IA: retos y oportunidades de una tecnología que marca una revolución

Reunió Arrow Enterprise Computer Solutions en las oficinas de Microsoft a cerca de 100 profesionales de su ecosistema de *partners* para hablar de IA, una tecnología que juega, a la vez, un doble papel: es un reto pero también se torna en oportunidad para cualquier compañía que opera en el universo Microsoft.

Un evento que abarcó una parte teórica y otra práctica; y en el que se habló del salto que ya están dando las empresas del asistente al agente, y en el que dio cumplida cuenta de las "capas" de inteligencia de la multinacional: Work IQ, Fabric IQ y Foundry IQ. No faltaron tampoco Microsoft Agent Factory y Microsoft Agent 365, que se lanzó el pasado 1 de mayo.

Marilés de Pedro

IA y empresa

Del impacto de la IA en las organizaciones, de su uso, del despliegue de los agentes y del liderazgo que deben asumir los directivos en su aplicación hablaron Sofía Virgós, AI *business solutions* CSA de Microsoft, y Magda Teruel, *partner* solution architect de Copilot de Microsoft. Ambas se refirieron al último índice de tendencias laborales de Microsoft presentado el pasado mes de mayo. "Las personas están listas para la IA. Las que no lo están son las organizaciones", destacó Sofía Virgós. Según el estudio el 67 % está centrado en factores organizacionales. "Para que la IA genere un impacto real en las organizaciones hay que tener una cultura segura donde los empleados puedan utilizar la IA sin ningún problema y contar con una capa ejecutiva que lidere con el ejemplo". Alertó de que hay que tener un modelo de gobierno que sustente todas estas prácticas y contar con talento que impulse el uso de la inteligencia artificial. "Y es donde están fallando las organizaciones", indicó.

Si se analiza en qué utilizan los empleados la IA, según el estudio, casi la mitad la está utilizando para generar trabajo de mayor valor. "Los empleados que antes se dedicaban a producir, ahora pueden dedicarse a analizar". El estudio se refiere al concepto de "empresa frontera": operada por agentes de inteligencia artificial pero liderada por humanos.

Magda Teruel señaló que los agentes "son como *minions* que vamos a tener en nuestras organizaciones haciendo cosas y que cuando acaben, van a venir a reportar". Ahora bien, para aprovechar todas las posibilidades de Copilot hay que elevarlo. "Hay que empezar a no aplicar IA en tareas pequeñitas, sino en procesos; lo que da paso a la automati-

zación". También a los casos de uso que las empresas podrán montar a escala.

Teruel se refirió a la dificultad de acceder a la información, que no está estructurada que hay en las organizaciones y que puede moverse entre el 80 y el 90 %; un contenido de mucho valor al que no se puede acceder. "Hay un *gap* que gracias a la IA podemos salvar ya que es muy buena captando valor de este contenido desestructurado".

La multinacional marca cuatro modos de trabajar con la IA. La primera señala al llamado "agente asistente", vinculado con las tareas de consulta; una actividad que va más allá de un resumen de un documento o de señalar si aparece un tema determinado. "Es una consulta más avanzada que permite contrastar opiniones", señaló Sofía Virgós. "Contamos con un consejo de agentes (GPT y Claude) que van a llevar a cabo un contraste de la información, con distintos informes, lo que nos ayuda a evaluar diferentes puntos de vista y a tomar decisiones respecto a un tema concreto".

> "Las personas están listas para la IA. Las que no lo están son las organizaciones"
>
> **(Sofía Virgós)**

El segundo modo es la exploración. "Se trata de ir un paso más allá, probar y experimentar con la IA". Después está la colaboración. "Se trabaja en conjunto con la IA, lo que nos permite disfrutar de un nivel de profundidad mayor en lo que entregamos", continuó Virgós. "Tenemos que invitar a nuestros clientes a que empiecen a pensar en escenarios que

> "Es clave descubrir el valor de la IA"
>
> **(Magda Teruel)**

generen autonomía y determinar cuántos agentes autónomos van a tener".

Por último, está el modo de delegación. "Es la estrella", calificó Magda Teruel. El protagonista es Copilot Cowork que señala la inclusión de capacidades agénticas en Copilot. "La IA lleva a cabo actuaciones de principio a fin".

Ambas portavoces insistieron en que lo importante es entender cómo vamos a trabajar con la IA y hasta dónde vamos a retarla. "Evoluciona a una velocidad increíble", recordó Virgós. "Hay que seguir retando a nuestros clientes a que prueben los diferentes escenarios; en ir más allá de la consulta y empezar a trabajar con Copilot Cowork".

Magda Teruel se refirió al retorno de la inversión. "Es clave descubrir el valor de la IA". Es muy difícil, alertó, medir la ganancia de productividad "si solo utilizamos la IA de manera reactiva". Hay que dar un paso más y encontrar un patrón que se pueda vincular a un indicador para medir los resultados "cuándo

usamos IA y cuándo no". La mayoría de los indicadores se vincula con el ahorro de tiempo. "Es bueno, pero hay que incluir otros de más calidad vinculados, por ejemplo, con la creatividad o con la calidad de los procesos".

Por último, se insistió en el papel clave de los líderes en las organizaciones en el uso de la IA. "Tienen que tomar el control", señaló Virgós. "La IA debe ser esponsorizada desde la capa ejecutiva para que amplifique el valor de los trabajadores. El juicio humano debe seguir en el centro".

La IA: madurez y uso

Kiko de Ángel, EMEA *data&AI architect* de Microsoft, habló de la madurez de la IA, de cuál es el estado real y de cómo se puede aprovechar realmente. También entró, en detalle, en cómo trabajar con los agentes.

La evolución de la IA es meteórica. "El CTO de Microsoft ya pronosticó que en menos de 3 años todo lo que no lleve IA, o no la utilice, va a parecer que está obsoleto o que está roto", señaló. "Ese es el verdadero reto para todas las organizaciones: *partners*, clientes y empresas nos tenemos que adaptar". Una realidad que, reconoció, a veces asusta. "Tenemos la sensación de que si no lo empiezo a adoptar, me quedo fuera del juego. Una ansiedad que provoca un ritmo imparable".

El directivo alertó de que la IA tiene alucinaciones y comete errores. "La IA es muy grande: cuenta con un montón de información y está entrenada con millones de datos", recordó. "La mayoría de los modelos avanzados están entrenados con toda la documentación que tenemos a lo largo de toda nuestra historia: tiene tanta información que se vuelve loca". Por tanto, se ha tratado de

dar respuesta a problemas más pequeños; lo que es el origen de los agentes que, detalló, se componen de 3 elementos: un modelo de lenguaje (LLM), unas instrucciones y unas herramientas.

En relación al LLM, aseguró que su utilidad es entender bien al usuario y, en base a las instrucciones (lo más importante del agente) generar una acción. "Con ello, conseguimos que los modelos LLM, tan grandes, sean más concretos para evitar que fallen".

Una de las capacidades más importantes de los agentes está en la información, en la inteligencia con la que se les dota para que lleven a cabo las acciones que el usuario requiere. "La inteligencia es la gasolina del agente", señaló. Ahora bien, debe procesar datos buenos. "Aunque esté muy capacitado o tenga muchas herramientas, si los datos son malos, los resultados también lo serán: la IA sin datos no es nada". Ahora bien, debe ser una IA con guardarraíles, con buenas instrucciones.

> "La IA sin datos no es nada"
>
> **(Kiko de Ángel)**

El 70 % de los proyectos que se ejecutan no llegan a producción, lo que se explica, fundamentalmente, a tres motivos. "El ritmo de la innovación es tan alto que las empresas se esperan al siguiente movimiento para ver cuál es el modelo ideal y posponen su prueba de concepto", explicó. También los riesgos y el gobierno. "Hay que asumir que la IA tiene ciertos riesgos, lo que hay que hacer es limitarlos y gobernarlos". Por último, el desalineamiento estratégico. "Las empresas no saben para qué hacen un proyecto, pero lo lanzan".

> "Para una buena IA los datos tienen que estar limpios"
>
> **(David Suz)**

El directivo trató de dar respuesta a los dos primeros. Para ello, es clave dotar a los agentes de las mismas capacidades y el mismo contexto que tienen los usuarios. "El mejor agente no podrá ser tan bueno como el mejor usuario si no le doy la información necesaria para que lo sea: agentes y usuarios se tienen que parecer cada vez más". Por tanto, para desbloquear las capacidades de la IA "tenemos que tener inteligencia, buenos datos, construir nuestros agentes y ser capaces de observarlos, controlarlos y gobernarlos. Son los elementos críticos en los procesos de IA".

Unos elementos que se materializan en tres soluciones, bajo la capa de inteligencia (Microsoft IQ), que agrupa a Work IQ (cómo trabajan los empleados y cuál es el contexto de la empresa), Fabric IQ (el agente tie-

ne que saber cuáles son los datos y cómo consumir la información de la organización) y Foundry IQ (los agentes tienen que saber cómo utilizar la información para responder a las dudas que le están planteando). Microsoft cuenta, además, con Agent Factory, para construir los agentes, con diferentes sabores; y Agent 365.

De Ángel insistió en que los modelos no son importantes. "La clave es saber para qué se utilizan y cuál es la inteligencia con la que se dota a la información". Microsoft cuenta con 11.300 modelos e, insistió, el usuario puede trabajar con el que quiera. También se refirió a la necesidad de "empequeñecer" los LLM, para que den respuesta a problemas más pequeños. "Hay que decidir cuál es el tamaño de ese agente y el de la aplicación: se hará tan pequeño como se necesite sin hacer microservicios que no tienen sentido. Hay que hacer agentes que aglutinen tareas, no acciones", alertó. Por tanto, hay que orquestar agentes. "Las empresas cuentan con

múltiples agentes que resuelven un problema grande y cada uno de ellos es experto en hacer una única cosa". La orquestación, por tanto, es crítica. Una tarea de la que se encarga Microsoft Agent Framework "que orquesta agentes de cualquier tecnología de una manera sencilla".

Unos agentes que incluso pueden construir código (gracias a GitHub Copilot). "Tenemos que saber aprovechar la IA para hacer aplicaciones que sean valiosas", lo que abre grandes posibilidades a los equipos de desarrolladores. "Desarrollar código solo es una pequeña parte de su trabajo: un desarrollador tiene que planificar, entender el proyecto, documentarlo, etc.". Microsoft cuenta,

para ello, con la iniciativa Scout, que "permite generar agentes que son necesarios para ejecutar un proyecto, cada uno con su modelo LMM diferente, experto en su área".

Microsoft Agent 365

Unos agentes que parecen "multiplicarse". De Ángel recordó que cada vez que un *partner* instala en un cliente un usuario nuevo de Microsoft 365, se "levantan" 139 agentes, lo que implica un enorme reto para los administradores. "Son agentes autónomos, en los que se delegan tareas y utilizan datos", recordó. "Y que necesitan control". A eso se dedica Microsoft Agent 365, disponible desde el pasado 1 de mayo. "Es la capa de control de los agentes de la empresa y lo que permite saber qué es lo que está pasando con ellos".

Abarca tres funciones. "Observa lo que ocurre en la organización, permite gobernarlo y protegerlo". Gobernar agentes, puntualizó, no es saber que existen sino controlar a lo que acceden y estar protegido con lo que todo lo que ocurre a su alrededor.

> "Con el nuevo cuadro de mando de oportunidades los *partners* pueden tener conversaciones de nuevo negocio con los clientes"
>
> **(Ignacio Sestafe)**

Ante el dato de que el 29 % de las empresas dice que tienen un programa para gestionar y gobernar a los agentes, de Ángel aseguró que le parece muy elevado. "La mayoría de las empresas no tiene nada. No hay una estrategia de gobierno".

Una gestión que evita que se utilice tecnología a la que la organización no ha dado permiso. "Tenemos un *AI shadow* que los administradores no saben que existe". No se trata de poner límites a la IA sino de saber lo que están haciendo los usuarios y "ofrecerles una alternativa con el control de la empresa".

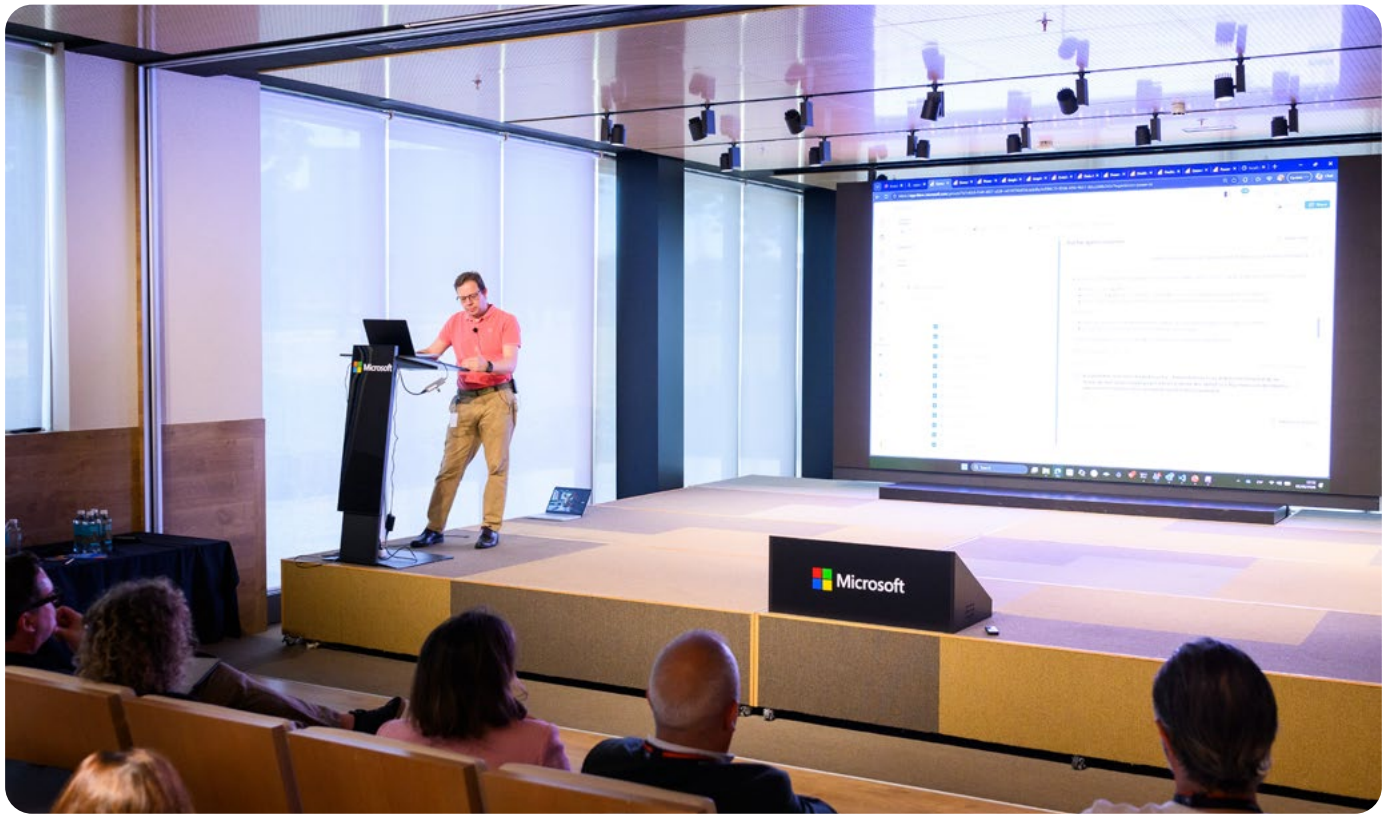
Aplicar políticas de gobernanza es esencial. A pesar de que el 21 % de las empresas asegura que cuentan con una madurez en este apartado, el directivo aseguró que no es cierto. "Si el 70 % de los proyectos de IA fracasa, es imposible que haya madurez en los proyectos de adopción de agentes", enfrentó. "Hay que aplicar unas reglas que tienen que cumplir".

La protección es otro punto crítico. "Los agentes pueden ser atacados". Alertó del *prompt injection* que trata de extraer datos a través de la formulación de preguntas maliciosas. "El *hacking* de agentes es una realidad", alertó.

Esta estrategia global se basa en el concepto de la identidad. Cada agente tiene su propia identidad: agentes y usuarios son lo mismo, por lo tanto, la gestión se realiza de la misma manera. Por último, se puso en valor la integración de la tecnología de Microsoft con

un ecosistema de *partners* que asegura que un agente creado en Anthropic, Wordtail o ServiceNow, por ejemplo, puede seguir este proceso de gestión, control y protección de agentes.

La parte práctica corrió a cargo de David Suz, *solution engineer* de Microsoft, que se encargó de realizar distintas demostraciones de Fabric IQ y la interacción con los agentes.



ArrowSphere Cloud

Ignacio Sestafe, EMEA *south regional sales lead* de Arrow, se encargó de recordar las funcionalidades de ArrowSphere Cloud, la plataforma *cloud* del mayorista que, además de simplificar la gestión de licencias, asegura la escalabilidad, lo que permite adoptar el *cloud* de forma acelerada.

Las funcionalidades de la plataforma se reparten entre el aprovisionamiento (presupuestos, pedidos, etc.), la gestión del ciclo de vida de la suscripción (cancelaciones, actualizaciones, etc.), las capacidades de analítica y la gestión de la facturación. Cuenta con la posibilidad opcional de que el *partner* despliegue un portal para ayudarle en la gestión de sus clientes.

La potencia de ArrowSphere Cloud cuenta con diferentes paneles de control. El primero de ellos, el más básico, se identifica con el interfaz que observa un *partner* cuando accede a la plataforma y que le permite analizar todo su negocio. Otros dos paneles permiten el acceso a las suscripciones contratadas en un modelo de pago por uso (SaaS) y al consumo de servicios en el área de IaaS.

Otro panel de control es SecOps, referido a la seguridad, que permite tener acceso a las potenciales vulnerabilidades que puede te-

ner el negocio. Cuenta con niveles: el primero permite observar las suscripciones de todos los clientes; otro observa el acceso por cliente y el último, que da acceso a la suscripción, detalla las posibles vulnerabilidades, incluyendo sugerencias de remediación.

FinOps está especializado en la optimización de costes. Se persigue una optimización de la infraestructura y los servicios que tienen instalados en los clientes, lo que les permitirá hacer más cosas y, por tanto, habrá un mayor consumo, lo que les permitirá incrementar su negocio.

Por último, GreenOps está vinculado a la sostenibilidad. Permite cumplir con la directiva CSRD, la Corporate Sustainability Reporting Directive de la Unión Europea, que asocia emisiones de gases de efecto invernadero con las suscripciones de infraestructura de Microsoft Azure.

Las novedades son dos nuevos cuadros de mando: el AI360, que permite supervisar el consumo de LLM, tanto SaaS como PaaS, para optimizarlo, no solo en coste sino en prestaciones; y un cuadro de mando de oportunidades. "A partir de un análisis, las determina, lo que permite a los *partners* tener conversaciones de nuevo negocio con los clientes. Es una herramienta muy efectiva".

> "Los modelos de razonamiento permiten construir soluciones mucho más avanzadas y útiles para las organizaciones"
>
> **(Jordi Herrero)**

La plataforma cuenta con ArrowSphere Assistant, un asistente digital, basado en Azure Open AI, que utiliza algoritmos avanzados de IA para analizar patrones de uso y hacer recomendaciones; y con Cloud Assistant, un asistente de IA que se ha integrado en el Customer Portal, lo que abre el uso de esta tecnología al cliente del *partner*. "Este permite detectar no solo las oportunidades que tienen vuestros clientes, sino presentar una oferta adecuada, generar un email, preparar una reunión, etc.".

Mesa redonda

Durante el evento tuvo lugar una mesa de debate, bajo el título "El ecosistema de la IA: creando valor juntos", en la que portavoces de tres *partners* de Microsoft ofrecieron su testimonio acerca de la realidad de la implantación de la IA en la empresa española.

Según el índice de tendencias laborales de Microsoft, el porcentaje de directivos españoles que tiene previsto utilizar agentes de IA en los próximos 12 a 18 meses es del 89 %, el más alto de los países europeos analizados en el estudio, y que supera en 12 puntos la media de Europa (77 %). Una cifra, realmente espectacular, que plantea muy buenas oportunidades para el ecosistema de *partners* de Microsoft. Para Jordi Herrero, director

de soluciones de IA en NexTReT, existe una clara voluntad de incorporar la IA, aunque los niveles reales de implantación aun sean reducidos: según el INE, alrededor del 20 % de las empresas españolas ya cuenta con agentes. "Hay interés por incorporar inteligencia artificial dentro de las organizaciones y este dato nos abre la posibilidad de realizar numerosos proyectos". Las grandes empresas, analizó, están más avanzadas, "mientras que muchas organizaciones pequeñas están empezando con herramientas gratuitas e implantación de alguna tecnología en la sombra", explicó.

Juan Ignacio Amorrortu, ejecutivo senior de infraestructura digital y de nube de Inetum, corroboró el interés, enorme, por la IA, y subrayó que la diferencia fundamental radica en el grado de transformación digital previo de cada organización. "Las empresas que han avanzado en su migración a la nube, han ordenado sus datos y cuentan con una estrategia de ciberseguridad sólida parten con ventaja. Cuando existe deuda técnica o los datos están dispersos o fragmentados, la madurez necesaria para adoptar IA todavía no es suficiente", afirmó.

Además, señaló que los factores organizativos están impactando en el éxito de adopción de la IA más que los individuales, lo que ha permitido que la conversación con los clientes esté evolucionando. "La IA ya no se percibe solo como una transformación tecnológica, sino empresarial. Las compañías quieren identificar qué procesos pueden optimizar y cómo capturar valor de negocio".

El concepto de empresa frontera, impulsado por Microsoft, fue otro de los temas centrales del debate. Miguel Tabera, *head of AI employee experience* de Bravent, explicó que, tras

dos años centrados en el uso de un asistente como Microsoft Copilot, con un perfil más generalista, las organizaciones están entrando en una nueva etapa marcada por los agentes inteligentes. "Cuando parecía que todo empezaba a estabilizarse, llegó la revolución de los agentes, de la hiperautomatización y de la IA autónoma. No estamos volviendo a la casilla de salida; estamos pasando a una nueva fase", puntualizó. Según Tabera, muchas empresas ya han superado la primera etapa, basada en asistentes individuales orientados a la productividad, y comienzan a explorar ecosistemas de agentes especializados para departamentos, áreas de negocio o procesos concretos. "Existe mucha necesidad y muchos casos de uso con sentido, pero seguimos algo verdes en cuanto a agentes". Entre los sectores más avanzados citó *retail*, energía y construcción, aunque también destacó que las diferencias suelen darse entre departamentos más que entre industrias. "Nos hemos encontrado con equipos de finanzas o recursos humanos que han avanzado más que otros equipos dentro de las organizaciones".

> "La IA ya no se percibe solo como una transformación tecnológica, sino empresarial"
>
> **(Juan Ignacio Amorrortu)**

Datos, liderazgo y casos de uso

A la hora de iniciar un proyecto de IA, Jordi Herrero identificó tres elementos imprescindibles. El primero es la gestión del dato. "Hay que tener claro de dónde sale la información, qué permisos existen y qué controles, guardarraíles, se establecen para evitar que un asistente acceda a información que no debería y sacarla fuera de la empresa", explicó. "En definitiva, estructurar muy bien las instrucciones previas que ofrece a la inteligencia".

El segundo es la madurez organizativa. Para el directivo de NexTReT, la adopción de la IA requiere liderazgo, patrocinio y formación internas y métricas claras que permitan medir el impacto de los proyectos. "No basta con lanzar iniciativas. Hay que definir cómo se va a medir el éxito y quién lidera el cambio". Finalmente, defendió la necesidad de priorizar casos de uso de alto retorno. "Es mejor empezar con proyectos pequeños que generen valor rápidamente y escalar después, en lugar de intentar abordar grandes transformaciones desde el principio".

En relación a las principales barreras para la adopción, Juan Ignacio Amorrortu, defendiendo una mínima madurez tecnológica para sacar partido a la IA, insistió en que la conversación ya no gira únicamente alrededor de la tecnología. "A los clientes les preocupa cuánto tiempo van a ahorrar, cuánto menos les va a costar o cuánto más van a

vender, lo que desemboca en cuál es el caso de uso con el que se tiene que empezar y cuál es la estrategia a largo plazo". En el fondo, recalcó, es una revolución empresarial. "No estamos hablando de una herramienta más. Estamos en los primeros pasos de una transformación que redefinirá industrias, la vida y la sociedad". Por ello, considera que las organizaciones, en una primera fase, están centradas en validar el retorno de las primeras iniciativas. A largo plazo, asegura que todas las empresas tendrán una IA; el reto será "cómo las empresas aprovechan esas nuevas capacidades mejor que sus competidores".

Del asistente al agente

La evolución desde los asistentes de IA hacia los agentes autónomos es una de las grandes tendencias que están observando los *partners* de Microsoft. Miguel Tabera explicó que muchas empresas ya han identificado los casos de uso donde los agentes pueden aportar valor, pero existe un desfase entre la velocidad que demandan los usuarios y el ritmo al que las organizaciones pueden desplegarlos de forma segura. "Los usuarios quieren trabajar con agentes porque los utilizan en su vida personal y tienen claro para qué lo necesitan, pero las empresas tienen que resolver antes cuestiones relacionadas con la gobernanza, la seguridad y la gestión del dato; retos que los usuarios no perciben", indicó. Esa situación está provocando la aparición de fenómenos de *shadow IT*. "Hemos detectado muchísimos agentes en la sombra

donde se están compartiendo datos o información que no se debe", advirtió.

Por su parte, Jordi Herrero cree que ya se ha pasado la fase de qué hace la IA a ver cómo puede aportar valor real a la compañía y considera que el salto hacia los agentes está siendo posible gracias a la evolución de los modelos de IA. "Hace dos años muchas de estas capacidades simplemente no existían. Hoy los modelos de razonamiento permiten construir soluciones mucho más avanzadas y útiles para las organizaciones". La evolución es continua: según datos de Microsoft, en el mundo, en el último año se ha multiplicado por 15 en las empresas los agentes y en las grandes empresas un 18.

Formación: mucho más que enseñar a usar una herramienta

La formación es esencial. El informe también deja claro que el entusiasmo por la IA debe venir acompañado de preparación. Mientras que el 63 % de los directivos españoles está familiarizado o muy familiarizado con los agentes de IA, sólo el 32 % de los empleados dice lo mismo. Miguel Tabera defendió que los programas de formación tradicionales ya no son suficientes. "El modelo clásico de implantar una herramienta y ofrecer unas sesiones formativas ya no funciona con la IA generativa, ya que implica cambiar la forma en la que trabajamos. Exige un acompañamiento y procesos de adopción largo; no vale con formaciones puntuales ni tradicionales", aseguró. "Hablamos de programas de seis meses o un año, con sesiones prácticas, análisis de escenarios reales, aprendizaje de *prompting* y seguimiento constante de los usuarios; que hacen que el uso de la IA se incremente en las organizaciones en las que pasan por un proceso así".

> "Muchas empresas ya han identificado los casos de uso donde los agentes pueden aportar valor"
>
> **(Miguel Tabera)**

Además, destacó que estos procesos deben involucrar tanto a empleados como a directivos. "Cuando ambos aprenden juntos surgen dinámicas muy enriquecedoras".

Para Juan Ignacio Amorrortu, la llegada de la IA supone una redefinición de las habilidades profesionales. "Las competencias claves ya no son aprender a utilizar una herramienta concreta. Hablamos de pensamiento crítico, creatividad, conocimiento del negocio y capacidad para colaborar con trabajadores agénticos", afirmó.

En este nuevo escenario, el papel de las personas será supervisar, validar y combinar a los trabajadores agénticos con los trabajadores humanos, garantizando que los resultados generados sean fiables y útiles para la organización. "Si lo enfocamos desde la perspectiva únicamente tecnológica y no conside-

ramos la gestión del cambio y su dimensión humana, no alcanzaremos el objetivo".

Copilot Cowork: productividad personal con impacto organizativo

La evolución de Copilot Cowork también ocupó parte de la conversación. Jordi Herrero lo definió como una herramienta de productividad personal que puede acelerar la adopción cultural de la IA dentro de las empresas. "El profesional del futuro tiene que tener conocimiento de IA y las empresas buscarán profesionales que sepan de esta tecnología, tengan un pensamiento crítico y extraigan resultados".

Miguel Tabera destacó el impacto que ya está teniendo dentro de Bravent. "Nos ha supuesto un salto enorme en productividad porque permite gestionar procesos completos, no solo resolver tareas puntuales. Puedes iniciar, por ejemplo, una campaña de marketing y recibir acompañamiento durante todo el proceso". Además, valoró que estas capacidades se desarrollen dentro del ecosistema de seguridad interno, controlado, algo que considera diferencial frente a otras soluciones del mercado.

IA y ciberseguridad

La mesa redonda concluyó abordando uno de los grandes desafíos de esta nueva etapa: la seguridad. Juan Ignacio Amorrortu recordó que las organizaciones deben proteger tanto los datos que alimentan los modelos como los propios agentes. Entre las amenazas emergentes citó ataques de *prompt injection*, envenenamiento de datos, abuso de modelos o riesgos derivados de conectores de terceros en la cadena de suministro. "Hay una nueva generación de ataques orientados a romper a los agentes que pueden tomar decisiones relevantes dentro de procesos críticos de negocio. Un fallo puede generar daños reputacionales, legales o económicos mucho más importantes que los de una aplicación tradicional", alertó. Por ello, defendió

que cualquier estrategia de adopción de IA debe desarrollarse de forma paralela a una estrategia específica de seguridad para la IA.