Foro TAI

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

TAI

it. Colexio Oficial Enxeñeiros de Telecomunicación Galicia

PATROCINADORES

CHECK POINT™

hp / AMD

GRUPO solitium

kaspersky

NTT DATA

SAMSUNG

Symantec™ by Broadcom

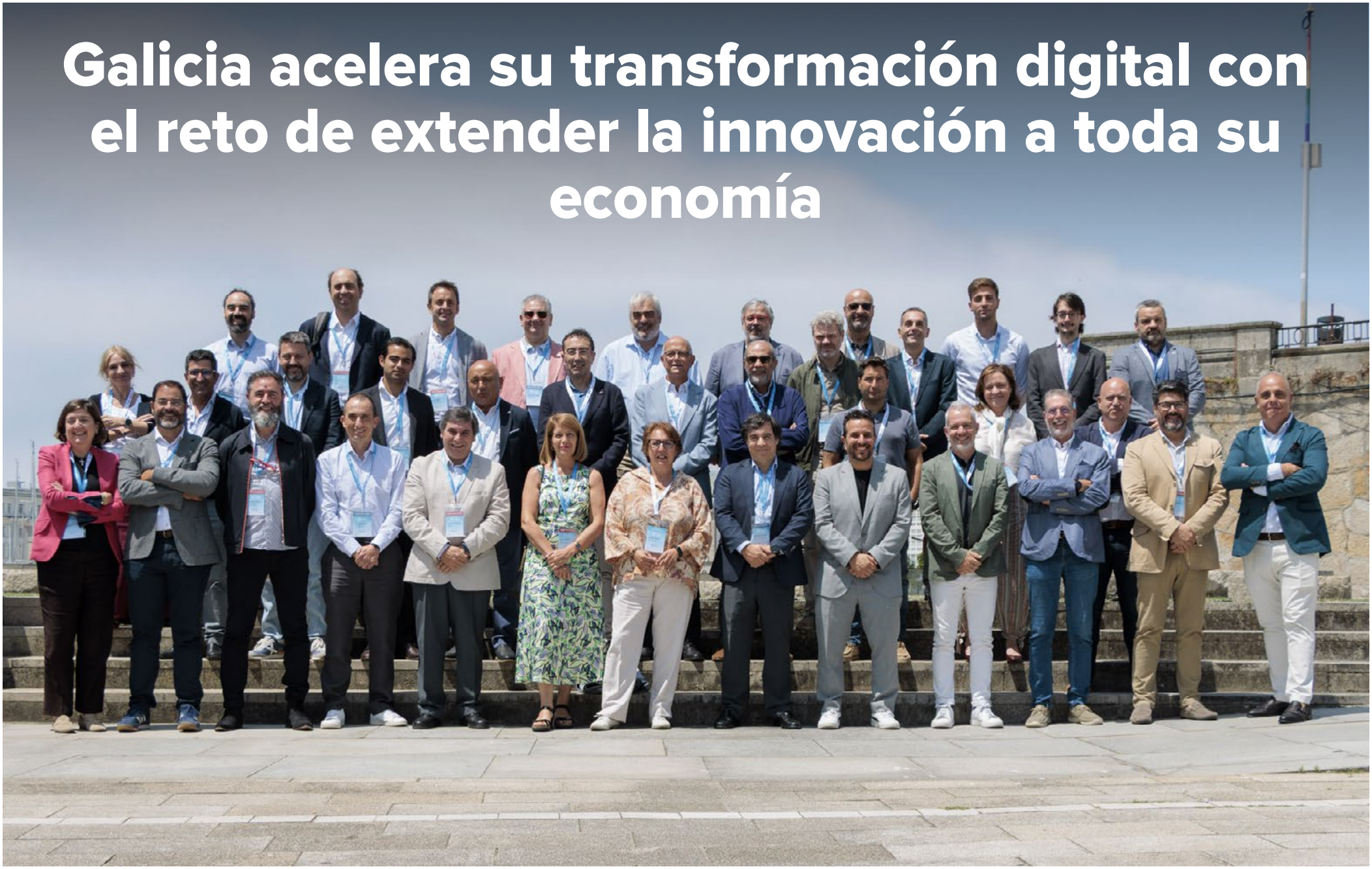
VIRTUAL CABLE

ciberseguridadTIC

Información de valor para la toma de decisiones directorTIC

IR A PÁGINA SIGUIENTE

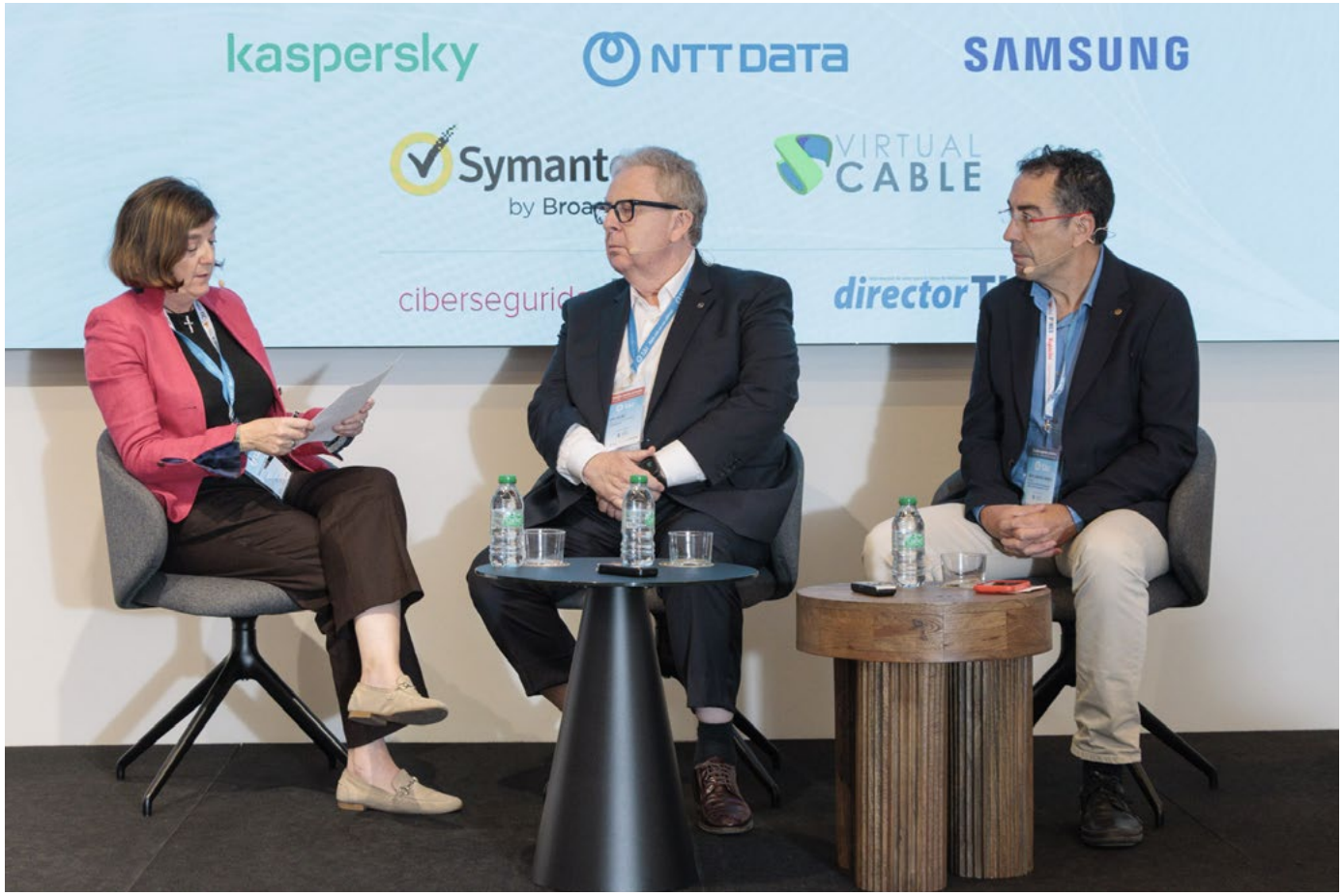
Galicia acelera su transformación digital con el reto de extender la innovación a toda su economía



Foro TAI Galicia

Galicia acogió, por segunda vez, una nueva edición de los foros tecnológicos que organiza el Grupo Tai, a través de sus publicaciones DirectorTIC y CiberseguridadTIC. En esta ocasión el evento contó con dos sesiones para analizar, respectivamente, las realidades tecnológicas del sector público y privado gracias a la participación de CIO y CISO de las principales empresas e instituciones públicas de la comunidad gallega. Grupo TAI contó con la colaboración del Colegio Oficial de Ingenieros de Telecomunicación (COIT) de Galicia. El evento estuvo patrocinado por Check Point Software, Kaspersky, HP-AMD-Grupo Solitium, NTT Data, Samsung, Symantec y Virtual Cable.

Marilés de Pedro



En la inauguración el protagonismo correspondió a Julio Sánchez Agrelo, decano del COIT en Galicia, y a José Manuel Valiño, decano de la Universidad Intercontinental de la Empresa (UIE), quienes coincidieron en que la inteligencia artificial se ha convertido en el principal vector de transformación, aunque su adopción todavía debe extenderse al conjunto del tejido empresarial.

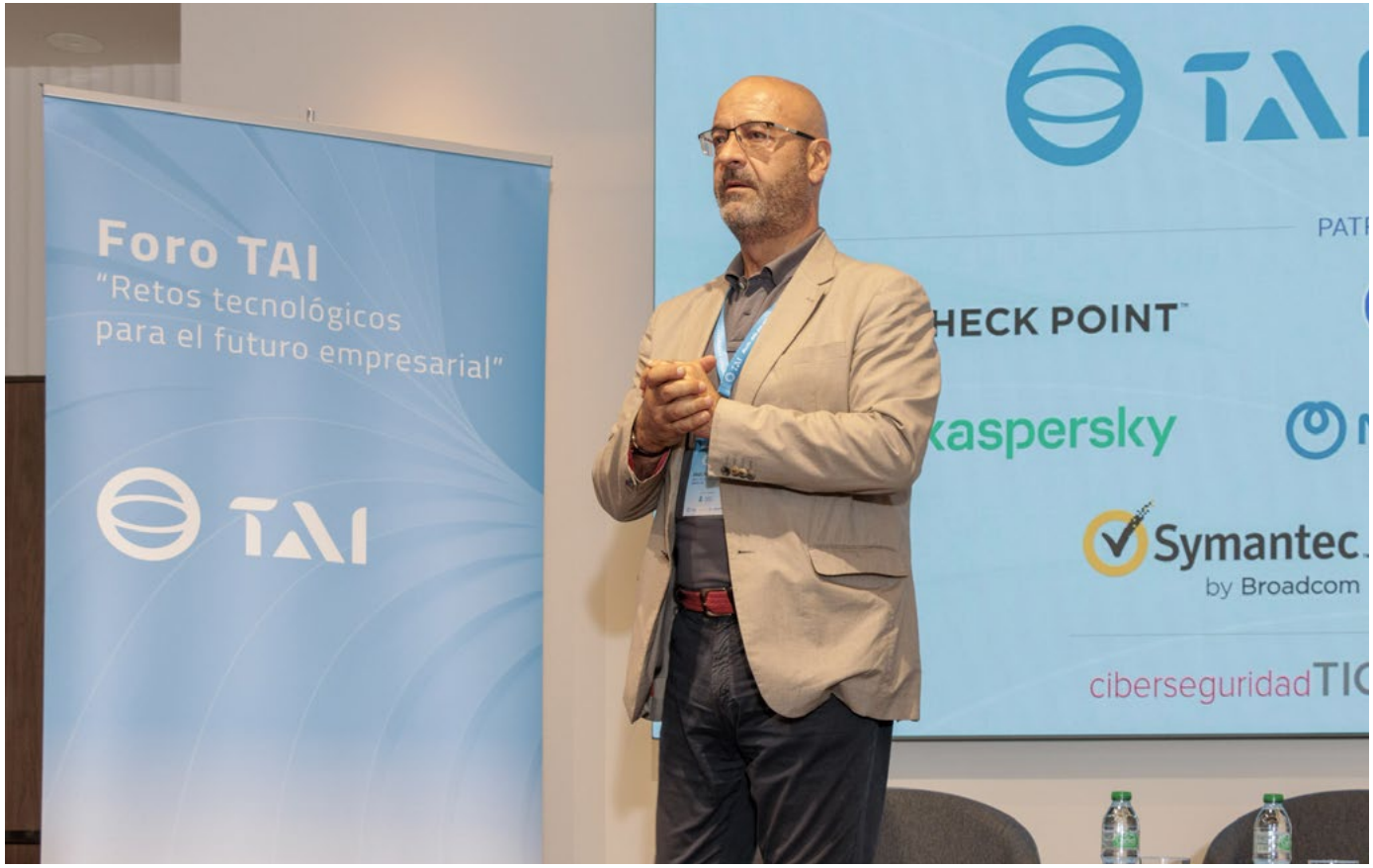
Una economía clave en España

Galicia cuenta con uno de los ecosistemas tecnológicos más dinámicos del país. La comunidad genera el 5,1 % del PIB nacional, con una economía de más de 81.800 millones de euros, lo que la sitúa como la sexta comunidad autó-

noma más importante de España por tamaño económico.

En 2025 la economía gallega creció un 2,6 %, en línea con España, que lo hizo un 2,8 %; y se sitúa 12,3 puntos por encima de los niveles prepandemia, consolidando una evolución superior a la media nacional. El sector TIC aporta entre el 2,5 % y el 3 % del PIB regional, integra a más de 3.500 empresas y da empleo directo a unas 24.000 personas.

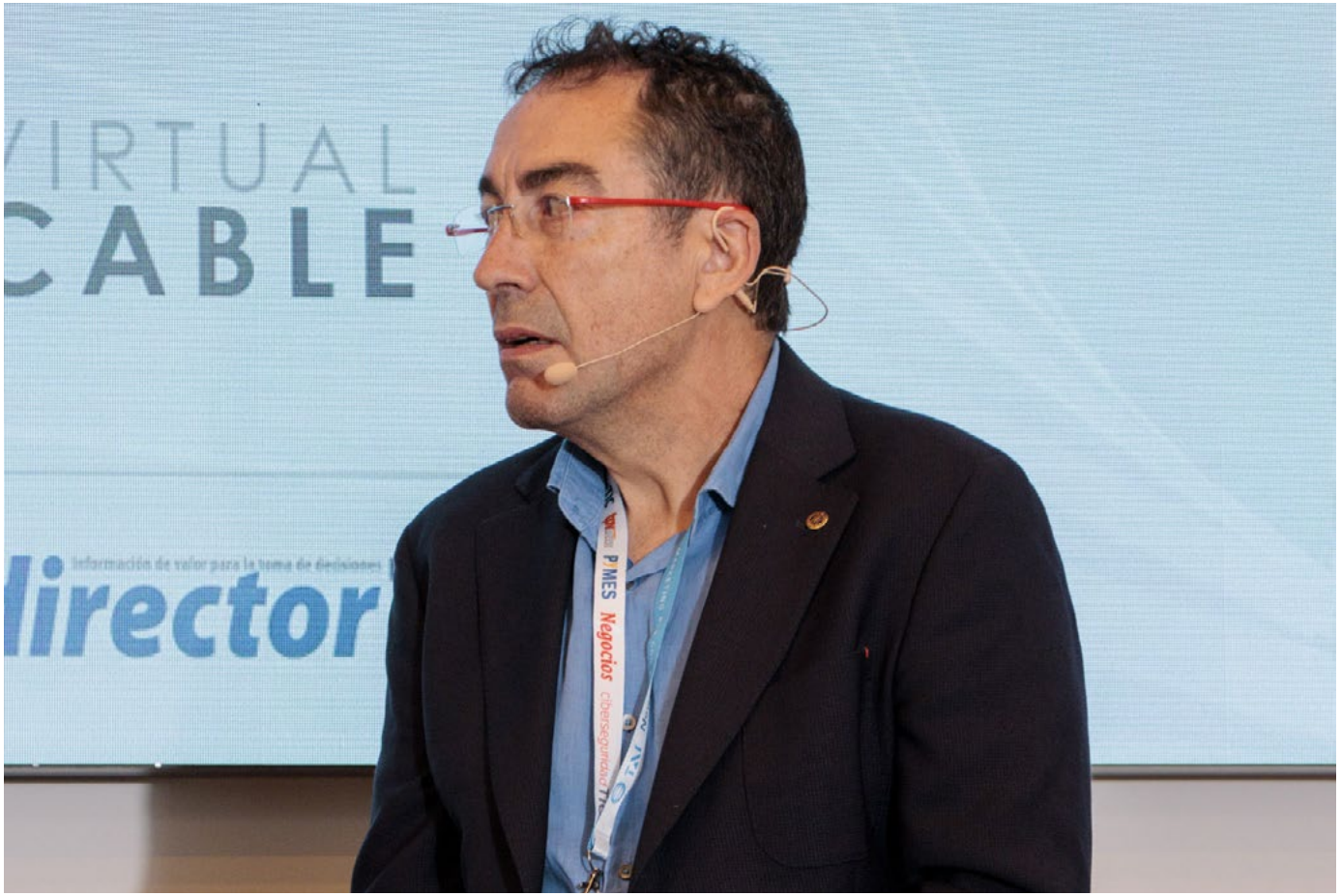
Julio Sánchez Agrelo abrió el encuentro destacando la fortaleza del sector TIC gallego, que ya ocupa la quinta posición nacional por volumen de empresas y alcanza una facturación cercana a los 4.000 millones de euros. Sin embargo, defendió que el éxito del sector debe medirse por su capacidad para impulsar la competitividad del resto de la economía. “La situación del hipersector TIC es muy buena”, valoró. “Cuenta con unas quince o veinte empresas tractoras que tiran de él, pero el tejido empresarial gallego está formado, en más de un 90 %, por pymes y autónomos. Mientras que la tecnología no alcance a ese tejido empresarial, seguiremos manteniendo una brecha entre quienes lideran la transformación y los que aún no se benefician de ella”.



En ese proceso, la inteligencia artificial aparece como el gran catalizador. El decano recordó que el 71 % de las empresas TIC gallegas ya utiliza esta tecnología (un 67 % más que hace un año), aunque considera que el verdadero reto comienza ahora. “La IA ya la estamos utilizando quienes trabajamos en el sector tecnológico, pero todavía no se ha incorporado de forma generalizada al resto de las empresas. Ese es el siguiente paso. Será inevitable; quien no lo dé acabará desapareciendo”.

Sánchez Agrelo también analizó el escenario al que se enfrentan los CIO y CISO tanto del ámbito público como del privado. Desde

> “La IA ya la estamos utilizando quienes trabajamos en el sector tecnológico, pero todavía no se ha incorporado de forma generalizada al resto de las empresas”
>
> (Julio Sánchez Agrelo)



su punto de vista, las prioridades son prácticamente comunes: cumplimiento normativo, ciberseguridad y captación de talento. “Compartimos exigencias regulatorias como NIS2 o el Esquema Nacional de Seguridad, y todos tenemos el mismo problema para atraer talento”. La gran diferencia, señaló, está en la capacidad para ejecutar las decisiones. “La empresa privada puede reaccionar con rapidez, mientras que la Administración está condicionada por los procesos de contratación y los plazos administrativos”.

José Manuel Valiño centró su intervención en la aceleración que la inteligencia artificial está imprimiendo a la transformación digital. Incluso sectores tradicionalmente avanzados, como el financiero, todavía tienen recorrido. “La banca es probablemente el sector que más ha invertido en transformación digital y el más competitivo, pero todavía tiene que culminar ese proceso, especialmente en lo que se refiere a la adopción de la inteligencia artificial”.

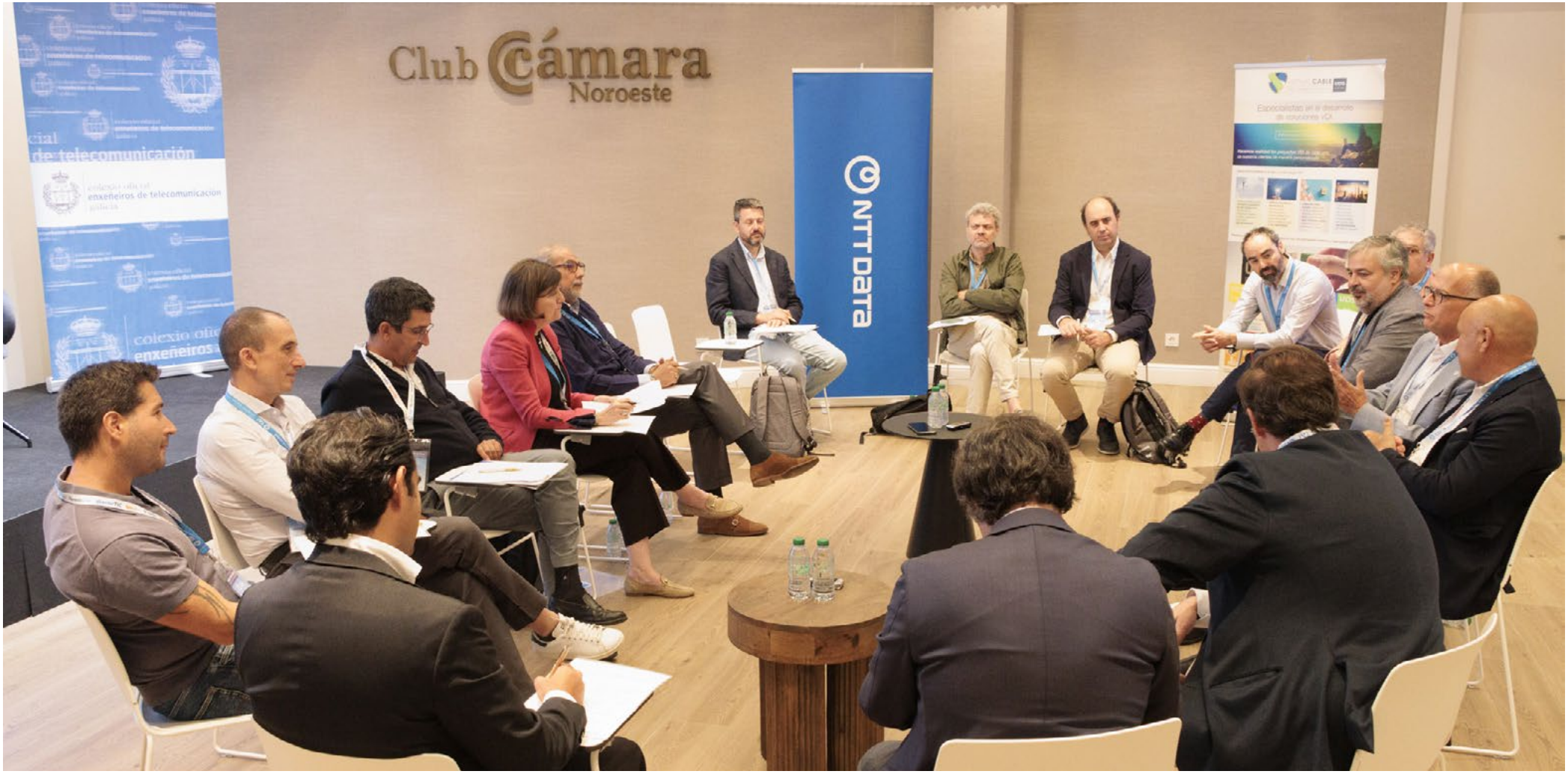
Junto a la IA, situó la resiliencia como la otra gran prioridad estratégica para las organizaciones. “Es una condición necesaria para cualquier organización, independientemente de su tamaño”.

> “La inteligencia artificial es la prioridad número uno, tanto en el ámbito público como privado”
>
> (José Manuel Valiño)

Valiño considera que la IA también obligará a revisar la forma en la que las organizaciones gestionan sus presupuestos tecnológicos. El consumo creciente de modelos de inteligencia artificial introduce un componente de incertidumbre que difícilmente encaja en los ciclos tradicionales de planificación. “Hasta ahora trabajábamos con presupuestos anuales, pero la IA probablemente nos obligará a revisiones semestrales o incluso trimestrales. Igual que apareció el *FinOps* para controlar el gasto en la nube, tendremos que desarrollar un “*TokenOps*” que permita gestionar el consumo asociado a la inteligencia artificial”. En este escenario, advirtió que la Administración pública deberá encontrar mecanismos que le permitan ganar flexibilidad presupuestaria para no quedar rezagada frente a la velocidad de innovación del sector privado.

Como conclusión, el decano de la UIE lanzó un mensaje claro sobre la agenda tecnológica que afrontan los comités de dirección. “La inteligencia artificial es la prioridad número uno. Su impacto alcanza al desarrollo de software, la ciberseguridad, la automatización, la gestión de vulnerabilidades y, en definitiva, a prácticamente todo lo que hacen hoy las organizaciones”.

Innovación, soberanía, IA y seguridad: claves para la transformación digital del poder público gallego



La transformación digital de las organizaciones públicas gallegas ha dejado de centrarse únicamente en la incorporación de nuevas tecnologías para convertirse en un ejercicio de equilibrio entre innovación, cumplimiento normativo y protección de la información. Con la IA como punta de lanza, responsables TIC de la Administración pública, la universidad, la sanidad, la industria y centros tecnológicos gallegos analizaron cómo están evolucionando ámbitos como el puesto de trabajo digital, la ciberseguridad, la inteligencia artificial o el gobierno del dato.

Marilés de Pedro

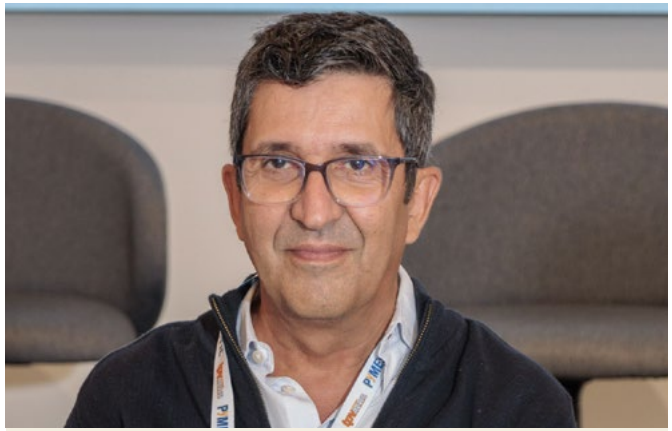
Más allá de las diferencias de enfoque, el encuentro permitió constatar que Galicia dispone de un ecosistema tecnológico especialmente sólido y converge en un mismo objetivo: construir una digitalización sostenible y segura. La soberanía tecnológica, la colaboración entre organismos, la validación continua de los modelos y la atracción de talento aparecen como los pilares sobre los que deberá construirse la próxima fase de la digitalización del sector público gallego.

El puesto de trabajo

Uno de los primeros consensos surgió alrededor de la evolución del puesto de trabajo digital. Ya no se trata únicamente de dotar a los empleados de un ordenador portátil o de facilitar el teletrabajo, sino de proteger un entorno mucho más complejo en el que conviven equipos corporativos, dispositivos móviles, acceso remoto, aplicaciones SaaS y servicios alojados en la nube. Un entorno en el que la seguridad es esencial y en el que muchas organizaciones toman como referencia el Esquema Nacional de Seguridad (ENS).

Emilio Álvarez-Miranda, director de digitalización del Ayuntamiento de La Coruña, explicó que la estrategia del consistorio parte de una premisa clara: todo el modelo debe construirse sobre el cumplimiento del ENS. Para ello, el ayuntamiento ha consolidado su entorno sobre tecnología Microsoft, complementándolo con soluciones específicas para asegurar los accesos remotos. Sin embargo, advirtió de que el ordenador ya no representa el principal foco de riesgo. “Todo el mundo piensa en el puesto de trabajo tradicional, pero los mayores riesgos son los dispositivos móviles y las comunicaciones”, explicó. Por ese motivo, el ayuntamiento cuenta con una capa adicional de seguridad, monitorizando la red, y prepara la implantación de una plataforma MDM que permita incrementar todavía más el control en este entorno.

Una preocupación similar por la seguridad comparte José Carlos Campos, jefe de división de innovación y tecnología de la Autoridad Portuaria de El Ferrol. En su caso, el elevado nivel de exigencia viene determinado por la propia naturaleza de la infraestructura. “Muchos puertos somos infraestructuras críticas y estamos sometidos a auditorías constantes del CCN-CERT”, recordó. Un entorno, absolutamente controlado que, sin embargo, les permitió responder con enorme rapidez durante la pandemia. Gracias a la virtualización del puesto de trabajo pudieron



"Hay que contar con una inteligencia artificial ética"

Javier Taibo, director del **Parque Tecnolóxico de Galicia**

pasar al trabajo remoto prácticamente de un día para otro sin comprometer la seguridad de los sistemas. "Aunque los tiempos de reacción de la Administración pública son más lentos, hay procedimientos de emergencia para responder con eficacia ante situaciones críticas", aseguró. También Javier Taibo, director del Parque Tecnolóxico de Galicia, describió una realidad especialmente compleja. El parque no solo debe proteger sus propios sistemas: también presta servicios de telecomunicaciones a las empresas instaladas en sus instalaciones. "Nuestra seguridad depende también de la seguridad de todas esas empresas", señaló, recordando además que el Centro de Excelencia en Ciberseguridad de Galicia (CECIGA) se ubicará precisamente dentro del parque tecnológico, lo que incrementa todavía más el nivel de exigencia.

También seguridad es un elemento indispensable en el entorno de Navantia. La entidad cuenta con la certificación nivel medio del ENS y se encuentra en proceso de lograr el nivel alto. Antonio Grandal, responsable de transformación digital, remarcó que la ciberseguridad se ha convertido en un factor inseparable de los proyectos de digitalización. "Estamos automatizando procesos industriales y eso significa conectar el mundo OT con el mundo TI. Cada vez que abrimos una puerta entre ambos entornos aparece una nueva superficie de riesgo", afirmó. La convergencia entre tecnologías operacionales y tecnologías de la información obliga, según explicó, a revisar continuamente la arquitectura de seguridad para evitar que la digitalización industrial se convierta en una puerta de entrada para los atacantes.

"Las organizaciones deberían apostar por modelos de IA de menor tamaño ejecutados en infraestructuras propias y entrenados exclusivamente con información interna"

José Carlos Campos, jefe de división de innovación y tecnología de la **Autoridad Portuaria de El Ferrol**

Una realidad diferente, aunque con desafíos similares, es la que describió Javier Laiño, ingeniero de telecomunicación del servicio de innovación de la Corporación de Servicios Audiovisuais de Galicia (CSAG). A diferencia de otras administraciones, la corporación presta un servicio público de difusión masiva, en el que la interacción no siempre se produce de forma individualizada ni resulta fácilmente identificable, lo que añade nuevas complejidades desde el punto de vista de la seguridad y la continuidad del servicio. En este contexto, explicó, conviven dos mundos tecnológicos muy distintos. Por un lado, la infraestructura TI tradicional, alineada con el Esquema Nacional de Seguridad y diseñada para minimizar riesgos y garantizar el funcionamiento de los sistemas corporativos. Por otro, la tecnología operacional que soporta el núcleo de la actividad audiovisual —como los sistemas de producción y emisión—, donde no siempre es posible aplicar los mismos criterios de certificación debido a las particularidades del negocio. “Esa coexistencia obliga a implantar medidas compensatorias, apoyadas en arquitecturas y patrones de seguridad, que permitan mantener protegido un entorno mucho más heterogéneo”, señaló.

> “El Esquema Nacional de Seguridad no debe entenderse como una limitación, sino como una guía que permite adaptar la protección a la realidad de cada organización”

Javier Laiño, ingeniero de telecomunicación del Servicio de Innovación de la **Corporación de Servicios Audiovisuais de Galicia (CSAG)**

Laiño trasladó esa misma reflexión al puesto de trabajo, donde las diferencias funcionales impiden aplicar un modelo único de protección. “No es lo mismo el puesto de un operador de control de realización, que decide en tiempo real qué contenido sale al aire, que el de un empleado que gestiona nóminas o derechos audiovisuales”, explicó. Esa diversidad hace que dentro de una misma organización convivan puestos plenamente alineados con el ENS junto a otros que requieren enfoques específicos, ampliando inevitablemente la superficie de exposición frente a posibles ciberataques.

Pese a ello, rechazó una visión rígida del marco normativo. En su opinión, el Esquema Nacional de Seguridad no debe entenderse como una limitación, sino como una guía que permite adaptar la protección a la realidad de cada organización. “La empresa se certifica allí donde es posible y, allí donde no lo es, aplica buenas prácticas y medidas compensatorias para garantizar que el negocio pueda seguir funcionando con seguridad”.

También hubo referencias a la “libertad” de la que goza el usuario. No solo en este ámbito público, en cualquiera. “Uno de los grandes

> “Los ayuntamientos pequeños necesitan utilizar la IA pero no cuentan con la estructura ni la capacidad para ello”

Javier Fernández, secretario técnico del **Colegio Oficial de Ingenieros de Telecomunicación de Galicia**

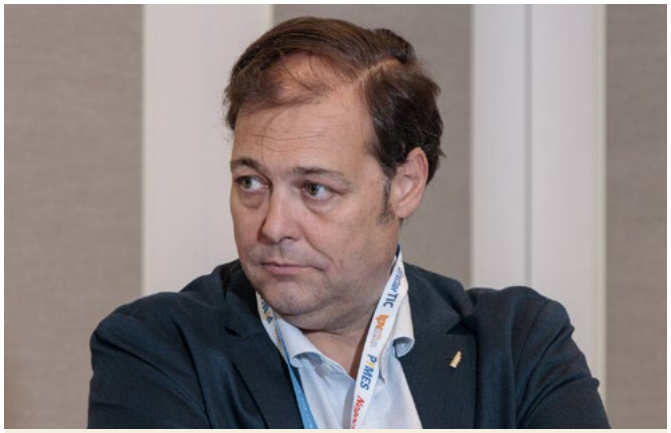
problemas, además de que es un desafío en sí mismo, es que tiene demasiado poder”, alertó Eusebio Nieva, director técnico de Check Point Software para Iberia.

Para “limitarla”, en el caso de Navantia han optado por erradicar casi todas las herramientas locales. “Contamos con auditorías continuas para verificar y desinstalar, detectando cualquier aplicación que puedan usar y que no está autorizada”, relata Antonio Grandal. “La reglamentación nos obliga a estar vigilantes de todas las instalaciones de nuestros equipos”.

Una política similar ha seguido la autoridad portuaria de El Ferrol. “Aunque siempre existe el riesgo de alguna aplicación como una base de datos o un Excel no autorizado”, relata José Carlos Campos. “Mientras que el usuario privado cumple lo que le ordena su superior, el público piensa que no está obligado y no lo hace”.

ENS y NIS2, ¿herramientas estratégicas?

Aunque el Esquema Nacional de Seguridad pueda observarse, por algunas empresas y organismos, como una exigencia administrativa, durante el debate se trasladó que puede convertirse en una herramienta que ayuda a ordenar la transformación digital. Javier Fernández, secretario técnico del Colegio Oficial de Ingenieros de Telecomunicación de Galicia, explicó que su organización logró certificarse



> “No basta con que la IA sea eficaz; también debe ser sostenible”

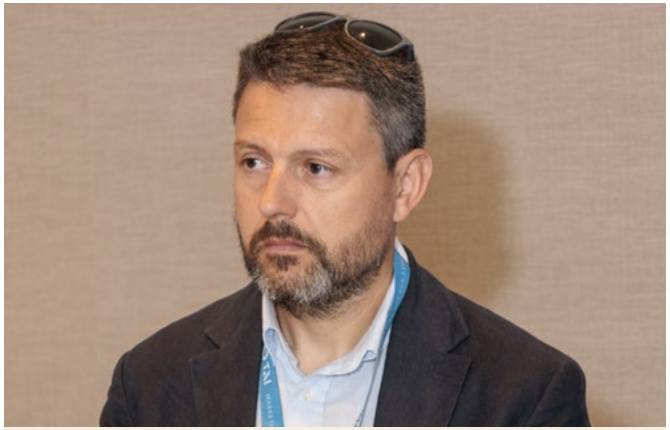
Emilio Álvarez-Miranda, director de digitalización del **Ayuntamiento de A Coruña**

con relativa facilidad debido a su tamaño y al trabajo previo realizado en materia de seguridad. Una introducción que le sirvió para llevar a cabo una reflexión sobre la evolución del ecosistema gallego. A su juicio, mientras la empresa privada dispone de una enorme capacidad de reacción, las administraciones públicas continúan condicionadas por procedimientos

administrativos y presupuestarios que ralentizan muchas decisiones. Aun así, considera que Galicia ha dado pasos muy relevantes gracias al impulso de la Axencia para a Modernización Tecnolóxica de Galicia (Amtega), "a la que se ha dotado de medios y de poder tecnológico", lo que ha permitido avanzar en temas esenciales, "con acciones destacadas en el entorno de la ciberseguridad", valoró.

La conversación también abordó el propio significado del ENS. Fernando Feliu, *executive managing director* de Virtual Cable, explicó que muchas organizaciones hablan de cumplimiento pero hacen uso de soluciones que todavía no cuentan con una certificación oficial, reivindicando que UDS Enterprise, la plataforma de virtualización de la compañía, es la única plenamente certificada por el CCN-CERT para este tipo de entornos.

Más allá del debate tecnológico, Javier Taibo quiso introducir un matiz importante. "El ENS no es un corsé". En su opinión, la certificación no consiste únicamente en utilizar productos que dispongan de un determinado sello, sino en aplicar medidas compensatorias que permitan



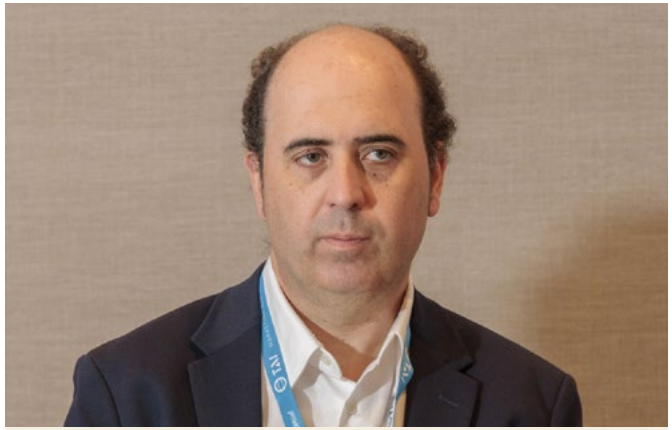
"La inteligencia artificial no entiende de parcelas. Si no colaboramos, nos vamos a quedar atrás"

Óscar Santos,
gerente del **Clúster TIC Galicia**

gestionar adecuadamente los riesgos cuando existen aplicaciones heredadas o sistemas que todavía no cumplen completamente con los requisitos establecidos. La certificación, defendió, debe entenderse como una estrategia integral de gestión del riesgo y no como una simple lista de comprobación tecnológica.

La llegada de la directiva europea NIS2 señala otro reto. Eusebio Nieva recordó que, aunque su transposición aún no se ha completado, las organizaciones que trabajan bajo el Esquema Nacional de Seguridad parten con una ventaja considerable. Sin embargo, advirtió de que la nueva normativa incorpora obligaciones adicionales, como la figura del responsable de seguridad de la información o una mayor implicación de la alta dirección en la gestión de los riesgos. Las organizaciones, sean públicas o privadas, afrontan tres grandes presiones simultáneas. "El incremento de las exigencias regulatorias, la aceleración de los ciberataques y contar con un presupuesto suficiente para aplicar una sólida política de ciberseguridad", enumeró. "La inteligencia artificial está multiplicando la velocidad del ataque", alertó, defendiendo la necesidad de planificar las inversiones pensando en escenarios futuros y no únicamente en las amenazas actuales.

También se recordó que NIS2 obliga a reforzar los programas de formación y concienciación. "La responsabilidad ya no recae únicamente sobre el responsable de seguridad; también alcanza a la dirección de las organizaciones", se-



"Con la llegada de los grandes modelos y de los agentes inteligentes, el reto de la gestión de la IA es mucho mayor"

Juan González, director de seguridad y privacidad del **Centro Tecnológico Gradiant**

ñaló Nieva, calificando este cambio como una de las aportaciones más relevantes de la nueva normativa. "Supone, además, un apoyo importante para conseguir presupuesto y apoyo".

Emilio Álvarez-Miranda abrió otro debate acerca de en quién recae la responsabilidad del cumplimiento. "En la Administración pública nadie se ocupa del *compliance*", alertó. No se trata, continuó, de cumplir solo con las cuestiones relativas a la seguridad. "Debería existir una función transversal de *compliance* que abarque todas las obligaciones regulatorias de la organización pública".

José Carlos Campos añadió otra dificultad propia del ámbito público: la renovación periódica de los equipos directivos. "La dirección puede cambiar cada cuatro años y muchas veces hay que volver a empezar el trabajo de concienciación", explicó.

Por último, Fernando Feliu llamó la atención sobre los sistemas de control. "La gran diferencia entre la empresa privada y la Administración es la dimensión pública de esta última". Mientras la primera observa un entorno más cerrado, los organismos públicos deben dar servicio a terceros, cuidando el acceso y contemplando tareas de observabilidad; "lo que obliga a contar con sistemas de control".

Sin embargo, a pesar de esta compleja realidad, la comunidad gallega es pionera en algunos aspectos. Juan González, director de seguridad y privacidad de Gradiant, recordó que Galicia creó hace más de una década comités de seguridad dentro de la Xunta, implicando tanto a responsables técnicos como a altos cargos de

"La gobernanza del dato consiste en saber dónde está cada dato, quién puede utilizarlo y para qué"

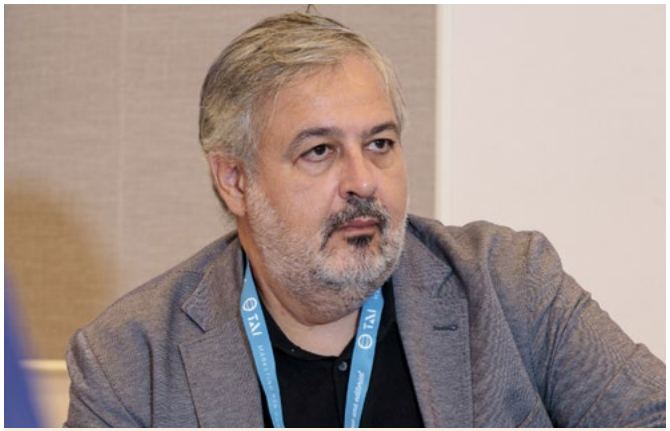
Antonio Grandal, responsable de transformación digital de **Navantia**

las distintas consejerías para reforzar esa cultura de responsabilidad compartida en relación a los datos. Aunque reconoce que hay una gran parte de la Administración pública muy sensibilizada con normas como NIS2 o GDPR, alerta de que en algunos casos el departamento de *compliance* debería estar mucho más cercano a la asesoría jurídica. “Sería muy interesante”.

IA y gobernanza

Si hubo un tema que monopolizó buena parte del debate fue el papel que la inteligencia artificial está llamada a desempeñar en las organizaciones públicas. Una de las conclusiones fue que el verdadero desafío ya no consiste en incorporar herramientas de IA, sino en hacerlo bajo criterios de seguridad, soberanía tecnológica y gobierno del dato.

Una utilización de la IA que es, junto a la gobernanza del dato, el eje principal de la Estrategia Galicia Digital 2030, que ya está siendo aplicada en los organismos públicos gallegos con enfoques diferentes. Mientras algunas entidades están desplegando asistentes internos para automatizar procesos administrativos, otras desarrollan modelos propios para explotar grandes repositorios documentales o mejorar la toma de decisiones mediante analítica predictiva. En todos los casos, el denominador común es el mismo: la inteligencia artificial solo tendrá sentido si trabaja sobre datos fiables, protegidos y correctamente gobernados.



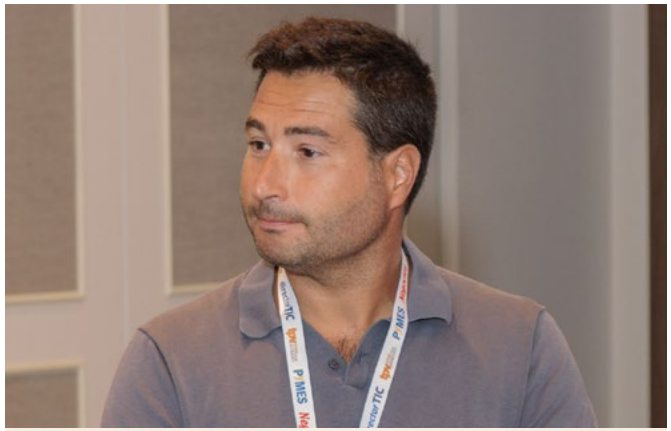
“Estamos asistiendo a una auténtica explosión del *Shadow AI*”

Eusebio Nieva,
director técnico de **Check Point Software** para Iberia

Javier Taibo apeló al concepto “ético” que debe acompañar el uso de la inteligencia artificial. A su juicio, la Administración tiene una responsabilidad añadida respecto al sector privado, ya que cualquier decisión tomada con apoyo de algoritmos debe responder no solo a criterios técnicos, sino también legales y éticos.

El Parque Tecnolóxico está desarrollando herramientas específicas para casos de uso muy concretos, como la identificación de sinergias entre empresas para proyectos europeos o la evaluación de candidaturas en programas de aceleración. La clave, explicó Taibo, es evitar depender de plataformas públicas cuyos criterios de funcionamiento resultan opacos y pueden incorporar sesgos difíciles de detectar. “Tenemos que saber exactamente cómo funciona el algoritmo y garantizar que las decisiones se apoyan en datos objetivos. Si una IA utilizada por la Administración no genera una información veraz, la responsabilidad recae sobre el propio organismo público”, advirtió.

Esa apuesta por desarrollos propios fue compartida por buena parte de los participantes. Antonio Grandal explicó que Navantia está definiendo un marco de trabajo que permita incor-



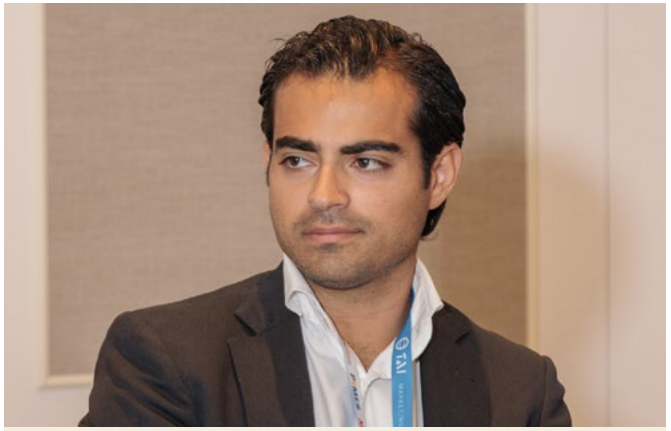
> "La única forma de retener talento en la Administración pasa por ofrecer otros incentivos: estabilidad, conciliación y teletrabajo"

Miguel Fernández,
responsable TIC de la **Universidad de La Coruña**

porar la inteligencia artificial de forma gradual y siempre bajo un estricto control sobre los datos. La prioridad, señaló, pasa por ordenar toda la información corporativa. "La gobernanza del dato consiste en saber dónde está cada dato, quién puede utilizarlo y para qué. Solo cuando eso está resuelto puedes plantearte abrir determinados servicios de IA a los usuarios", explicó. Navantia cuenta con distintos proyectos piloto destinados a mejorar tareas administrativas y procesos internos, siempre mediante modelos desplegados en entornos locales.

Sin dato no hay IA

Si hubo una idea repetida durante toda la conversación fue que no existe inteligencia artificial útil sin una estrategia previa de gestión del dato. José María Ares, jefe del servicio de innovación tecnológica del Ayuntamiento de La Coruña, resumió esa realidad de forma contundente. "La IA es el tema de moda, pero sin datos no hace absolutamente nada". Para el responsable municipal, el trabajo verdaderamente complejo comienza mucho antes del despliegue de cualquier algoritmo. "Es imprescindible conocer qué datos existen dentro de la organización, catalogarlos, identificar su procedencia, garantizar su calidad, controlar su linaje y almacenarlos de forma segura, especialmente en un contexto donde cada vez más aplicaciones funcionan bajo modelos SaaS o arquitecturas híbridas".



> "Ser CIO del sector público es muy complicado"

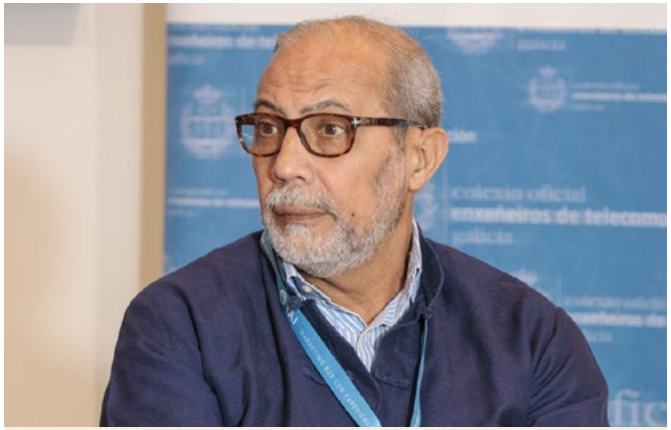
Javier Sánchez,
GTM *practice solutions specialist* de **NTT Data**

José Carlos Campos apostó por el desarrollo de modelos de IA locales. La autoridad portuaria ha prohibido el uso de plataformas públicas de IA generativa con información corporativa y ya trabaja en un ambicioso proyecto de gobierno del dato apoyado sobre tecnologías de código abierto que servirá para entrenar un modelo

propio de inteligencia artificial para garantizar que todas las respuestas estén sustentadas en información verificada.

El responsable portuario defendió que, siempre que sea posible, las organizaciones deberían apostar por modelos de menor tamaño ejecutados en infraestructuras propias y entrenados exclusivamente con información interna. A su juicio, la evolución del hardware está permitiendo que muchas organizaciones puedan ejecutar modelos suficientemente potentes sin depender permanentemente de servicios en la nube. “No necesitamos el modelo más grande del mercado. Lo importante es que esté bien entrenado con nuestros datos y responda exactamente a nuestras necesidades”.

Campos introdujo un concepto, repetido posteriormente durante el encuentro: el del “usuario perezoso”. Uno de los riesgos de la inteligencia artificial, más allá de la tecnología, es la tendencia de algunos profesionales a aceptar automáticamente las respuestas generadas por la IA sin comprobar su veracidad. “Es esencial que por cada dato que suministre haya un agente detrás que compare y controle si ese dato, ese informe o esa contestación es correcta”.

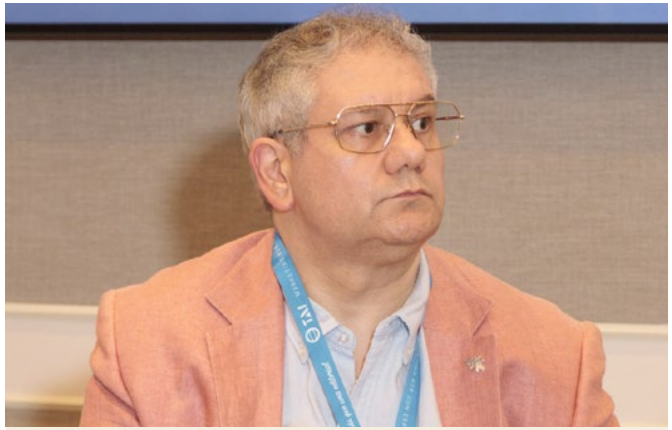


> “Ya no se trata del usuario y cómo accede; también hay que proteger el transporte de la información”
>
> **Fernando Feliu,**
> executive managing director de **Virtual Cable**

Un usuario que busca lo que necesita. Javier Sánchez de la Poza, GTM *practice solutions specialist* de NTT Data, alertó de que es ahí donde comienza la gestión de la seguridad. “Si la organización no pone a disposición una IA suficientemente potente para que el empleado lleve a cabo su labor aparece el riesgo de que recurra a una que no esté regulada y que no sea segura”, relata. “Ser CIO del sector público es muy complicado”.

También se alertó sobre la tecnología en la sombra. Eusebio Nieva advirtió de la rápida evolución desde el conocido *Shadow IT* hacia un nuevo escenario de *Shadow AI*. Si hace unos años el problema consistía en que los empleados instalaban aplicaciones no autorizadas, ahora el riesgo reside en que utilizan herramientas de inteligencia artificial públicas para tratar información corporativa sin ningún tipo de supervisión. “Estamos asistiendo a una auténtica explosión del *Shadow AI*”, afirmó.

El responsable técnico de Check Point Software recordó además que todos los grandes modelos lingüísticos presentan vulnerabilidades inherentes a su diseño. “No existe ningún LLM completamente inmune. La diferencia está en la arquitectura que construyes alrededor del modelo y en las tecnologías que incorporas para



"La medicina personalizada necesita modelos entrenados sobre nuestros propios datos"

Daniel Llamas, subdirector TIC del **área sanitaria da Coruña e CEE (SERGAS)**

detectar ataques, validar respuestas o impedir la extracción de información".

En el caso de Gradiant, el uso de la IA les ha permitido un gran impulso, no solo en el desarrollo de software sino en todas las etapas de I+D, desde redactar estados del arte hasta la preparación de hipótesis. La compañía combina modelos locales con plataformas de IA frontera, dependiendo del tipo de actividad, y trabaja en la implantación de pasarelas de inteligencia artificial (*AI gateways*) capaces de inspeccionar los *prompts* enviados por los usuarios para impedir la fuga de información sensible. Sin embargo, ese potencial, que hay que poner en manos de los investigadores para mantener la competitividad de la compañía, obliga a establecer nuevas salvaguardas. "Antes era mucho más sencillo controlar el uso de la IA. Con la llegada de los grandes modelos y de los agentes inteligentes, el reto es mucho mayor", reconoció Juan González.

Por último, el secretario técnico del Colegio de Ingenieros de Telecomunicaciones de Galicia alertó de la heterogeneidad del ecosistema público gallego que cuenta con velocidades y capacidades distintas. Las grandes y medianas administraciones tienen una gestión, cada vez mejor, del dato pero "los ayuntamientos pequeños también necesitan utilizar la IA y sin embargo no cuentan con la estructura ni la capacidad para ello". Una barrera que el concurso de las diputaciones "puede ayudar a superar", concluyó.

"La IA es el tema de moda, pero sin datos no hace absolutamente nada"

José María Ares, jefe del **Servicio de Innovación Tecnológica del Ayuntamiento de A Coruña**

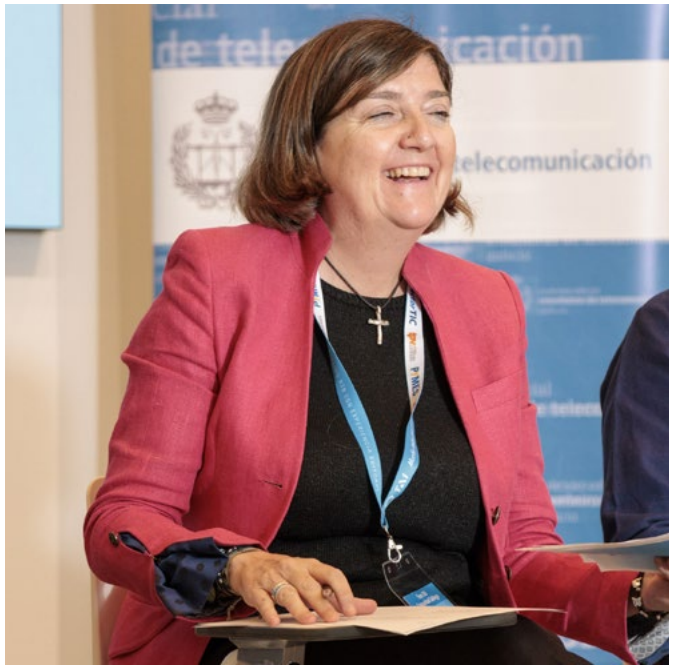
Casos de uso reales

El debate permitió comprobar que la inteligencia artificial ya está abandonando la fase experimental para incorporarse a servicios públicos concretos.

Emilio Álvarez-Miranda explicó que el Ayuntamiento de La Coruña desarrolla asistentes específicos para departamentos como los recursos humanos, mientras regula paralelamente el uso de herramientas generalistas como ChatGPT o Copilot entre sus empleados.

Uno de los casos más destacados es el proyecto de BiciCoruña. El servicio municipal utiliza modelos predictivos para anticipar la demanda y redistribuir automáticamente las bicicletas entre estaciones, optimizando el servicio mediante algoritmos que analizan el comportamiento de cientos de usuarios diarios. La ciudad también trabaja en proyectos de movilidad inteligente, gestión de residuos y seguimiento de incidencias y atención de quejas de los ciudadanos. “En el futuro, para definir estos casos de uso de la IA, deberemos introducir un gobierno de la IA, con un proceso reglado. Por el momento, contamos con un proceso de innovación”, defendió el responsable de digitalización.

Especialmente destacado es el proyecto ALLOCATE (Acelerar el Empoderamiento y Liderazgo Tecnológico Local mediante la Computación Abierta y la IA), centrado en el desarrollo de



algoritmos verdes, éticos y energéticamente sostenibles, que están llevando a cabo junto a la cátedra de Algoritmos Verdes, y en la que también participa el Cluster TIC de Galicia. “No basta con que la IA sea eficaz; también debe ser sostenible”, defendió Álvarez-Miranda, recordando que el crecimiento exponencial de los grandes modelos plantea también importantes desafíos desde el punto de vista energético. “En 2030 el mayor emisor de gases de efecto invernadero va a ser la IA. Tenemos que plantearnos esquemas de desarrollo en los modelos que sean no solamente éticos, sino mucho más sostenibles”.

En un ámbito completamente distinto, Javier Laiño explicó cómo la IA puede transformar la explotación del enorme archivo audiovisual acumulado por la televisión pública gallega desde 1985. Décadas de emisiones de radio y televisión constituyen un patrimonio documental de enorme valor cuya catalogación manual resulta prácticamente imposible. La inteligencia artificial permitirá identificar contenidos, gestionar derechos de explotación y facilitar la reutilización de ese material. “En nuestro caso la gobernanza es complicada porque hay que saber exactamente qué datos proporcionas a cada uno de los sistemas y para qué se usan”. Por ello, la corporación trabaja con pruebas de concepto y, a partir de ellas, ir creciendo.

Miguel Fernández, responsable TIC de la Universidad de A Coruña, recordó que el ámbito universitario presenta un escenario especialmente complejo por la enorme diversidad de usuarios que conviven sobre una misma infraestructura tecnológica. Investigadores, estudiantes y personal docente utilizan nuevas herramientas de

La inteligencia artificial ya está abandonando la fase experimental para incorporarse a servicios públicos concretos

IA, lo que multiplica las posibilidades de innovación, pero también las superficies de exposición y los riesgos para la seguridad de la información. “El principal peligro es que se ataquen los datos desde dentro”, alertó.

La presencia de Virtual Cable en este entorno alcanza al 54 % de las universidades de España. También ha desplegado sus sistemas de virtualización en centros académicos en Europa, Asia o Estados Unidos. “El reto de la ciberseguridad se ha incrementado con el uso de los agentes de inteligencia artificial”, alerta Fernando Feliu. “Las personas desarrollan su propio agente de inteligencia artificial, sin ningún tipo de *compliance*”. También es un desafío la salida de los datos y el transporte de la información. Feliu señaló la encriptación postcuántica como el camino de solución. “Ya no se trata del usuario y cómo accede; también hay que proteger el transporte de la información”.

En el caso de NTT Data cuentan con casos destacados en el ámbito de la salud, un ámbito crítico. “Se utilizan datos de los pacientes en el entrenamiento de inteligencia artificial para mejorar los diagnósticos médicos y diseñar tratamientos personalizados”, explica Javier Sánchez de la Poza. “Una IA que debe ser soberana, diseñada para un uso tecnológico muy solvente y segura”.

La soberanía tecnológica, prioridad estratégica

La irrupción de la inteligencia artificial ha reabierto un debate que ya comenzó con la llegada masiva de la computación en la nube: ¿hasta qué punto las administraciones públicas pueden depender de infraestructuras, plataformas y modelos desarrollados fuera de sus fronteras? Para los participantes, la respuesta pasa por reforzar la soberanía tecnológica, aunque con matices sobre cómo alcanzarla.

Daniel Llamas, subdirector TIC del Área Sanitaria da Coruña e Cee (SERGAS), defendió que la soberanía no puede responder únicamente a una cuestión tecnológica, sino que debe convertirse en una decisión estratégica de las administraciones. “Tiene que pesar más que la inmediatez”. Recordó que, con la adopción de la nube, muchas organizaciones públicas no tomaron decisiones motivadas por una estrategia tecnológica claramente definida, sino por las dificultades que encontraban para contratar o desplegar infraestructuras propias. Ahora, advirtió, existe el riesgo de repetir el mismo error con la inteligencia artificial. “La presión que existe alrededor de la IA generativa es enorme. Los fabricantes han conseguido que cualquier ciudadano utilice estas herramientas todos los días y esa expectativa acaba trasladándose a las organizaciones. Nuestro papel como CIO es explicar que esto no es un proyecto a corto plazo, sino una estrategia que debe construirse para durar muchos años”.

En el ámbito sanitario, esa reflexión adquiere una relevancia especial. Llamas mostró su pre-

ocupación por la creciente dependencia de soluciones desarrolladas por la industria tecnológica y por la dificultad de validar modelos entrenados con datos ajenos a cada organización. Puso como ejemplo los sistemas de ayuda al diagnóstico mediante inteligencia artificial, cuya eficacia suele acreditarse mediante estudios realizados en otros hospitales y sobre poblaciones diferentes. En su opinión, la regulación debería evolucionar hacia modelos de validación continua que permitieran adaptar esos algoritmos a los datos propios de cada centro sanitario. “La medicina personalizada necesita modelos entrenados sobre nuestros propios datos. Lo mismo ocurre en cualquier otro sector”.

La conversación sobre soberanía derivó rápidamente hacia el concepto de IA soberana, una expresión cada vez más presente en el mercado, pero cuyo significado todavía genera interpretaciones diferentes. “Es el nuevo topic”, asegura Javier Sánchez de la Poza, que se pregunta si las empresas que aseguran que cuentan con una IA soberana para implementar en sus clientes, se aseguran de que sus procesos de *data science* y de preparación de los modelos, se hace en un entorno que no es soberano. En el caso de NTT, en los proyectos de segmentos de sectores críticos, que exigen una IA privada y soberana, “nos aseguramos de que sean entornos seguros y que cumplan con esa exigencia soberana gracias a la red de centros de datos propios en Espña”.

Javier Taibo reivindicó el papel, esencial, de la soberanía “más con las realidades geopolíticas que estamos viviendo a nivel mundial”, mostrando una posición clara: cuando los desarrollos se financian con recursos públicos, el resultado debería revertir igualmente en la sociedad. Emilio Álvarez-Miranda señaló que el verdadero reto reside en la falta de transparencia de muchos modelos y, sobre todo, en la enorme complejidad que supone validarlos y afinarlos antes de desplegarlos en producción. “Muchas veces no sabemos exactamente por qué un modelo funciona o deja de funcionar. El entrenamiento y el *fine tuning* siguen siendo procesos muy costosos y poco transparentes”. Además, ad-

virtió de que la apertura total de determinados modelos puede facilitar también la introducción de nuevos sesgos o vulnerabilidades si no existen mecanismos adecuados de supervisión.

Eusebio Nieva coincidió en la importancia de controlar esos sesgos, especialmente cuando la inteligencia artificial mantiene una interacción directa con los ciudadanos. “Una cosa es utilizar un modelo para tareas internas y otra muy distinta utilizarlo para atender al público. En ese caso hay que vigilar no solo los datos que devuelve, sino también los posibles sesgos de sus respuestas”.

José Carlos Campos volvió a introducir un elemento práctico en el debate. A su juicio, un modelo abierto correctamente gobernado y entrenado exclusivamente con información propia reduce enormemente ese riesgo.

El talento sigue siendo el gran reto pendiente

Además de hablar de infraestructuras, algoritmos y regulación, la conversación terminó poniendo el foco en el factor humano. Miguel Fernández resumió uno de los problemas estructurales que afecta a prácticamente todas las administraciones públicas: la dificultad para atraer y, sobre todo, retener profesionales especializados. El sector público, reconoció, difícilmente puede competir con los salarios que ofrece la empresa privada. “La única forma de retener talento pasa por ofrecer otros incentivos: estabilidad, conciliación y teletrabajo”.

> El reto de la ciberseguridad se ha incrementado con el uso de los agentes de inteligencia artificial

La transformación digital no depende únicamente de disponer de mejores herramientas tecnológicas. También requiere profesionales capaces de gobernarlas, comprenderlas y evolucionarlas a medida que cambian las necesidades de las organizaciones.

Y la obligada colaboración

Por último, se dio visibilidad a una idea esencial: ninguna organización podrá afrontar en solitario los retos que plantea la inteligencia artificial. Óscar Santos, gerente del Clúster TIC Galicia, explicó que el ecosistema gallego está intentando evitar esa fragmentación mediante la creación de grupos de trabajo que reúnen a empresas, centros tecnológicos y administraciones para compartir conocimiento y validar nuevos modelos de IA. “En Galicia estamos muy acostumbrados al minifundismo y a defender cada uno su parcela. Pero la inteligencia artificial no entiende de parcelas. Si no colaboramos, nos vamos a quedar atrás”.

Santos señaló que el mismo problema aparece en la gestión de los datos. “No tiene sentido ningún proyecto sin unos *dataset* estructurados de valor”, alertó. Muchas organizaciones consideran que la información que generan constituye un activo exclusivamente propio y muestran reticencias a compartirla, incluso dentro de la misma entidad. “Encontrar el equilibrio entre protección y acceso a los datos es un importante desafío”.

Cómo convertir la tecnología en una ventaja competitiva real

La inteligencia artificial ya no ocupa el centro del debate por sí sola. Las organizaciones empiezan a asumir que su verdadero impacto dependerá de la calidad de los datos, de la transformación de los procesos, de la implicación de las personas y de la capacidad para reforzar la ciberresiliencia. Ese fue el principal mensaje que dejó el Foro TAI Galicia, organizado por TAI Editorial junto a HP|AMD, Samsung, Symantec y Kaspersky, que reunió a responsables de tecnología y ciberseguridad de empresas de sectores tan diversos como la banca, la industria, la energía, la alimentación, los medios de comunicación o el juego para analizar cómo convertir la innovación en una ventaja competitiva real.

Rosalía Arroyo

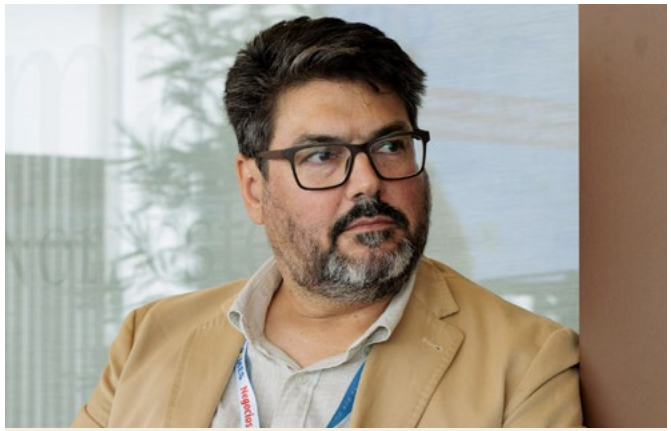
La tecnología ya no se percibe como un elemento de apoyo, sino como un factor que condiciona la competitividad de las organizaciones. Así lo defendió Carlos González Jardón, director de Gobierno y Estrategia IT de Abanca, al asegurar que "no hay área en la que la tecnología no se haya vuelto indispensable". En su opinión, el gran reto ya no consiste en incorporar nuevas herramientas, sino en extender el conocimiento tecnológico a toda la organización y en impulsar una verdadera alfabetización tecnológica para que cualquier área de la empresa entienda tanto las oportunidades como los riesgos que conlleva el uso de estas tecnologías.

En esa misma línea, Javier Cabana, director de Sistemas y Seguridad de Ecoener, explicó que la tecnología ha sido clave para acompañar el crecimiento internacional de la compañía, permitiendo unificar procesos y compartir conocimiento entre equipos distribuidos en distintos países. Sin embargo, advirtió de que el verdadero desafío sigue siendo convertir la enorme cantidad de información que generan las organizaciones en conocimiento útil para el negocio. Reconociendo que "a veces estamos sobreinformados", defendió un mayor esfuerzo en el gobierno del dato para respaldar la toma de decisiones estratégicas.

"La ciberseguridad es una ventaja competitiva", afirmó Ana Salazar, CISO de Hijos de Rivera, recordando que el riesgo ya no depende únicamente de la propia organización, sino también de toda la cadena de suministro. "Que un colaborador tenga un incidente es un problema para la organización", señaló, subrayando que un incidente en un colaborador puede puede acabar afectando a la continuidad del servicio del mismo y, en consecuencia, a la actividad de la empresa.

IA con retorno

Si hubo una idea compartida durante el debate fue que el verdadero reto ya no consiste en hablar de inteligencia artificial, sino en convertirla en una herramienta que aporte valor al negocio. Sin embargo, no todos los participantes la observan desde la misma perspectiva. Miguel Silva Gayoso, director de Sistemas de La Voz de Galicia, reconoció que, en el caso de los medios de comunicación, el auge de los asistentes conversacionales está afectando directamente al tráfico y, por tanto, al modelo de negocio. Más allá de ese impacto negativo, defendió que el principal obstáculo sigue siendo la transforma-



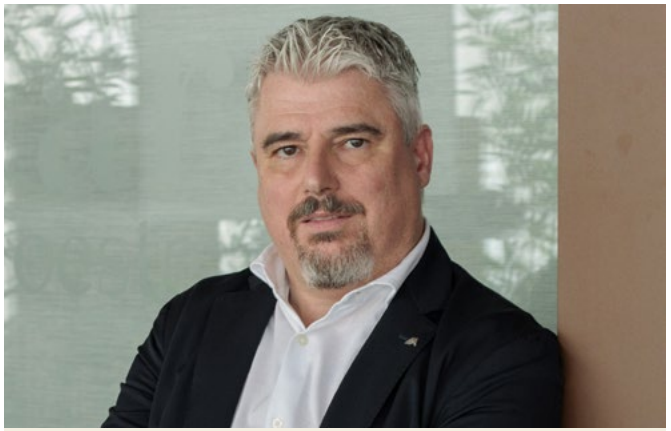
> “Los modelos pequeños y especializados serán los que más valor aporten a las empresas”
>
> **Melchor Sanz,**
> CTO de **HP** Iberia

ción de las organizaciones y aseguró que “la IA no va a sustituir personas, va a sustituir tareas”.

La experiencia de Extrugasa refleja una evolución muy diferente. Gustavo Comparada, director IT de la compañía, reconoció que hace apenas unos años contemplaban esta tecnología con cierto escepticismo, mientras que hoy ya desarrollan proyectos en áreas como marketing, el departamento comercial o la evolución de su ERP. Aun así, insistió en que el éxito depende tanto de la tecnología como de la gobernanza del dato y de la formación de los empleados. “Lo principal es hacer un buen uso de la IA”, afirmó, convencido de que todavía queda mucho trabajo por hacer para que las organizaciones comprendan qué información puede utilizarse y cuál debe permanecer protegida.

Un planteamiento parecido expuso Eneko Lizarralde, técnico del Departamento de TI de Aira S.C.G., aunque desde la realidad de una cooperativa que presta una treintena de servicios a más de 3.000 ganaderos con un reducido equipo tecnológico. “Somos pocos”, aseguró y la IA ya está permitiendo desarrollar aplicaciones que antes resultaban inviables, automatizar procesos que seguían siendo manuales y avanzar en la modernización de su ERP: “sin la IA sería imposible”.

A partir de esas experiencias, Melchor Sanz, CTO de HP Iberia, defendió que una de las grandes tendencias pasa por acercar la inteligencia artificial al lugar donde se generan los datos. Frente a un modelo basado exclusiva-



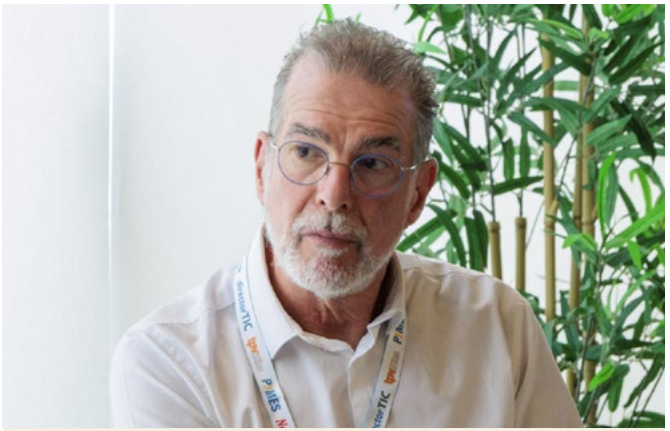
> “La tecnología tiene que dejar de ser un silo para convertirse en una capacidad compartida por toda la organización”
>
> **Carlos González Jardón,**
> director de Gobierno y Estrategia IT de **Abanca**

mente en la nube, explicó que el procesamiento en el propio dispositivo o en el edge permite ganar eficiencia, reducir costes y mantener un mayor control sobre la información. Javier Sanz, Pre Sales Manager de Kaspersky, completó esa reflexión recordando que la tecnología debe ir

acompañada de políticas de uso y de una adecuada concienciación de los usuarios. Cada vez son más las organizaciones que se preguntan cómo proteger la información que comparten con estas herramientas y, en su opinión, “hay que tener en cuenta también la concienciación del trabajo con la IA”, porque el comportamiento de las personas seguirá siendo un elemento decisivo para aprovechar su potencial sin incrementar el riesgo.

IA, privacidad y soberanía del dato

El debate dejó claro que la discusión ya no gira únicamente en torno a dónde ejecutar la inteligencia artificial, sino también a cómo gobernar su uso dentro de las organizaciones. En Hijos de Rivera esa reflexión comenzó hace ya más de un año con la elaboración de una guía corporativa que definía qué herramientas podían utilizar los empleados y en qué condiciones, lo que llevó a revisar los mecanismos tradicionales de seguridad. “Es muy importante que todo esté auditado”, subrayó Ana Salazar, al explicar que la compañía ha incorporado auditorías específicas para modelos de lenguaje y monitoriza el uso de herramientas de IA no autorizadas para detectar aplicaciones que no han sido validadas y reforzar la concienciación de los empleados.



> “Para una organización pequeña, la IA no es un lujo; es una herramienta de supervivencia”
>
> **Eneko Lizarralde,**
> técnico del Departamento de IT de **Aira S.C.G.**

La experiencia de UFD (Grupo Naturgy) apunta en una dirección similar, aunque con un enfoque diferente. Para Iago Crespo, Business Information Security Officer de la compañía, intentar prohibir el uso de la IA suele producir el efecto contrario, por lo que defendió que las organizaciones deben ofrecer herramientas autorizadas que permitan experimentar y aprender con garantías, mientras evolucionan sus procesos para aprovechar realmente el potencial de esta tecnología.

Ese cambio de paradigma también está abriendo un nuevo debate: hasta qué punto conviene depender exclusivamente de servicios de IA en la nube. Iago Crespo explicó que en UFD ya analizan cómo mantener determinadas capacidades cerca del negocio para garantizar la continuidad operativa si esos servicios dejan de estar disponibles. “No sé dónde vamos a estar dentro de dos años, pero ahora estamos en un momento maravilloso”, afirmó, convencido de que la transformación afectará tanto a la tecnología como a los procesos y a la forma de trabajar de las personas.

No todos compartían ese optimismo. Pablo Iglesias Veiga, Security Officer de Luckia Gaming Group, recordó que los modelos generativos actuales no nacieron con la seguridad

"Todas las organizaciones, grandes o pequeñas, necesitan un plan de ciberresiliencia"

Javier Sanz,
Pre Sales Manager de **Kaspersky**

como prioridad, y aludió tanto a los riesgos inherentes de estas herramientas como al crecimiento del shadow AI, que dificulta controlar el uso que hacen los empleados de aplicaciones no autorizadas.

En respuesta, Luckia ha optado por combinar formación, gobernanza, políticas de uso y fomentar el desarrollo de modelos entrenados con el conocimiento de la propia organización ya que, a su juicio, los modelos generalistas "no conocen nuestros negocios". Paradójicamente, añadió, la irrupción de la IA también está teniendo un efecto colateral positivo: obliga a revisar y reforzar la gobernanza del dato, ordenar repositorios y revisar y fortalecer la monito proactiva de su clasificación y de los permisos de acceso.

Carlos González Jardón amplió el foco de la conversación al introducir una cuestión de la que, en su opinión, se habla poco: muchas de las estrategias que hoy se plantean —desde desplegar infraestructura propia hasta acercar el procesamiento al edge— resultan difíciles de asumir para la inmensa mayoría de las empresas españolas, especialmente para las pymes. Asegurando que "la IA es imprescindible en cualquier organización", recordó que esa adopción debe ir acompañada de alfabetización tecnológica, una adecuada gobernanza del dato y una reflexión realista sobre los costes, la infraestructura y la capacidad de cada organización para incorporar estas tecnologías de forma sostenible.

"La tecnología solo tiene sentido cuando acelera realmente el negocio"

Javier Cabana,
director de Sistemas y Seguridad de **Ecoener**

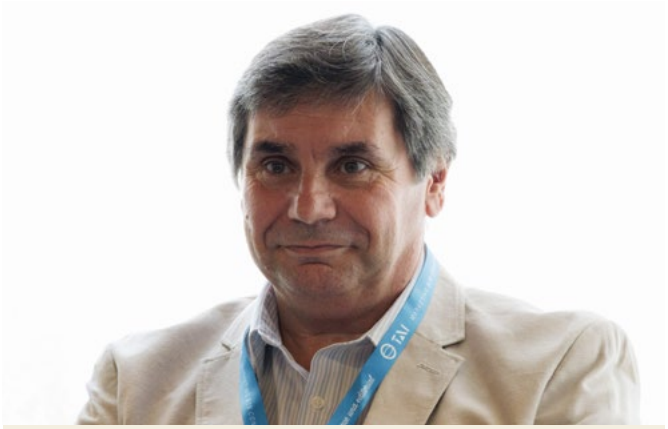
Jorge Chamizo, New Models Pre-Sales de Symantec & Carbon Black, coincidió en que el desafío consiste en encontrar el equilibrio entre innovación y protección. En su opinión, las organizaciones deben decidir hasta dónde quieren automatizar sus procesos sin perder el control de la información. Existen tecnologías capaces de proteger los datos incluso cuando

abandonan el perímetro corporativo, pero insistió en que ninguna solución será suficiente si los usuarios no entienden cómo utilizarla. “Lo más difícil de la concienciación y de la formación es que realmente le importe al empleado y que lo incorpore a sus tareas diarias” señaló.

Melchor Sanz, cerró el bloque cuestionando otra de las ideas más extendidas en torno a la IA: la necesidad de recurrir siempre a grandes modelos alojados en la nube. “Olvidémonos un poco de la moda de la inteligencia artificial generalista y utilicemos la inteligencia artificial en el negocio”, propuso, explicando que, en muchos casos, organizaciones obtendrán mejores resultados con modelos más pequeños, entrenados para resolver problemas concretos y capaces de ejecutarse sobre infraestructuras propias. “Seguramente sea un modelo mucho más pequeño, pero muy preciso y muy adecuado a su negocio”, concluyó, convencido de que ese enfoque permitirá ganar precisión, controlar mejor la información y contener los costes.

Industria y operaciones

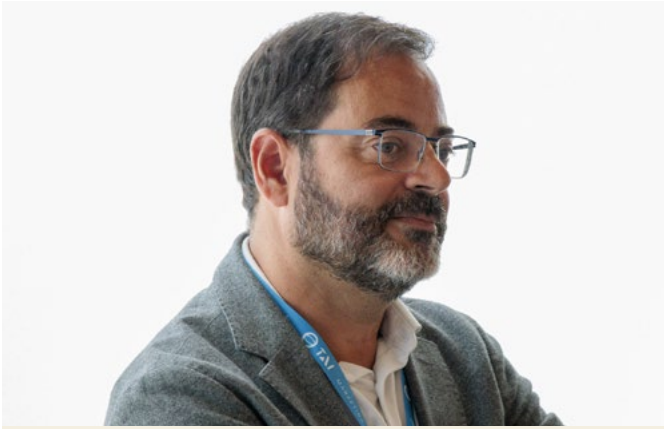
La conversación se trasladó después al ámbito industrial, donde los participantes coincidieron en que todavía existe un amplio margen para ganar eficiencia mediante la digitalización de las operaciones. “La cadena de suministro para nosotros es importante; también la parte logística y la producción, porque va toda en cadena”, aseguró durante su intervención Eneko Lizarralde. Más allá de los grandes proyectos de transformación, destacó el impacto que tiene digitalizar procesos cotidianos como la gestión de pedidos de última hora, la planificación de rutas o la coordinación de la información procedente de las explotaciones. Ese trabajo, explicó, ya se está ampliando al ámbito del mantenimiento predictivo.



> “La formación de los usuarios será tan importante como la implantación de la IA”
>
> **Gustavo Comparada,** director IT de **Extrugasa**

Una realidad muy similar describió Gustavo Comparada. Reconociendo que determinados procesos industriales seguirán siendo manuales, defendió que todavía existe un amplio recorrido para automatizar tareas que aporten mayor eficiencia a la planta. “Todo lo que podamos digitalizar y todo lo que podamos tener operativamente más cómodo para el operario, lo vamos a realizar”, aseguró.

La importancia de adaptar la tecnología a la realidad de cada organización también fue uno de los mensajes de Javier Cabana. En un sector donde las inversiones en infraestructuras se planifican a muy largo plazo, recordó que la rápida evolución tecnológica obliga a convivir con activos que pueden quedar obsoletos mucho antes de finalizar su vida útil. Por ello, situó la gestión del mantenimiento y de las operaciones entre las áreas con mayor potencial de



> “Muchas veces una pequeña mejora digital aporta más valor que un gran proyecto de IA”
>
> **Carlos Gándara,**
> Head of B2B de **Samsung** España

mejora, aunque advirtió de que “cada empresa es un mundo” y debe identificar aquellos casos de uso capaces de generar un retorno tangible para el negocio.

A partir de esas experiencias, el debate derivó hacia el papel que debe desempeñar la inteligencia artificial dentro de la industria. Carlos Gándara, Head of B2B de Samsung España, defendió que “todavía falta mucho por digitalizar”, recordando que numerosas empresas siguen dependiendo del papel o de procesos que aún no han completado su transformación digital. En su opinión, la prioridad debe estar en incorporar inteligencia allí donde aporte valor inmediato al negocio; “digitalizar primero y luego ya pensaremos en lo que hacemos con la IA”, resumió.

Esa visión fue compartida por Melchor Sanz, quien defendió que los mayores beneficios llegarán de modelos pequeños y especializados, diseñados para resolver necesidades muy concretas. Citó ejemplos ligados a la logística, la gestión de flotas o la optimización de rutas al tiempo que se mostraba mucho más prudente respecto al uso generalizado de herramientas como ChatGPT en el ámbito empresarial.

El dato

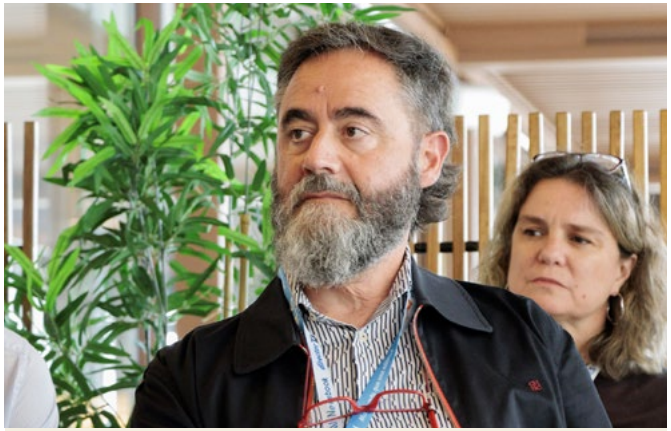
La conversación se desplazó después hacia el verdadero combustible de la inteligencia artificial: los datos. Para Santiago Ramón Paz, jefe de Infraestructura TIC y Ciberseguridad de La

> “Los procedimientos tienen que servir para responder a un incidente, no para aprobar una auditoría”
>
> **Ana Salazar,**
> CISO de **Hijos de Rivera**

Voz de Galicia, el principal problema no es la falta de información, sino la dificultad para convertirla en un activo útil para el negocio. “Los datos existen y lo que falta es confianza, resumió, añadiendo que muchas organizaciones si-

guen conviviendo con información dispersa en distintos sistemas y repositorios, lo que dificulta su explotación. Antes de pensar en inteligencia artificial, defendió, es necesario clasificar los datos, etiquetarlos correctamente y definir qué información resulta realmente relevante para cada área de negocio. Sólo así podrá analizarse con las garantías necesarias y manteniendo el control sobre su confidencialidad. Además, recordó que el negocio debe implicarse en todo el proceso. "TI no puede trabajar por trabajar"; el dato sólo adquiere valor cuando ayuda a tomar mejores decisiones.

Esa necesidad de combinar gobierno del dato y ciberseguridad también fue destacada por Ana Salazar, quien explicó que la evolución de las plataformas de datos en la compañía ha ido acompañada de revisiones continuas para garantizar que la información permanezca protegida. Además, señaló que el análisis de la telemetría generada por las herramientas de seguridad está permitiendo detectar comportamientos de riesgo, como la instalación de aplicaciones no autorizadas, reforzando así la protección de la organización avanzando hacia análisis theat hunting.



"La continuidad del negocio debe formar parte de la cultura de la organización"

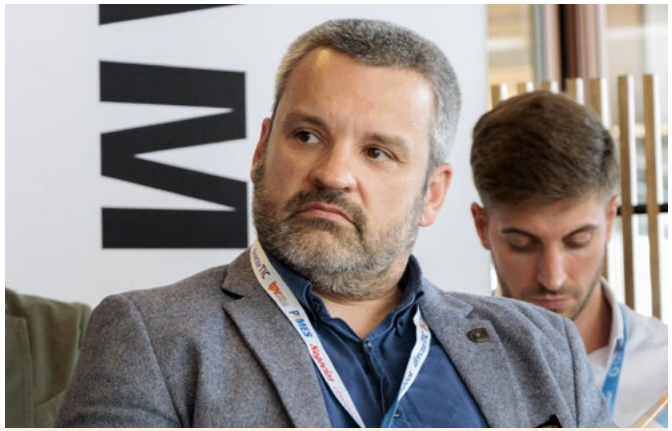
Santiago Ramón Paz, jefe de Infraestructura TIC y Ciberseguridad de **La Voz de Galicia**

La misma idea fue desarrollada por Iago Crespo, quien situó el gobierno del dato como el punto de partida de cualquier estrategia de analítica o inteligencia artificial. "La base está en tener un buen gobierno del dato", afirmó, insistiendo en la necesidad de conocer quién es responsable de cada conjunto de información, dónde se almacena y cómo circula por la organización.

A partir de esa base, explicó, resulta mucho más sencillo obtener valor mediante la analítica avanzada y la IA. Como ejemplo, citó los proyectos que UFD desarrolla para detectar el fraude en la red de distribución eléctrica. "Con buenos datos, bien gobernados, la IA nos está ayudando muchísimo a ser mucho más eficientes", aseguró.

Las intervenciones de los responsables de TI dieron pie a las aportaciones de los patrocinadores. Jorge Chamizo defendió que el gobierno del dato comienza mucho antes de incorporar inteligencia artificial. En su experiencia, muchas organizaciones todavía tienen dificultades para identificar y clasificar correctamente su información, un paso imprescindible para protegerla y extraer valor de ella. "El etiquetado de la información me parece especialmente importante", subrayó, apostando por analizar los procesos desde la perspectiva del usuario y no únicamente desde la tecnología, un enfoque que permite aplicar políticas de protección más precisas sin penalizar la experiencia de uso.

Por su parte, Carlos Gándara, Head of B2B de Samsung España, puso el foco en otro aspecto



"La gran preocupación actual es la gran asimetría que está introduciendo la IA entre atacantes y defensores donde las vulnerabilidades se descubren y explotan en horas"

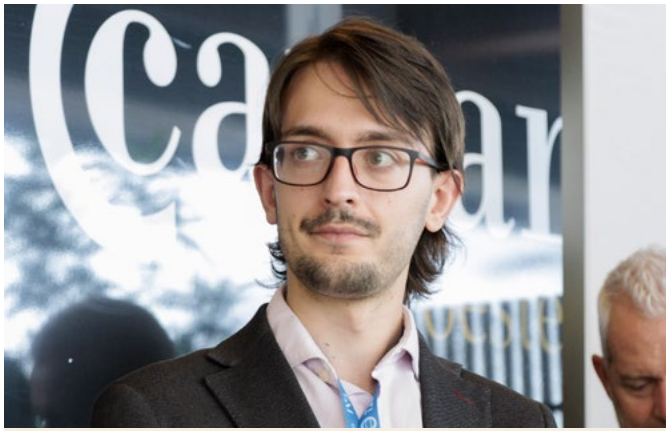
Pablo Iglesias Veiga,
Security Officer de **Luckia Gaming Group**

cada vez más relevante: la necesidad de que las organizaciones puedan decidir qué herramientas de inteligencia artificial están autorizadas a utilizar sus empleados desde los dispositivos corporativos. A su juicio, disponer de mecanismos de control y políticas de uso claras resulta fundamental para mantener el gobierno de la información y evitar que datos sensibles acaben siendo utilizados por aplicaciones no autorizadas.

Ciberresiliencia

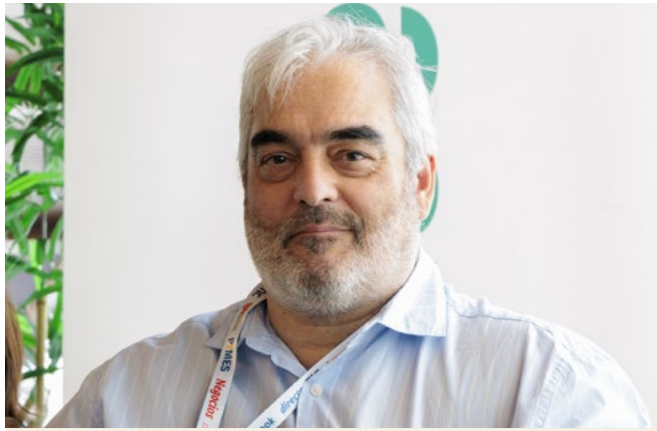
El debate se desplazó después hacia la ciberresiliencia, un concepto que los participantes desvincularon del mero cumplimiento normativo. Ana Salazar defendió que garantizar la continuidad del negocio es una responsabilidad compartida y no exclusiva del área de ciberseguridad. Incidió en que "la ciberseguridad somos toda la empresa", recordando que existen otro tipo de incidentes como un apagón eléctrico capaces de paralizar la actividad sin que medie un ciberataque.

Con esa filosofía, explicó, la compañía ha tomado como referencia marcos como ISO 27001 para avanzar hacia los requisitos que previsiblemente impondrá NIS2, aunque dejó claro que el objetivo va mucho más allá de superar una auditoría. "No por cumplir, sino para que podamos usar los controles de forma real", afirmó. Esa misma visión la aplica a los procedimientos internos: documentos sencillos, revisados periódicamente y útiles cuando realmente hacen falta; "que sean procedimientos que te valgan para que cuando venga un ataque los puedas utilizar de verdad", concluyó.



"El gobierno del dato empieza mucho antes de aplicar inteligencia artificial"

Jorge Chamizo,
New Models Pre-Sales de **Symantec & Carbon Black**



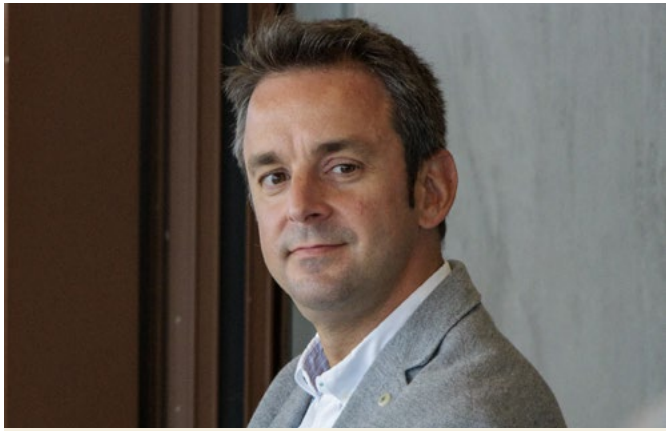
> “La IA no va a sustituir personas; va a sustituir tareas”

Miguel Silva Gayoso,
director de Sistemas de **La Voz de Galicia**

Una preocupación compartida por Pablo Iglesias Veiga, aunque desde otra perspectiva. En un sector especialmente regulado, explicó, proteger la información, garantizar la continuidad del negocio y cumplir con la normativa forman parte de una misma realidad. Sin embargo, considera que el mayor desafío es la creciente asimetría entre atacantes y defensores, agravada porque el tiempo disponible para reaccionar se ha reducido drásticamente. Si antes podían transcurrir semanas o meses entre el descubrimiento de una vulnerabilidad y la aparición de un exploit, ahora ese margen puede medirse en horas. “¿Están los negocios preparados para eso?”, planteó. A su entender, esta nueva realidad obligará a replantear los procesos internos para validar y desplegar correcciones con la misma rapidez con la que evolucionan las amenazas y con el riesgo de no poder ser tan rigurosos en los procesos de gestión del cambio.

Santiago Ramón Paz compartió ese diagnóstico y fue un paso más allá. “El paradigma ha cambiado”, afirmó, convencido de que negocio y tecnología tendrán que actuar de forma mucho más coordinada porque los tiempos de respuesta ya no admiten los ritmos tradicionales.

En el caso de La Voz de Galicia, la cultura de resiliencia forma parte del ADN de la empresa. El diario lleva cerca de 140 años publicándose de forma ininterrumpida y el apagón eléctrico vivido recientemente volvió a ponerlo a prueba: “fuimos el único medio gallego que sacó el periódico en papel”, destacó, convencido de que



> “Estamos viviendo un momento único para transformar la forma de trabajar”

Iago Crespo, Business Information Security Officer de **UFD (Grupo Naturgy)**

cuando la continuidad del negocio y la protección de la información forman parte de la cultura de una organización, el cumplimiento de normativas como NIS2 “va de la mano”.

Esa evolución también la destacó Javier Sanz, de Kaspresky, quien diferenció entre resiliencia y ciberresiliencia para defender que las organi-

zaciones ya no pueden limitarse a reforzar las medidas preventivas. Durante años, explicó, la prioridad fue impedir los ataques mediante nuevas herramientas de seguridad; hoy el reto consiste en asumir que, tarde o temprano, "van a ser víctimas de un ataque" y prepararse para responder y recuperarse con rapidez.

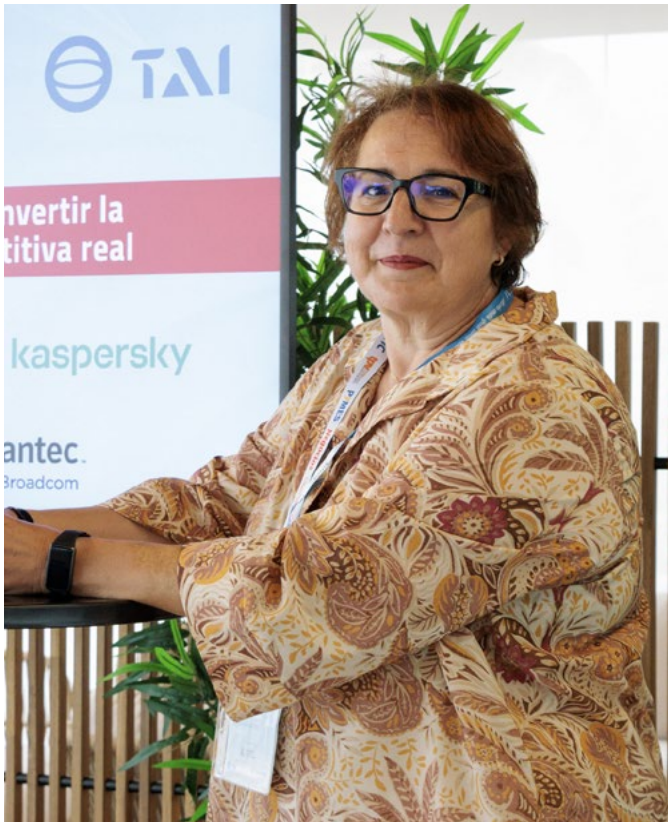
A su juicio, ese cambio de enfoque está modificando igualmente el papel de los responsables de ciberseguridad dentro de las organizaciones. Cada vez es más habitual que participen desde el inicio de los proyectos y no únicamente al final, cuando la seguridad se incorporaba "como un parche en el último momento". Sin embargo, advirtió de otro riesgo: responder a cada incidente incorporando nuevas soluciones sin contar con el conocimiento necesario para gestionarlas. "Hay que tener cuidado con la tecnología por la tecnología", señaló, recordando que una herramienta mal utilizada puede terminar generando nuevas brechas de seguridad.

Como broche final, Carlos Gándara recordó que buena parte del tejido empresarial todavía tiene un amplio recorrido en materia de digitalización.

> La inteligencia artificial ya no es el reto; el verdadero desafío es transformar procesos, personas y datos

En muchas pymes, explicó, avances aparentemente sencillos, como implantar un ERP, digitalizar la gestión documental o permitir que un cliente solicite una cita desde el móvil, pueden aportar un impacto mucho mayor que la incorporación de tecnologías más sofisticadas. "Aquí estamos ya en la IA, pero todavía queda mucho para llegar ahí", resumió.

Miguel Silva Gayoso cerró el intercambio con una reflexión que sirvió para sintetizar buena parte de las ideas surgidas durante el debate: digitalizar no consiste únicamente en incorporar nuevas herramientas, sino en replantear la forma de trabajar. Como ejemplo, recordó que todavía existen organizaciones donde procesos tan cotidianos como la aprobación de hojas de gasto siguen dependiendo del papel. Una muestra de que, antes de hablar de inteligencia



artificial, muchas empresas aún tienen margen para simplificar y modernizar sus procesos.

El gran reto tecnológico para los próximos doce meses

Al pedir a los participantes que resumieran en una única prioridad el principal reto tecnológico para el próximo año, las respuestas dibujaron un denominador común: la inteligencia artificial

ya no se percibe como un proyecto aislado, sino como un elemento que deberá integrarse en toda la organización, acompañado de una mejor gestión del dato, más automatización y un importante esfuerzo de cambio cultural.

Para Iago Crespo, el desafío consiste en extender el uso de la IA a todos los procesos de la organización y evitar que la transformación avance a velocidades diferentes. En su opinión, no basta con acelerar determinadas tareas; también es necesario que la propia organización utilice esa tecnología para supervisar y controlar esos nuevos procesos.

Asegurando que disponer de mayor visibilidad será clave para responder a un escenario de amenazas cada vez más dinámico, Pablo Iglesias Veiga situó la prioridad en mejorar la observabilidad, la monitorización y la automatización de la respuesta a los eventos de ciberseguridad

Para Santiago Ramón Paz el gran reto pasa por trasladar la cultura tecnológica al conjunto de la organización. A su juicio, muchos profesionales siguen percibiendo los controles asociados al gobierno del dato, las normas o los marcos de seguridad como una carga administrativa, sin comprender que su objetivo real es proteger la continuidad del negocio.

> La gobernanza del dato, la ciberresiliencia y el cambio cultural marcarán la agenda tecnológica de los próximos años

Esa transformación cultural también centró la intervención de Miguel Silva Gayoso, que explicó que uno de los principales proyectos de La Voz de Galicia será culminar la transición hacia un modelo digital first, un cambio que obligará a modificar la forma de trabajar de una redacción acostumbrada durante décadas a priorizar la edición impresa.

En Hijos de Rivera, Ana Salazar situó el foco en la implantación de la IA generativa en todos los procesos de la compañía, sin perder de vista la necesidad de reforzar al mismo tiempo las inversiones en ciberseguridad para acompañar esa transformación.

Por su parte, Gustavo Comparada volvió a poner el acento en las personas. Aunque considera imprescindible avanzar tanto en inteligencia artificial como en ciberseguridad, cree que el mayor reto sigue siendo formar a los usuarios y mejorar su concienciación.

En Ecoener, Javier Cabana destacó que la IA ya condiciona prácticamente todos los ámbitos de la organización, desde la productividad individual hasta la transformación del negocio. No obstante, reconoció que su prioridad inmediata sigue siendo reforzar el gobierno del dato para descubrir y clasificar información todavía todavía no inventariada o sin clasificar.

Finalmente, Eneko Lizarralde cerró el turno insistiendo en que el verdadero reto continúa siendo humano. La tecnología seguirá evolucionando, explicó, pero sólo generará valor si las personas comprenden cómo utilizarla y si las organizaciones consiguen construir una cultura basada en el dato y en el aprendizaje continuo.

Cierre

Como cierre del encuentro, los patrocinadores resumieron cómo están abordando los retos

que las organizaciones plantearon durante el debate. Más allá de las tecnologías concretas, todos coincidieron en la necesidad de adaptar las soluciones al grado de madurez de cada empresa y acompañar esa evolución con servicios de apoyo y asesoramiento.

Desde Kaspersky, Javier Sanz recordó que el tejido empresarial gallego está formado mayoritariamente por pymes con necesidades muy distintas a las de las grandes corporaciones. Explicó que, mientras las organizaciones más maduras ya preguntan por protección de la inteligencia artificial o cifrado poscuántico, muchas empresas medianas están dando ahora sus primeros pasos en ámbitos como EDR, MDR o NIS2. En cualquier caso, defendió que todas comparten una misma necesidad: fortalecer su ciberresiliencia. “Todas, grandes y pequeñas, necesitan un plan de resiliencia”, resumió.

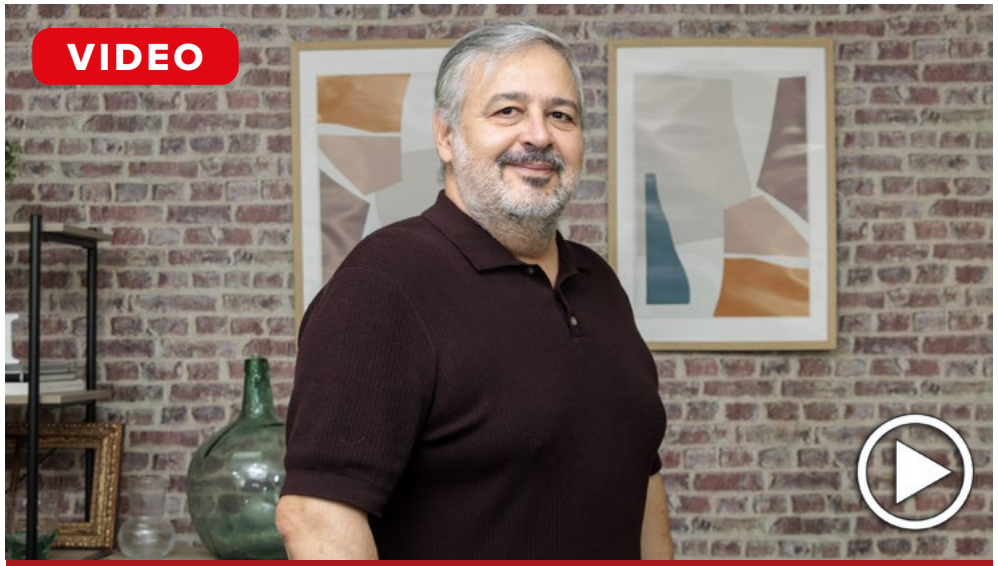
Carlos Gándara, Head of B2B de Samsung España, insistió en la importancia de construir un ecosistema conectado y seguro en torno al puesto de trabajo. Recordó que la compañía trabaja para que todos sus dispositivos puedan gestionarse de forma integrada y destacó el papel de Samsung Knox como plataforma para reforzar la administración y la seguridad de los entornos corporativos. “Estamos aquí para ayudaros a sacar partido tanto a la gestión como a la seguridad”, señaló.

Por su parte, Jorge Chamizo, New Models Pre-Sales de Symantec & Carbon Black, explicó que la estrategia de la compañía pasa por ofrecer una protección unificada de la información, independientemente de que las organizaciones trabajen en entornos cloud, on-premise o híbridos. Tras integrar las distintas tecnologías de seguridad bajo una misma plataforma, defendió que esa visión permite abordar proyectos relacionados con la protección del dato, las identidades, la red o los puestos de trabajo desde un enfoque común. “Retadnos con los problemas que tenéis”, invitó a los asistentes.

Finalmente, Melchor Sanz, CTO de HP Iberia, recordó que la seguridad comienza mucho antes del software y defendió la importancia de proteger toda la cadena de suministro, empezando por el propio dispositivo. En su intervención subrayó que el hardware constituye la primera capa de confianza sobre la que se construye el resto de la estrategia de ciberseguridad y destacó la incorporación de capacidades de observabilidad y protección poscuántica en los equipos de la compañía para reforzar esa visión de seguridad desde el origen.

Check Point Software apuesta por una ciberseguridad inteligente para proteger la transformación digital de la AA.PP.

La inteligencia artificial está revolucionando la forma de trabajar de las administraciones públicas, pero también está abriendo la puerta a nuevas amenazas de ciberseguridad, por lo que desde Check Point Software consideran imprescindible reforzar la protección de datos, identidades y accesos a medida que las organizaciones incorporan agentes de IA y automatizan procesos. La compañía apuesta por un modelo de seguridad basado en zero trust, el cifrado de la información y la automatización inteligente de las políticas de protección. Eusebio Nieva, *sales engineering manager Iberia* de Check Point Software, analiza todos estos retos.



Eusebio Nieva, *sales engineering manager Iberia* de **Check Point Software**

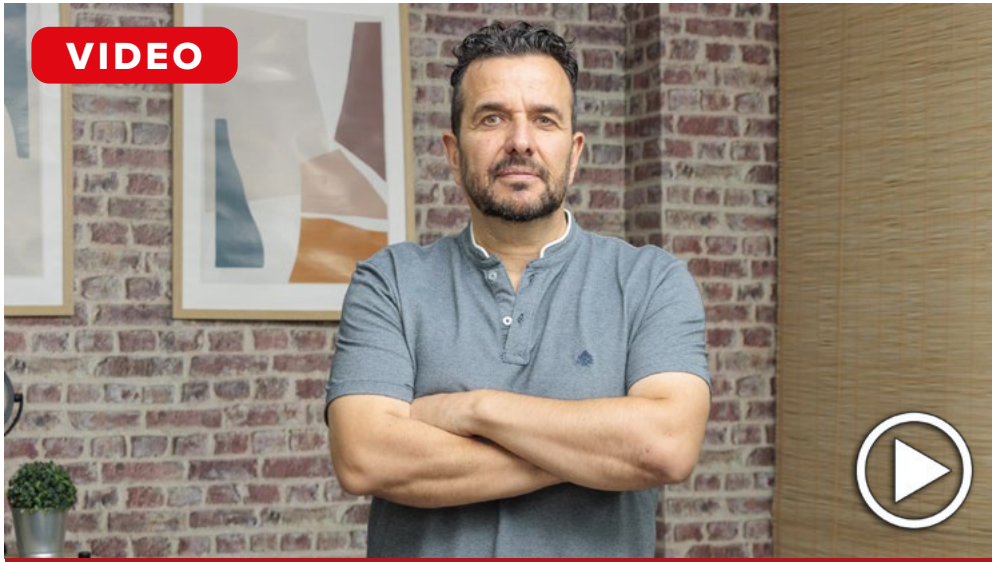
CHECK POINT™

Kaspersky: “La seguridad tiene que avanzar al mismo ritmo que la transformación digital”

La aceleración de la transformación digital está obligando a las organizaciones a replantear su estrategia de ciberseguridad. Para Javier Sanz, Pre Sales Manager de Kaspersky, la innovación solo tendrá sentido si la protección avanza al mismo ritmo. “La seguridad tiene que ir de la mano de ese avance tecnológico”, afirma.

Aunque el ransomware sigue siendo la principal amenaza, advierte de que la inteligencia artificial está acelerando la evolución de los ataques y reduciendo el tiempo necesario para desarrollarlos. En este escenario las empresas deben asumir que, antes o después, sufrirán un incidente y prepararse para recuperar su actividad con rapidez. Esa filosofía da sentido a conceptos como la ciberresiliencia y la ciberinmunidad, una aproximación que busca reducir la superficie de ataque desde el diseño de los sistemas.

Sostiene que la ciberseguridad se ha convertido en un elemento de confianza y competitividad, tanto en la relación con los clientes como dentro de la cadena de suministro.



Javier Sanz, Pre Sales Manager, **Kaspersky**

kaspersky

NTT DATA acompaña a la Administración pública en todo su ciclo de vida

Tras dos décadas de presencia en Galicia, NTT DATA considera que la comunidad se ha consolidado como un polo tecnológico de referencia tanto para el ámbito empresarial como para la Administración pública. La compañía acompaña a las organizaciones durante todo su proceso de transformación digital, desde la definición de la estrategia hasta la puesta en marcha y evolución de los proyectos. Javier Sánchez de la Poza, GTM practice solutions specialist de la compañía señala que la inteligencia artificial, la gobernanza del dato y el cumplimiento de la normativa europea son algunos de los ejes sobre los que basa su propuesta de valor.

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

Samsung: “Si conseguimos conectar personas, procesos y la herramienta está bien escogida, la transformación funciona”

La inteligencia artificial está devolviendo protagonismo a los dispositivos desde los que los profesionales acceden a la información y a los procesos de negocio. Para Carlos Gándara, Head of B2B de Samsung España, móviles, tabletas y PCs se han convertido en la puerta de entrada a la IA generativa y, próximamente, a la IA agéntica. Sin embargo, advierte de que la transformación digital no consiste en incorporar más herramientas, sino en conectar personas, procesos y tecnología de forma coherente.

El directivo defiende que las organizaciones deben identificar primero qué procesos merece la pena digitalizar y aplicar la inteligencia artificial solo allí donde aporte un beneficio real. También destaca el papel de la movilidad en sectores como la logística, la sanidad o la industria, donde los dispositivos inteligentes ya están transformando la operativa diaria. En paralelo, subraya que la seguridad debe acompañar todo el proceso para garantizar la protección de los datos.

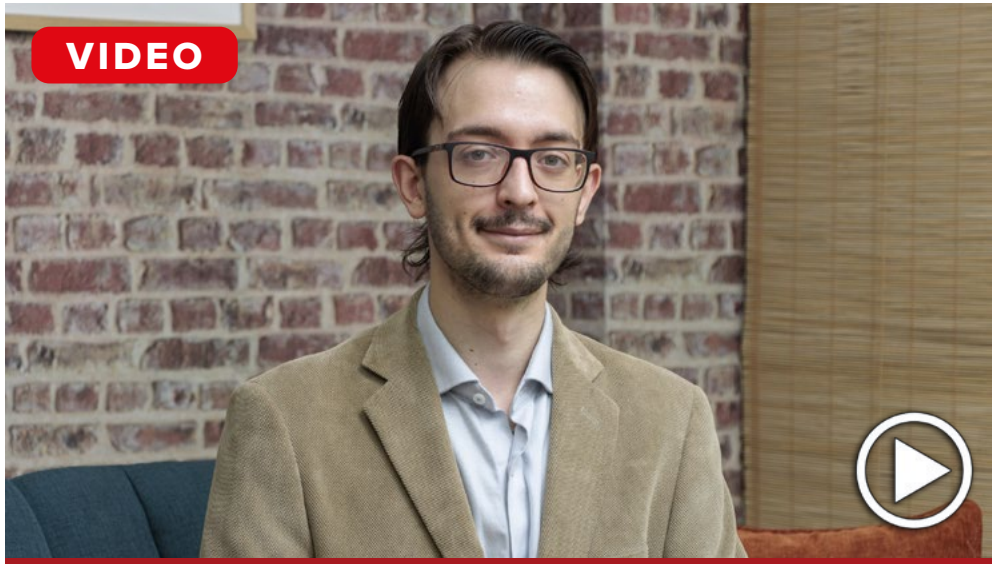
Carlos Gándara, Head of B2B de **Samsung** España

SAMSUNG

Symantec: “El reto ya no es proteger el endpoint, sino controlar el dato”

La inteligencia artificial está obligando a las organizaciones a replantear la forma en que protegen su activo más valioso: el dato. Para Jorge Chamizo, New Models Pre-Sales de Symantec & Carbon Black, muchas empresas siguen centrando sus esfuerzos en el endpoint cuando el verdadero reto es conocer dónde reside la información, quién accede a ella y cómo se utiliza. “Los clientes se centran en el canal del endpoint” sin definir un marco de riesgo para todos los canales, advierte.

Chamizo identifica el Shadow AI como uno de los principales riesgos actuales, mientras que la IA agéntica exigirá controlar asistentes capaces de interactuar con bases de datos y APIs. Ante este escenario, defiende analizar la información allí donde reside, en lugar de trasladarla a plataformas externas, y evolucionar tecnologías como DLP y DSPM para aplicar políticas homogéneas de seguridad. A su juicio, el gran desafío será encontrar el equilibrio entre automatización, productividad y riesgo, sin perder el control sobre el dato.



Jorge Chamizo, New Models Pre-Sales de **Symantec & Carbon Black**

Symantec™ by Broadcom

Virtualización inteligente para impulsar una AA.PP. más segura y eficiente con Virtual Cable

La transformación digital de la Administración pública pasa por contar con puestos de trabajo más inteligentes, seguros y flexibles. Esa es la visión que defiende Virtual Cable, con una propuesta basada en la virtualización como herramienta para facilitar un acceso seguro a la información desde cualquier lugar y dispositivo, adaptándose a las necesidades de cada usuario. La compañía pone el foco en reducir la brecha tecnológica entre administraciones de distinto tamaño y en reforzar la ciberseguridad con un enfoque de confianza cero. Todo ello junto a la sostenibilidad y una tecnología cercana, adaptada a las necesidades del sector público gallego. Fernando Feliu, executive managing director, destaca el valor de soluciones como UDS Government o UDS Education.

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

VIRTUAL CABLE