Órdago del canal en la nube

Del valor que concede la tecnología y los servicios que se orquestan en torno a la nube fue claro reflejo la celebración de la segunda edición del Hybrid Cloud Summit de Arrow en Madrid. Un evento en el que participaron los hiperescalares AWS, IBM, Microsoft y Oracle, y más de una veintena de fabricantes que despliegan su foco de negocio en el centro de datos y en el desarrollo de la ciberseguridad: Arista, Check Point Software, Dell Technologies, Fortinet, F5, HPE, HPE Aruba, Lenovo, Huawei, Ivanti, NetApp, Nutanix, Pure Storage, Radware, Red Hat, Splunk, Symantec by Broadcom, Veeam, Veritas y VMware. *Partners* y fabricantes compartieron espacio y, sobre todo, oportunidades de cara a los próximos meses.

Marilés de Pedro | Olga Romero

Como un foro de intercambio de ideas definió Iñaki López, *regional director south* EMEA de Arrow, el Hybrid Cloud Summit. "La evolución hacia el todo como servicio (XaaS) está clara. Es hacia donde evoluciona la tecnología". El directivo recordó los cuatro pilares en los que reposa la estrategia del mayorista: los clientes, los proveedores tecnológicos, la plataforma ArrowSphere y el equipo humano. En el marco de un encuentro de *cloud*, ArrowSphere contó con un protagonismo destacado. "Contamos con un mayor número de tecnologías que se pueden aprovisionar en la plataforma y hemos incorporado nuevas funcionalidades en seguridad como la ISO 27001 o capacidades de *single sing on* (SSO), con una herramienta de gestión de la seguridad (*dashsboard*) muy importante", enumeró. Una plataforma comprometida con el medio ambiente y que permite una gestión de los costes, a la que se han incorporado, como valor añadido para los *partners*, los servicios gestionados de Arrow como el *backup* o la orquestación.

Panorama "público"

Los modelos operativos en la nube continúan siendo el enfoque predominante entre las organizaciones españolas. El pasado año, según IDC, el mercado español de *cloud* alcanzó los 2.875 millones de euros, con una tasa de crecimiento anual compuesto que se prevé que

> "La tecnología evoluciona hacia el todo como servicio (XaaS)"
>
> **(Iñaki López. Arrow)**

> "La nube representa tres retos para las empresas: FinOps, SecOps y GreenOps"
>
> **(Eric Gourmelen. Arrow)**

sea del 21,9 % entre 2021 y 2025. Un apartado en el que la nube pública es esencial y en el que España, con la enorme apuesta que los principales hiperescalares están haciendo por el país, es pieza clave. De las oportunidades que permite al canal este panorama se habló en la mesa en la que participaron IBM, Microsoft y Oracle.

Javier Grande, *cloud business manager* de Arrow, defendió el papel que juega el mayorista en este complejo entorno, apelando, sobre todo, al valor de ArrowSphere como herramienta esencial en los modelos como servicio. Igual de importantes, señaló, son las personas, a las que se forma, en el lado técnico y comercial, a través de Arrow Education.

"Es un cambio muy importante al que estamos haciendo frente, que se va a acelerar con el uso de la inteligencia artificial". Una estrategia que reposa en el diseño de un plan de negocio para hacer realidad la tecnología. Un plan en el que identificó, como gran oportunidad, la oferta de servicios gestionados de Arrow.

La inteligencia artificial es un motor de innovación para el despliegue de nuevos servicios en los hiperescalares. IBM lanzó hace unos meses Watsonx. "Lo más importante es identificar con el cliente el caso de uso para que lo aproveche el canal", puntualizó Raúl García, director de canal de IBM. "Va mucho más allá de un *chatbot*", remarcó. Casos de uso que, por ejemplo, deben mejorar la experiencia del cliente a través de los diferentes canales, los procesos de automatización o, incluso, la generación de código.

Según McKinsey la inteligencia artificial generará una riqueza a nivel mundial cada año de entre 2,4 y 4 trillones de dólares. Microsoft ofrecerá el próximo 1 de noviembre esta tecnología para todos sus clientes Enterprise como un Copilot más "para ayudarnos en nuestro trabajo", apuntó Antonio Budia, director de *partners* de Microsoft en España. "El *partner* tiene una posición privilegiada, por su conocimiento del cliente, para aprovechar esta oportunidad".

Para Mariano Rodríguez, *cloud sales director* de Oracle, la inteligencia artificial ha llegado para quedarse y para desarrollarse. "En los últimos siete años se ha multiplicado por cien la capacidad del hardware, lo que nos concede más capacidad de cómputo; que hay que aplicar para que se convierta en un beneficio". Rodríguez señaló la sanidad como uno de los campos de uso más importantes que

> "ArrowSphere actúa como un agregador de contenidos"
>
> **(Jordi Soler. SEMIC)**

"otorga más productividad a los médicos, mitigando los riesgos para el paciente".

Regiones *cloud*

El pasado mes de julio IBM abría en España su primera región "Cloud Multizona" (MZR), que comprende tres centros de datos ubicados en Alcobendas, Las Rozas y Madrid capital. Raúl García recordó que se trata de un polo para la atracción de negocio y de talento; y, por el compromiso de IBM con el ecosistema, "el canal se torna en el elemento esencial para conseguirlo. García recordó que el objetivo es ofrecer un entorno seguro y abierto. "Va a ayudar a dar el salto a la nube pública, a eliminar reticencias por parte de algunos clientes, como los organismos públicos, la sanidad o los entornos financieros, y a cumplir con la normativa".

Microsoft ha anunciado la inminente apertura de su región *cloud* en España, en Madrid, a la que se unirá un centro de datos que abrirá en Aragón, desde el que se ofrecerá un sistema de recuperación ante desastres. Budia explicó que va a ofrecer hasta un 40 % menos de latencia, lo que permite que las arquitecturas híbridas que van a desplegar los *partners* sean óptimas. "La región española incluirá todos los servicios *cloud* de los que dispone Microsoft: 365, Azure, Power Platform y Business SAS", recordó. Una nube, con precios competitivos, "lo que concede al canal una ventaja en sus proyectos".

La región *cloud* de Oracle en España se inauguró en septiembre de 2022. La red de regiones de la multinacional está constituida por 64 zonas, 46 de ellas públicas. En Europa, en línea con la soberanía del dato, cuentan con dos centros de datos, que son espejo: el ubi-

cado en Madrid y otro en Frankfurt. "Tenemos muchos sabores de nube", remarcó Mariano Rodríguez. "Nuestros *partners* pueden crear un viaje a la nube para sus clientes, desde una máquina pequeña, para que pierdan el miedo al *cloud*, hasta dónde quieran llegar; lo que permite, incluso, que el *partner* gestione y genere su nube privada".

Unas regiones que para el ecosistema del mayorista son una oportunidad. "Cada vez que hay una apertura de un centro de datos ha aumentado la gestión de la nube por parte del canal", aseguró Javier Grande. "El *partner* cuenta con una enorme capacidad de consumir los diferentes sabores del *cloud*". También apeló al valor de las alianzas que mantienen los hiperescalares para los despliegues de los *partners*.

> "El canal es el elemento esencial para desarrollar negocio en la región *cloud* de IBM"
>
> **(Raúl García. IBM)**

Unas zonas que vuelven a poner en primera línea el debate sobre la soberanía del dato y el obligado cumplimiento de las normativas europeas sobre su seguridad y custodia. El directivo de Oracle asegura que han adoptado, de manera natural, su nube soberana con la legislación europea. "La Administración pública, por ejemplo, debe perder el miedo y debe confiar en que su dato va a estar protegido. Somos especialistas en ello, cumpliendo la normativa europea e, incluso, generando claves para que solo sean los clientes los que pueden acceder a sus datos".

Raúl García especificó, incluso, que se protege al cliente del propio hiperescalar, con tecnologías de encriptación. "Solo la empresa accede a los datos. Ni siquiera IBM". Budia corroboró que la soberanía del dato es uno de los temas más relevantes para las empresas. "En Microsoft cumplimos con todas las regulaciones locales, lo que incluye la GDPR". La multinacional ha anunciado Microsoft EU Data Boundary que asegura, por contrato, que todos los clientes que operan en su nube cumplen con la normativa de que no solo los datos residen en Europa sino que "son gestionados por manos europeas".

> "Los *partners* pueden crear un viaje a la nube para sus clientes"
>
> **(Mariano Rodríguez. Oracle)**

Centro de datos

Ya no hay duda de que el dato es el activo fundamental en la estrategia de las empresas. Su gestión en los entornos híbridos y *multicloud*, en los que han ganado peso los modelos de tecnología como servicio, se hace más compleja. En la mesa en la que participaron Dell Technologies, HPE, NetApp, Pure Storage

y Veritas se abordaron los nuevos retos que se abren en estos entornos y de la respuesta que están dando proveedores y canal. Una mesa moderada por Beatriz Casillas, directora de la unidad de negocio Next Generation Data Center en Arrow.

Purificación Cortés, responsable de canal APEX para Europa en Dell Technologies, recordó que los datos siguen creciendo. Según IDC, en los próximos cinco años, su expectativa de crecimiento ronda el 23 %. Unos datos que, además de crecer, están cada vez más distribuidos. "Más del 90 % de las empresas se declara *multicloud*". Una estrategia *multicloud* que, a su juicio, es tremendamente beneficiosa pero que ha abierto al departamento TI un reto: cómo gestionar ese entorno tan complejo y diverso. "En ocasiones ese desborde a la nube se ha hecho de manera precipitada, muy rápida, poco planificada, lo que ha generado mayor complejidad en la gestión; lo que permite al *partner* desempeñar un rol muy importante en su diseño".

Para Jorge Lorenzo, embajador de HPE, la atracción del dato es la clave. "Los retos son múltiples y multidisciplinares", señaló. "Saber identificar dónde están las cargas y llevarlas o no al *cloud*, y durante cuánto tiempo ubicarlas en un sitio o en otro, es uno de los valores principales que aportan los *partners*". Lorenzo se refirió al entorno cada vez más heterogéneo en el que los grandes hiperescalares conviven con proveedores locales e integradores. "Muchos están evolucionando hacia un perfil de proveedor de servicio". En el terreno de la analítica del dato recordó conceptos esenciales como la soberanía del dato. "Ya no es solo dónde está, sino quién y cómo accede, y qué beneficio va a obtener de ello".

Francisco Torres-Brizuela, director de Canal, Alianzas y Cloud de NetApp en España y Latinoamérica, recordó que los analistas apelan a cuatro conceptos que competen a la gestión de los datos. "Se trata de la seguridad, el ahorro que podemos obtener, la simplicidad y la sostenibilidad". La nube exige el concurso de un número enorme de centros de datos, con un gran consumo eléctrico. "Cuanto más eficiente sea nuestra tecnología, más rentabilidad tendrán las empresas". Torres-Brizuela alertó de la situación a la que se está enfrentando Madrid, en materia energética, ante las numerosas aperturas de centros de datos que se han producido. "La sostenibilidad está en la agenda de los CEO". No olvidó la seguridad. "El *ransomware* ataca al último bastión, que son los datos, que residen en nuestras cabinas. Y eso es lo que hay que proteger".

La marca ha lanzado un nuevo programa de canal, PartnerSphere, que entró en vigor el pasado mes de agosto. Torres-Brizuela se refirió a él como "aire fresco" en el entorno de la infraestructura de almacenamiento y la gestión de los datos. El programa cuenta con 19 competencias. "Los *partners* eligen dónde quieren estar en el mundo de los datos: SAP, Oracle, SQL, Hybrid *cloud*, *analytics*, inteligencia artificial, FlexPod, etc.", señaló. "Hemos dado más flexibilidad y hemos simplificado los distintos niveles, pasando de seis niveles a tres, Approved, Preferred y Prestige. Cada uno con distintas ventajas y beneficios".

> "El *partner* tiene una posición privilegiada para aprovechar la oportunidad de la IA"
>
> **(Antonio Budia. Microsoft)**

> "El *partner* cuenta con la visión holística de lo que ocurre en cada cliente"
>
> **(Eugenio Díaz. Pure Storage)**

Calcula Gartner que los centros de datos consumen entre el 1 y el 2 % de la energía a nivel mundial; y de ella, entre el 20 y el 25 % corresponde al gasto en almacenamiento. Eugenio Díaz, ingeniero de sistemas en Pure Storage, recordó que los fabricantes tienen que entregar al mercado tecnologías cada vez más eficientes con el objetivo de reducir el consumo. "Es un beneficio no solo para nuestros clientes, también para la sociedad".

También se refirió a los retos que se abren en el pujante entorno de los contenedores. "Supone un cambio radical; hay que protegerlos y dotarles de disponibilidad, de *backup* y de soluciones de recuperación ante desastres. Es esencial contar con el control de quién accede a qué y qué hace en todas las capas". Respecto al papel del *partner*, recordó que es el que cuenta con la "visión holística de lo que ocurre en cada cliente y el que tiene el conocimiento de todo el ecosistema".

Santiago Sánchez, responsable de preventa para Iberia en Veritas, insistió en que el gran desafío es el gobierno del dato y localizarlo en el momento preciso. Tareas que en un entorno *cloud* se vuelven mucho más complejas. "Es el *partner* el que debe guiar a los clientes".

Con el *backup* como motor tradicional del negocio, la amenaza del *ransomware* lo ha devuelto a la primera línea tecnológica. "Contar con entornos aislados, en los que se albergue una copia de los datos, inmutable, es imprescindible". El directivo de Veritas cree que el crecimiento de esta amenaza ha hecho conscientes, "a la fuerza", a las compañías de la importancia que tiene el *backup*. "A lo largo de los últimos años el *backup* tenía un cierto carácter de *commodity*; ahora nos hemos dado cuenta de lo importante que es tener una copia segura de los datos. Y no solo por el *ransomware*, también por las exigencias europeas en materia legislativa". El *backup*, insistió, es la vacuna. "No vamos a impedir que se sufra un ataque, pero sí que se sobreviva al mismo". Una tecnología en la que también se aplica la inteligencia artificial "para identificar la última copia de datos limpia".

Oportunidades "como servicio"

Los servicios de suscripción crecen a doble dígito en el negocio de Pure Storage a nivel mundial. Una fórmula, identificada en la gama Evergreen, que cuenta con tres opciones (Forever, One y Flex). "Dotamos a nuestros clientes y a nuestros *partners* de la flexibilidad para elegir cómo quieren acceder y cómo quieren consumir el dato", explicó Eugenio Díaz. "En los últimos años es Evergreen One el modelo que más rápido está creciendo.

> "El *backup* es la vacuna. No vamos a impedir el ataque, pero sí que se sobreviva al mismo"
>
> **(Santiago Sánchez. Veritas)**

Los clientes, no solo buscan un modelo de operaciones *cloud*, que tenemos en todas las suscripciones, sino que quieren un modelo de consumo de infraestructura como servicio". El directivo recuerda que la primera opción que lanzaron, Evergreen Forever, supuso una revolución para el canal. "Se eliminó la obsolescencia de todas las plataformas de almacenamiento".

HPE GreenLake marca la estrategia "como servicio" de HPE. Jorge Lorenzo desvela que su adopción por parte del canal en el último año ha sido mayoritaria. "Hay muchos sabores de GreenLake", recuerda. La marca, para incrementar el número de *partners* que lo adoptaran, ajustó el modelo, poniendo en el centro la idea de lo que GreenLake puede hacer por mejorar el modelo de negocio del *partner*. "Hemos escuchado mucho más al canal, poniendo el foco en la experiencia del *partner* y en cómo construir, de manera conjunta, el ecosistema "como servicio".

La estrategia de canal de Dell Technologies también tiene en los modelos como servicio un pilar de crecimiento. El modelo, que lleva el nombre de APEX, fue presentado hace un par de años por Dell, y recientemente se ha incorporado al negocio mayorista. "Se trata de optimizar al máximo los beneficios de los entornos *multicloud*, siendo APEX el paraguas que aglutina esta estrategia", explicó Purificación Cortés. Diseñar una estrategia *multicloud* se apoya en la posibilidad de ofrecer una gestión consistente y transparente. "Pasa, además, por extender los *stacks* de la nube, independientemente de dónde se estén desarrollando las aplicaciones. Es esencial que estas se comporten de la misma manera, sin tener que estar reescribiendo código permanentemente". Y, por último, hay que dar a los clientes la opción de consumir la infraestructura como servicio. "Es una tendencia clara", aseguró. Con APEX, "el *partner* es capaz de seguir ofreciendo nuevas vías de negocio a sus clientes, adaptándose a sus necesidades; lo que le aporta mucho valor". Su política de canal incentiva, de manera notable, las ventas que se realizan bajo el paraguas APEX. "Es una fuente de rentabilidad para los *partners* que además les permite seguir desplegando toda su capacidad de servicios".

Cortés recuerda que el negocio de infraestructura va a seguir creciendo a nivel mundial

> "El *ransomware* ataca al último bastión, que son los datos. Eso es lo que hay que proteger"
>
> **(Francisco Torres-Brizuela. NetApp)**

en torno a un 13 %, lo que señala los modelos de infraestructura como servicio como los que van a generar más crecimiento. "El negocio de infraestructura tradicional seguirá representando la parte más grande pero serán las fórmulas como servicio las que crecerán de manera más intensa; sobre todo la infraestructura como servicio privada".

También Jorge Lorenzo cree en el desarrollo de las nubes privadas, "no como entes aisladas de la nube pública, sino como parte de una estrategia *multicloud*".

Un discurso similar al de Torres-Brizuela que, entre otras áreas, remarcó el desarrollo de la seguridad, "la resiliencia del dato", especificó; y su análisis. "El gran desafío es la inteligencia artificial generativa donde los datos juegan un papel fundamental. Será la gran oportunidad para los próximos cinco años".

Por su parte, Eugenio Díaz identificó dos vías de desarrollo para el canal. "Hay que dar a los clientes la libertad de elegir cómo quieren consumir y cómo quieren acceder a sus datos. Hay que hacerlo con plataformas, sencillas, que evolucionen junto con sus necesidades". Díaz recordó que la mayor capacidad de cómputo también exige mayor capacidad para procesar el dato. "La inteligencia artificial necesita plataformas que proporcionen, además, paralelismo. Es imposible desarrollar modelos de inteligencia artificial si no cuentas con una plataforma adecuada".

Santiago Sánchez volvió a referirse al gobierno del dato y a la necesidad de controlar la explosión de la información. "Hay que saber cuál es el valor de los datos y quién y cómo los utiliza en los entornos multinube; y saber cuál es el mejor repositorio para el dato", explicó.

Caso de uso en SEMIC

El evento contó con el caso de uso que está haciendo de la plataforma ArrowSphere un *partner* del ecosistema de Arrow, SEMIC, dedicado al despliegue de proyectos tecnológicos, con soluciones y servicios, y con cerca de 100 millones de euros de facturación el pasado año. Jordi Solé, director técnico de la compañía, recordó que cuentan con 10 sedes en España y que, desde hace un año, pertenecen al grupo Econocom.

SEMIC inició la integración de sus sistemas con ArrowSphere en 2020. Solé recordó que el cambio en el modelo de gestión de licencias de Microsoft (NCE) actuó como un catalizador. "Analizamos diferentes opciones pero, al final, vimos que la mejor era ArrowSphere, que actúa como un agregador de contenidos, al que acceden los clientes".

SEMIC ha invertido en áreas como la automatización de procesos, con la integración de su ERP. "Hemos modificado las suscripciones, otorgando autonomía a los clientes para que realicen las modificaciones que necesiten". En el ámbito de la facturación ha sido posible cargar las facturas de SaaS y

de IaaS de manera automática en el sistema de gestión de SEMIC. "Los usuarios pueden consultar el estado de sus suscripciones, con una visión en tiempo real de sus costes en todas las áreas", señaló. En el campo de la analítica, SEMIC asegura una interacción con las plataformas digitales. "Además contamos con un análisis del comportamiento de los clientes en la plataforma".

SEMIC ha logrado 587 nuevos clientes en el último año, con más de 900 suscripciones y 63.000 puestos gestionados, lo que le ha permitido elevar su facturación en un 41 % (doblando su negocio en el área del SaaS). Solé indicó que su objetivo es aumentar la oferta y su catálogo "privado" de soluciones. "Empezamos con Microsoft y con AWS; y ahora contamos con nuevos proveedores y también hemos incorporado los servicios propios de Arrow". SEMIC seguirá experimentando con los nuevos *dashboard* de la plataforma y dinamizando su portal e intensificando su imagen digital. Solé ofreció su conocimiento al resto de *partners*. "Podemos ayudarles en este camino de integración con ArrowSphere".

Oportunidad de la nube híbrida

Según IDC, el 45 % de las empresas españolas ha adoptado una estrategia de nube híbrida dentro de un escenario *multicloud*. Un panorama al que se une el alza de la nube pública. Según sus estimaciones, este mercado público podría alcanzar los 6.878 millones de euros para 2026, lo que supondría una tasa de crecimiento anual compuesta del 13,7 %. De las oportunidades que abre al canal este panorama versó la mesa, moderada por Ignacio Sestafe, BDM de ArrowSphere en el sur de Europa, y en la que participaron HPE Aruba, Lenovo, Nutanix, VMware y Red Hat.

Carlos Piñera, SASE *Business development manager* para el sur de Europa de HPE Aruba, recordó que es esencial "poner criterio en las transformaciones del centro de datos". Muchas empresas se lanzaron a mover sus aplicaciones a la nube, sin mucho orden, y algunas han decidido volver a los entornos tradicionales, aprovechando la infraestructura de la que disponen. "El *partner* debe ayudarles a extraer el máximo valor de cada infraestructura".

Gregorio Chillón, *solutions architect* de Lenovo, señaló las dos áreas en las que Lenovo está apostando y que suponen una oportunidad para el canal: el *edge computing* y la inteligencia artificial. "Se trata, en primer lugar, de las oportunidades que se producen cerca de donde se produce el procesamiento del dato; donde aplica la inteligencia artificial, y donde es posible realizar funciones, por ejemplo, de reconocimiento de patrones".

Alejandro Solana, *technical director* de Nutanix en Iberia, recordó que el canal tiene el desafío de saber de todo. "Estar al día de todo es complicado ya que hablamos de entornos complejos", explicó. La respuesta de Nutanix es apostar por la simplicidad gracias a las alianzas con las que cuenta. "Se trata de proporcionar a los *partners* un entorno en el que, independientemente de la ubicación, del hiperescalar, del centro de datos, del hipervisor y de la plataforma PaaS, puedan proporcionar lo realmente importante para las organizaciones, que son las aplicaciones, los datos y la calidad de servicio (SLA), ayudándoles a diferenciarse en el mercado".

> "Ya no es solo dónde está el dato, sino quién y cómo accede, y qué beneficio va a obtener de ello"
>
> **(Jorge Lorenzo. HPE)**

> "Los modelos como servicio son una fuente de rentabilidad para los *partners*"
>
> **(Purificación Cortés. Dell Technologies)**

Javier Guijarro, responsable de alianzas para IBM, Kyndryl, Viewnext y CCSP en Red Hat, desveló que la mitad de su negocio en 2025

> "El *partner* se convierte en el orquestador de un modelo y de un viaje hacia la nube
>
> **(Alejandro Solana. Nutanix)**

procederá de estos entornos híbridos y de los modelos como servicio. Red Hat ha adaptado sus procesos y programas para ello, con especial foco en las formaciones gratuitas y en los programas de incentivos, "tanto internamente, a nuestra fuerza comercial, como a nuestro ecosistema".

Lluís Altés, *senior business solutions strategist* de VMware, recordó las dudas que existieron, con la explosión *cloud*, acerca de la supervivencia del canal. "La realidad ha demostrado que el *partner* sigue siendo fundamental para los proveedores", aseguró. Una realidad más compleja, en la que se ha establecido un modelo como servicio en el que el *partner* desempeña un papel fundamental "acompañando a su cliente". Altés remarcó que "nadie llega al éxito solo. No hay ningún *partner* ni proveedor que lo domine todo".

Uno de los focos prioritarios de VMware en su relación con su ecosistema es favorecer el despliegue de su modelo de suscripción con el objetivo de que vaya teniendo un mayor peso en el negocio. Altés aseguró que la adopción está siendo muy buena y recordó el mayor peso que tienen en las decisiones de negocio las direcciones financieras. "Quieren una mayor predictibilidad en los costes".

En el caso de Red Hat, estos modelos de suscripción, junto a su filosofía *open source*, de código abierto, siempre han formado parte de su propuesta de negocio. "De media, por cada euro de suscripción que Red Hat vende, hay una oportunidad de negocio de 4 euros en servicios; que en algunos casos puede alcanzar los 10 euros".

Alejandro Solana recordó que la aproximación de Nutanix se basa en tratar de eliminar la complejidad que rige en los entornos híbridos y *multicloud*. "Se han ido uniendo piezas y más piezas, para acabar convertido en un Frankenstein", relató. La "juventud" de Nutanix, al irrumpir en un momento en el que la nube era una realidad, permitió que su oferta se basara en el diseño de "un entorno híbrido, *out of the box*, eliminando la complejidad que supone abordarlo desde una aproximación tradicional". Y, además, hacerlo de "una forma industrializada y automatizada para que entre el 70 y el 80 % de las tareas estén garantizadas". Con ello, la conversación "que establece el *partner* con su cliente está basada en una mayor confianza. El *partner* se con-

> "El *edge computing* y la inteligencia artificial son oportunidades para el canal"
>
> **(Gregorio Chillón. Lenovo)**

Impulsando la excelencia empresarial en la nube

Eric Gourmelen, *vicepresident* y CTO Global de ArrowSphere, comenzó su intervención lanzando una pregunta: ¿Qué es lo más importante que le ha ocurrido al sector TI en 2023? La inteligencia artificial, señalaron los asistentes. Sin embargo, el directivo apuntó otro acontecimiento: la Corporate Sustainability Reporting Directive (CSRD), una normativa que obligará a las empresas europeas a elaborar y reportar informes sobre sus emisiones de GEI/CO2. Se trata del mismo procedimiento que ya siguen las organizaciones para el envío de sus informes financieros.

La normativa entrará en vigor el próximo año para las empresas de más de 500 empleados, las cuales tendrán que enviar el informe en 2025. Año en el que las compañías de más de 250 trabajadores deberán acogerse a esta ley y enviar el informe en 2026. Será a partir de 2028 cuando la normativa ya será obligatoria para todas las organizaciones europeas, independientemente de su tamaño. Con esta iniciativa la Unión Europea tiene como objetivo reducir las emisiones de GEI/CO2 en un periodo de cinco años para alcanzar la neutralidad de carbono en 2050 tal y como se acordó en el Pacto Climático de París.

Pero Gourmelen no podía obviar la IA. El directivo apuntó a la predicción de que en los próximos años cada empleado tendrá múltiples agentes autónomos o copilotos trabajando para ellos. Una realidad que provocará un consumo de 300Kwh/mes por agente; razón por la que es necesario trabajar para que las empresas controlen sus emisiones, ya que, como aseguró, "definitivamente la CSRD y la IA están conectadas". Una conexión vinculada también con el modelo XaaS, que está dominando el

mercado. "Es la tendencia principal y se espera que para 2026 más del 50 % del gasto mundial en el mercado IT sea en XaaS", comentó. Por ello, contar con una plataforma como ArrowSphere que permita "gestionar todo el ciclo de vida de los servicios es imprescindible".

Volviendo a los desafíos que supone la nube, Gourmelen mencionó tres: la seguridad, los costes y la sostenibilidad. En relación a este último, el directo explicó que las novedades de ArrowSphere permiten a las organizaciones analizar las emisiones de CO2 para, después, optimizarlas. En cuanto a la seguridad, Gourmelen mostró el crecimiento que han experimentado las ciberamenazas en los últimos años, incremento que supera el 25 % interanual y que se refleja en el coste que se prevé que alcance el cibercrimen en 2025: 10.000 millones de dólares. Para mantener bajo control la seguridad en la nube, ArrowSphere ofrece monitorización y análisis con el fin de garantizar mayor visibilidad a las empresas sobre su nivel de seguridad. Por último, el directivo habló sobre los costes, la gestión y la optimización del *cloud*. Actualmente el 30 % del gasto en la nube se desperdicia, por ello es de vital importancia optimizar al máximo los costes en la nube. "ArrowSphere simplifica está tarea estudiando el consumo y monitoreando el ahorro potencial".

vierte en el orquestador de un modelo y de un viaje hacia la nube de manera práctica".

En el caso de Lenovo su apuesta por el modelo de pago por uso lleva el nombre de TruScale. Gregorio Chillón recuerda que es una opción para los clientes que buscan flexibilidad y que quieren olvidarse de la obsolescencia de la plataforma, en el largo plazo. "Es una opción pensada para trabajar con el canal, disponible también en ArrowSphere".

Carlos Piñera corrobora que va a seguir existiendo una diversidad. "Todo va a estar interconectado y va a haber múltiples conexiones, lo que otorga mucho protagonismo al *edge*", aseguró. "Es necesario orquestar esta conectividad con una seguridad con la que deben contar las aplicaciones, que ya no solo están en el centro de datos, sino en cualquier parte". Esto exige el concurso de una plataforma, habilitadora de servicios, "que permita al canal construir y ayudar a los clientes a maximizar sus inversiones".

> "El *partner* debe ayudar a las empresas a extraer el máximo valor de cada infraestructura"
>
> **(Carlos Piñera. HPE Aruba)**

Seguridad y entornos híbrido, ¿cuál es su verdadero papel?

La seguridad sigue siendo uno de los segmentos de mayor oportunidad. Según datos de IDC, este año el mercado de la seguridad en España está creciendo un 9,2 % respecto al año anterior lo que permitirá alcanzar 2.130 millones de euros. La consultora prevé también que para 2026 este mercado pueda llegar a superar la barrera de los 2.995 millones de euros, manteniendo ritmos de crecimiento que se acercan al doble dígito (9,9 %). Como resultado la ciberseguridad representa una oportunidad, pero también un gran reto ya que en el nuevo contexto híbrido en el que nos encontramos la superficie de ataque es cada vez mayor. De ello se habló en la mesa en la que participaron Fortinet, Ivanti, Splunk, Symantec by Broadcom y Veeam, moderada por Ángel García, director de seguridad y *networking* de Arrow.

> "De cada euro de suscripción en Red Hat, hay una oportunidad de 4 euros en servicios; que incluso puede alcanzar los 10"
>
> **(Javier Guijarro. Red Hat)**

Sobre los retos comenzó hablando Guillermo Martínez, *cloud BDM* Iberia de Fortinet. "El 69 % de los clientes están trabajando con dos o más hiperescalares o plataformas *cloud* y a esto se le suma la falta de perfiles preparados", aseguró. Realidad que hace imprescindible que las organizaciones dispongan de "una práctica consistente

de seguridad en todas las nubes". ¿Cómo? Con una plataforma consistente en todos los entornos. "En este sentido nuestra apuesta está clara, vamos a trabajar con conceptos como Security Fabric", afirmó. Una plataforma que, gracias a que engloba un amplio abanico de productos que abarcan la totalidad de los aspectos de seguridad, permite a Fortinet registrar datos para ir más allá porque "el objetivo ya no es saber dónde me están atacando o saber responder, es empezar a predecir dónde me pueden atacar".

Desde Ivanti, José Manuel Marcos, *sales engineer*, señaló como principal reto la visibilidad. "Tener la capacidad de saber qué tienes en cada entorno, qué usuarios acceden a las aplicaciones en la nube y cuáles lo hacen *onpremise*, así como qué aplicaciones dependen de otras", explicó. Para Ivanti "la primera ley es que no puedes proteger lo que no sabes que existe". Tal y como detalló, sin una foto fija de los activos, las empresas no saben cuáles son sus riesgos potenciales. Cuando esto está claro, llega el momento de proteger los activos y aplicaciones y garantizar la seguridad de todo el ecosistema. En este punto lo difícil, como indicó, "es tenerlo todo agregado en una base de datos que te pueda dar servicio".

> "Nadie llega al éxito solo. No hay ningún *partner* ni proveedor que lo domine todo"
>
> **(Lluís Altés. VMware)**

La superficie de ataque ampliada, la combinación de diferentes cosas "construidas con sus propias reglas y terminología, pero que queremos observar de manera continua", y la sofisticación de los ciberataques debido a la inteligencia artificial fueron los tres puntos en los que Miguel Pleite, *sales engineer manager* de Splunk, resumió los retos que suponen los entornos híbridos en lo que a seguridad se refiere. En relación a la IA, recordó la necesidad de utilizarla, al igual que lo hacen los malhechores digitales, porque "nos permitirá mejorar la detección de amenazas y brindar automatismo para poder manejar todo ese volumen de distintas nubes". Contar con un SIEM es importante porque "se necesita detectar", pero "se queda muy corto para lo que estamos viendo". Por ello, el directivo comentó que "se necesitan hacer muchísimas más cosas y eso tiene que apoyarse en los datos que existen".

> "El objetivo es empezar a predecir dónde me pueden atacar"
>
> **(Guillermo Martínez. Fortinet)**

Rufino Honorato, *regional technology officer* de Symantec by Broadcom, y Santiago Pérez, *cloud manager* de Veeam, ratificaron todos los desafíos ya mencionados y añadieron alguno más. Honorato habló del caos que está

creando el *multicloud*: "Ya no hablamos de híbrido, sino de *multicloud*". Un caos cuya solución se encuentra en dos puntos. Por un lado, "las empresas necesitan una solución que les permita aplicar controles y políticas centralizadas a través de todas las nubes" y, por otro lado, deben centrarse en los datos.

En el camino hacia el *cloud*, en el que "unas empresas son más ágiles que otras", los *vendors*, *partners* y proveedores deben adaptarse a la velocidad de cada cliente. Una adaptación que la compañía hace con Symantec Enterprise Cloud en el que engloban todos sus servicios de seguridad. "Aplicamos conceptos de ZTNA, que comienza con una gestión de la identidad".

Pérez resumió los retos en cinco. A los ya mencionados (consistencia, visibilidad, amplia superficie de ataque y complejidad), añadió el quinto, la problemática de evitar la degradación de los procesos. "Lo que hoy es seguro dentro de seis meses no lo va a ser". Además, sobre los desafíos que supone proteger los datos dispersos en diferentes nubes e infraestructuras aseguró que "tener, por un lado, la visibilidad de lo que tienes en cada entorno y hacer consistentes las políticas de seguridad en cada uno de ellos y, por otro lado, la flexibilidad a la hora de saltar entre ellos, son las mayores complejidades".

Para finalizar los expertos señalaron cuáles serán las oportunidades que se le presentarán al

> "No puedes proteger lo que no sabes que existe: si conoces los activos que tienes, sabes a qué riesgos te enfrentas"
>
> **(José Manuel Marcos. Ivanti)**

canal de distribución en el fragmentado y cambiante mercado de la ciberseguridad. Todos ellos coincidieron en señalar oportunidades como la automatización o el resto de nuevas tecnologías y los servicios gestionados como puntos clave para los negocios del canal. Además, resaltaron el papel de orquestador que tiene el canal y su capacidad para conseguir la colaboración entre los diferentes fabricantes.

El hándicap de proteger redes, aplicaciones y nube

Se podría decir que nos encontramos en el contexto más preocupante de los últimos años porque se calcula que cada 1,5 segundos hay un ataque en algún punto de Internet. Según datos del Instituto Nacional de Ciberseguridad (INCIBE), su Centro de Respuesta a Incidentes de Seguridad detectó en 2022 un total de 118.820 incidentes, un 9 % más que en el año anterior.

En un mundo marcado por lo híbrido y el *multicloud*, la superficie de ataque es cada vez mayor, lo que exige a las empresas y organismos públicos un diseño de la seguridad que abarque la nube, las aplicaciones y la red. Una exigencia que también impacta sobre el ecosistema de socios. Pero, ¿cómo están abordando esta seguridad, que ha pasado de ser una barrera a un habilitador, las empresas? Reflexionaron sobre ello Arista, Check Point Software, F5, Huawei y Radware, en una mesa moderada por Alejandro Soto, director comercial de Arrow.

> "El SIEM es importante, porque es necesaria la detección, pero se necesita hacer muchas más cosas"
>
> **(Miguel Pleite. Splunk)**

"En el contexto de infraestructura, redes y conectividad la seguridad es muy importante, pero lo que estamos viendo es que a veces nos olvidamos de esa infraestructura", arrancó diciendo Manuel Méndez, *systems engineering manager* de Arista. En los actuales entornos híbridos, los cuales han llegado para quedarse, se está dando "un gran consumo de ancho de banda". Realidad que obliga a que la seguridad sea prioritaria. "En Arista estamos trabajando con nuestros clientes en garantizar que todo el tráfico, ya proceda del *cloud*, *onpremise* o de cualquier fibra, esté encriptado".

Otro punto que también están trabajando desde Arista es en construir la conectividad lo más simple posible. "Insistimos mucho en utilizar protocolos estándar". Algo que puede sonar a un nivel bajo de seguridad, pero que,

> "Tener la visibilidad y flexibilidad son las mayores complejidades para proteger los datos en diferentes nubes"
>
> **(Santiago Pérez. Veeam)**

como afirmó Méndez, "ayuda a mantener los sistemas actualizados" y evitar problemas de seguridad derivados de no haber podido actualizar por no saber cómo funciona el sistema. Para Check Point Software "intentar simplificar la seguridad" es la prioridad. Como apuntó Javier Rodríguez, *southern Europe cloud manager*, "los entornos híbridos son la tónica general, lo que señala una complejidad, desde cualquier punto de vista. Y en seguridad, cuanto más complejo menos seguro". Ofrecer una capa de abstracción es su apuesta que busca que "la política de seguridad de la empresa, que es una, pueda aplicarse en los diferentes entornos de forma automatizada".

> "Debemos adaptarnos a la velocidad de cada cliente y no llevarle a la nube demasiado rápido"
>
> **(Rufino Honorato. Symantec by Broadcom)**

> "Es importante disponer de redes sencillas que permitan solucionar un problema de seguridad en cinco minutos"
>
> **(Manuel Méndez. Arista)**

Pero no solo hay que simplificar teniendo una plataforma: hay que ir más allá y es imprescindible "cuantificar el riesgo porque es fundamental saber cómo están las operaciones. Somos capaces de poner un numerito a cada una de las amenazas que hay en los activos", detalló. Gracias a ese "numerito" los clientes conocen a qué riesgos se enfrentan y a los que deben prestar especial atención.

Sencillez que también buscan desde F5. Luis Miguel Cañete, *channel manager* de España y Portugal, señaló las dos tendencias: la proliferación de aplicaciones y la expansión de la superficie de ataque. Tendencias que han complicado la vida a las empresas que se están encontrando con diferentes silos tecnológicos, muy difíciles de gestionar. "Hay que hacer absolutamente fácil lo que, en los últimos tiempos, se ha complicado mucho". F5 garantiza que la gestión y protección de los diferentes entornos se haga de una "forma totalmente homogénea, como si estuviéramos trabajando con un único *cloud*".

El responsable de canal incidió en la proliferación de las aplicaciones; una realidad vinculada con el objetivo de brindar la mejor experiencia de usuario. Finalidad que ha derivado en la adopción del *cloud* y de los modelos *as a service* que "proporcionan una escalabilidad infinita y garantizan trabajar con la última versión de dicha tecnología", comentó. Una

> "Simplificar y cuantificar el riesgo es fundamental"
>
> **(Javier Rodríguez. Check Point Software)**

> "La adopción del *cloud/ multicloud* y de los modelos *as a service* se explican por ganar la batalla de la experiencia del usuario"
>
> **(Luis Miguel Cañete. F5)**

carrera de fondo en la que F5 trabaja para "acercar la aplicación al usuario allí donde esté y la seguridad allí donde se está produciendo el ataque".

"Los clientes ya están solicitando que las estrategias incluyan medidas de seguridad", afirmó Leticia Valcarce, *ecosystem development manager* de Huawei. En este sentido, tal y como explicó, la compañía trabaja con sus clientes siguiendo unos pasos muy definidos que empiezan por la definición de permisos de accesos, verificación de datos y protección de los contenidos compartidos entre los diferentes departamentos. "Les enseñamos a gestionar las cargas que tienen en Internet y cómo protegerlas". Huawei desarrolla una infraestructura tolerante a fallos, autoescalable, y apuesta por trabajar con *partners* que sean especialistas en ciberseguridad.

Valcarce recordó que las infraestructuras de Huawei, quinto proveedor *cloud* a nivel mundial, son atacadas constantemente. Realidad que permite a la compañía "entrenar nuestros modelos de inteligencia artificial, capaces de aprender y responder". De esta manera, "podemos ofrecer esa seguridad más avanzada y dar más especificaciones a nuestros clientes". Por último, la directiva subrayó la importancia de las alianzas con proveedores, *partners* y fabricantes para avanzar en sistemas de seguridad.

Jorge Maraña, *regional sales manager* de

Radware, afirmó que "cuando los clientes empiezan a tener madurez se encuentran que los desafíos de ir al *cloud* son grandes, tanto en términos de seguridad como de *networking*". Al mismo tiempo, y al ver que la superficie de ataque se amplía, apuestan por las soluciones de seguridad de los hiperescalares, soluciones que requieren conocimiento, mantenimiento y actualizaciones. Generar todo eso "es muy costoso". Por ello, desde Radware ofrecen su solución en la nube, que puede ser utilizada en cualquier entorno *multicloud* y que "al ser gestionada 100 % por nosotros reduce costes y ofrece una visibilidad absolutamente integrada que permite tener todos los eventos de seguridad de vídeos o de web en una misma plataforma". También se refirió a las soluciones de seguridad tradicionales, las cuales "pueden no ser suficiente ya que no están preparadas para los nuevos ataques" y recordó que detrás de estas soluciones sigue habiendo mucho proceso manual. La solución que apuntó es combinar las bondades del *cloud* con la capacidad de cómputo de los hiperescalares y "añadirles automatización basada en *machine learning*".

> "Los ciberataques permiten entrenar a los sistemas de IA para que aprendan y respondan, y podamos ofrecer una seguridad avanzada"
>
> **(Leticia Valcarce. Huawei)**

Unas aportaciones que tienen muchas ideas en común y que dejan de manifiesto la colaboración existente entre los diferentes fabricantes para aportar al mercado soluciones con las que hacer frente a los complejos entornos en los que se mueve. Aplicaciones que encuentran su punto de encuentro en plataformas como ArrowSphere.

También coincidieron los expertos en algunas de las oportunidades de negocio que tendrá el canal; que debe jugar su papel de asesor porque conoce a los clientes, sus necesidades y demandas; siendo el punto de unión entre la tecnología y los clientes. A partir de ahí tiene la oportunidad de proveer de conocimiento a los usuarios y perfiles no técnicos, así como de servicios. Y es que el modelo de seguridad como servicio ha llegado para quedarse.

> "Las soluciones de seguridad tradicionales no están preparadas para los nuevos ataques"
>
> **(Jorge Maraña. Radware)**

Otras opciones de negocio se centran en la renovación de las redes que se prevé para el próximo año y en la criptografía. Los participantes animaron al ecosistema de canal a formarse, especializarse y aliarse con otras empresas para aprovechar al máximo estas oportunidades.