegos tenga una organización, más capacidad de detección y respuesta tendrá”, destaca.

La compañía combina soluciones XDR, EDR y MDR con inteligencia artificial para reducir falsos positivos y priorizar incidentes reales. Además, sus herramientas ayudan al cumplimiento de NIS2 gracias a la recolección de evidencias y trazabilidad. Viana subraya que la transparencia y la inteligencia de amenazas son algunos de los rasgos diferenciales de Kaspersky.



Pedro Viana, responsable de Preventa de **Kaspersky** para Iberia, Reino Unido e Irlanda

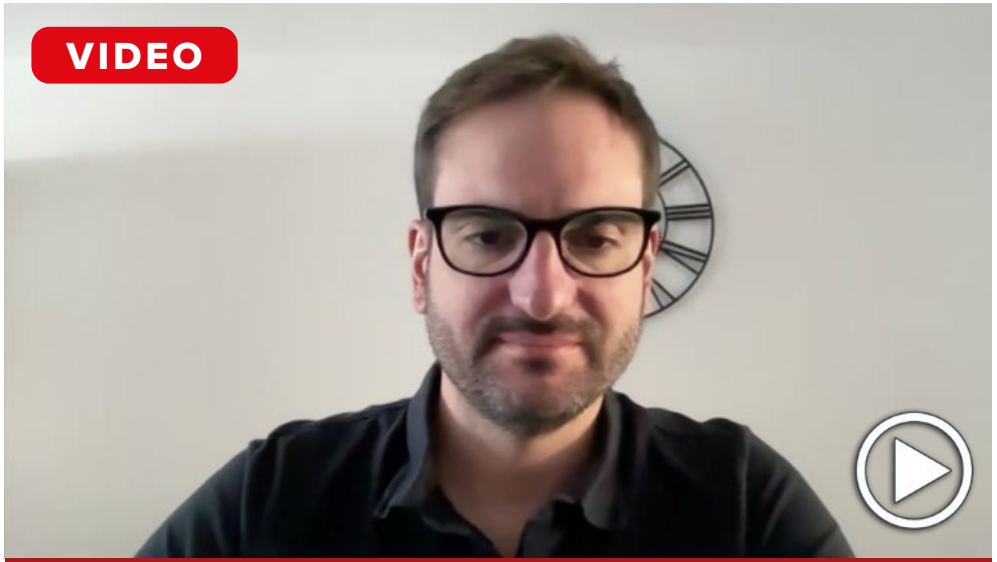
kaspersky

NTT DATA Inc: “Las organizaciones deben aprender a defenderse con la misma velocidad con la que evoluciona la amenaza”

Durante este vídeo José Manuel Moreno Guerra, Cybersecurity Director de NTT DATA Inc Europe & Latam, explica cómo la compañía ayuda a las organizaciones a protegerse en un entorno cada vez más complejo.

Destaca el directivo el crecimiento de ataques impulsados por inteligencia artificial, “más rápidos y precisos”, especialmente contra infraestructuras críticas. Defiende el valor de los modelos Zero Trust y SASE como un cambio de cultura, no sólo de tecnología, que requiere experiencia y acompañamiento.

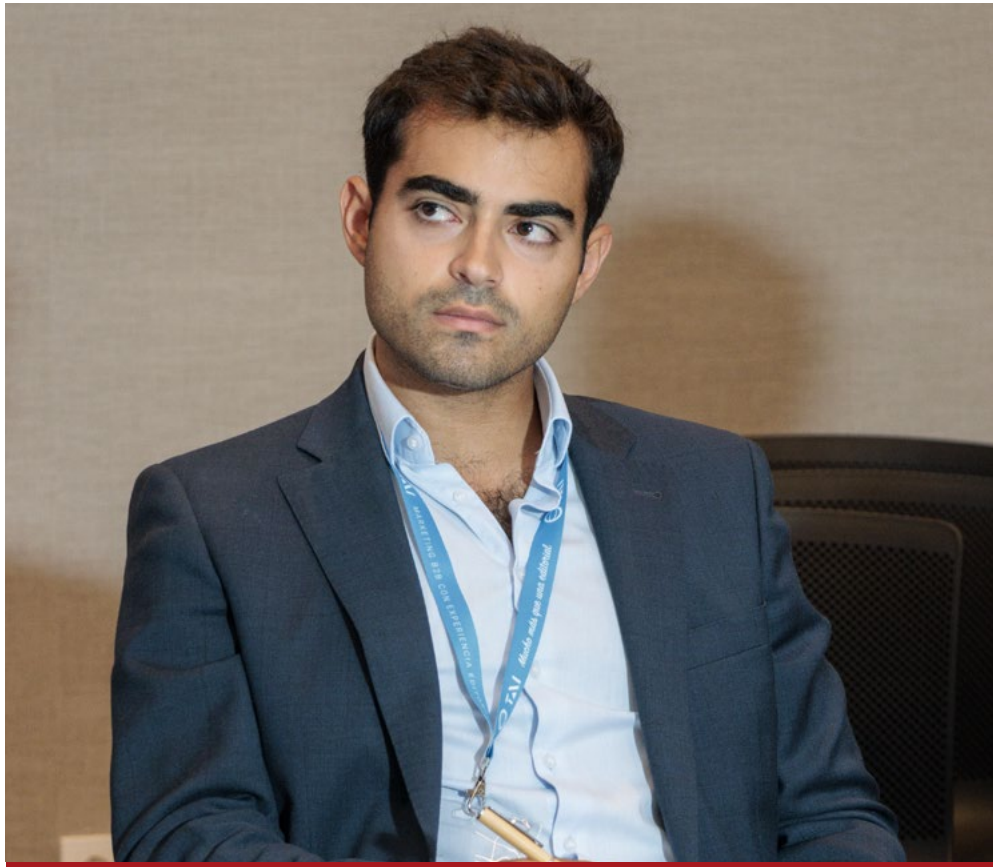
En materia de cumplimiento, NTT DATA Inc combina inteligencia artificial y metodologías GRC para simplificar la adaptación a normativas internacionales. Su ventaja competitiva, señala, radica en su visión global, la capacidad tecnológica y una infraestructura que permite anticipar amenazas y ofrecer una respuesta rápida y eficaz, elevando la resiliencia empresarial.



José Manuel Moreno Guerra, Cybersecurity Director de **NTT DATA Inc** Europe & Latam

NTT DATA Inc, soluciones para empresas que no quieren perder el paso de la innovación

Las organizaciones tienen que superar retos en torno a la seguridad. A la hora de escalar sus entornos digitales y adaptarlos a cargas más dinámica o distribuidas. O a la de diseñar y desplegar infraestructuras para la IA, por poner algunos ejemplos. ¿Cómo puede ayudar NTT DATA Inc en este sentido? Javier Sánchez de la Poza, *GTM practice solutions specialist* responde a estas preguntas.



Javier Sánchez de la Poza, *GTM practice solutions specialist* de **NTT DATA Inc**

“No se trata sólo de proteger, sino de mantener el negocio operativo pase lo que pase”

Álvaro García, Senior Manager, Enterprise Sales Spain & Portugal de Sophos, explica en el vídeo cómo la compañía aborda la ciberseguridad desde una visión integral centrada en la resiliencia operativa. “No se trata sólo de proteger, sino de mantener el negocio operativo pase lo que pase”, afirma.

La extorsión y las vulnerabilidades no parcheadas son hoy los principales vectores de ataque, y Sophos responde combinando prevención, detección y respuesta gestionada (MDR) y modelos de inteligencia artificial capaces de actuar como analistas o threat hunters. Además, su solución Zero Trust Network Access (ZNA) refuerza la segmentación y el control de identidades en entornos distribuidos. Con 40 años de historia, Sophos mantiene una premisa clara: adaptarse, innovar y proteger con transparencia.

Álvaro García, Senior Manager, Enterprise Sales Spain & Portugal de **Sophos**

SOPHOS

“Sin una infraestructura de red sólida, segura y bien gestionada, la transformación digital no puede afrontarse con garantías”

En un contexto de transformación digital, la red se convierte en el sistema nervioso de la organización. “Todo pasa por ella, desde la conectividad de sedes y almacenes, hasta aplicaciones críticas en la nube, servicios de videoconferencia o Voz IP”, recuerda Óscar León Mora, responsable de desarrollo del negocio profesional en TP-Link. Y, aunque cada vez gana más protagonismo, la red no siempre tiene el peso específico que se merece en las compañías. El fabricante trabaja para que la red pase de ser de un recurso estático a un habilitador clave del negocio con soluciones como Omada SDN, una plataforma que integra la gestión de *routers*, *switches* y puntos de acceso con soluciones o capacidades de SD-WAN avanzadas, lo que permite a las empresas gestionar y monitorizar toda la red desde un único panel.

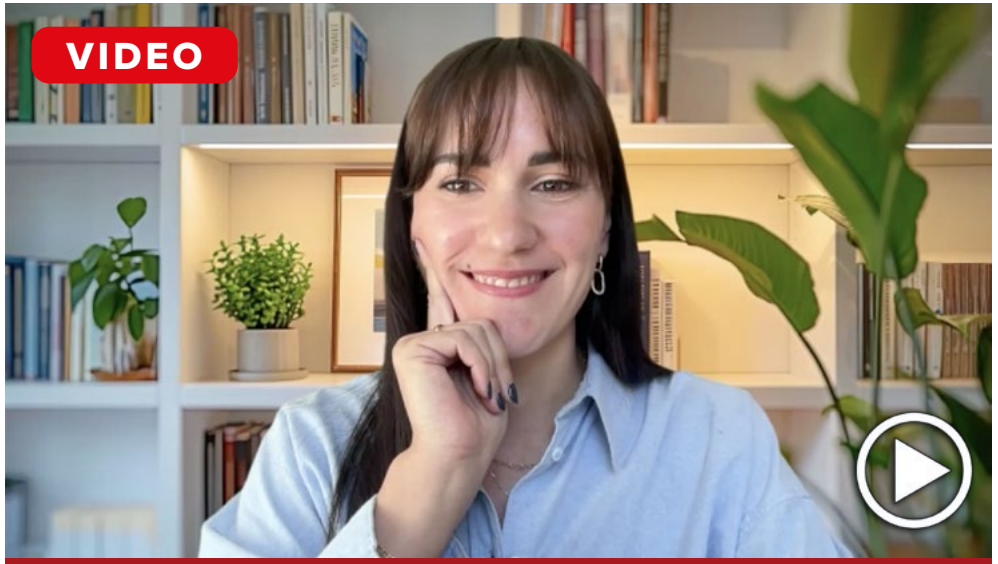
Óscar León Mora, responsable de desarrollo del negocio profesional en **TP-Link**

tp-link

Varonis: “La automatización es la única forma de mantener una estrategia Zero Trust viva”

En el Foro TAI Galicia, Mónica Banegas, Sales Engineer Team Leader en Iberia de Varonis, destacó que el mayor reto en la protección de datos es la visibilidad: “Saber dónde está la información y quién tiene acceso”, repite en el vídeo, explicando que, en un entorno híbrido y colaborativo, Varonis ofrece una clasificación completa y en tiempo real para identificar datos sensibles y reducir su exposición. Banegas subraya que los fallos de configuración o los permisos heredados amplían la superficie de ataque y que la automatización es clave para mantener una estrategia Zero Trust eficaz.

“Si hablamos de millones de archivos, la remediación debe ser automática y continua”, apunta durante la entrevista. Con su modelo *find, fix and alert*, Varonis combina visibilidad, remediación y alertas en tiempo real, reforzando la ciberresiliencia de las organizaciones.



Mónica Banegas, Sales Engineer Team Leader en Iberia de **Varonis**