ISTOCK

IA EMPRESARIAL: EL OBSTÁCULO NO ES LA TECNOLOGÍA, ES LA GESTIÓN

Esta innovación aún se encuentra en una etapa muy temprana de adopción, si bien se espera que sea el motor de las economías en el futuro

IBERIA indra MERCADONA Supermercados de Confianza

Tecnología

Los baches de la IA en las empresas: el problema no está en la tecnología

Las empresas han invertido entre 30.000 y 40.000 millones de dólares en estas innovaciones, sin embargo, siete de los nueve grandes sectores económicos analizados por los expertos no muestran cambios estructurales

Miguel Terán Haughey

Podemos decir que el lanzamiento de ChatGPT al público de manera gratuita fue el inicio de la "Era de la Inteligencia Artificial", ya que fue la primera vez que esta nueva tecnología llegó a las manos de todo el mundo y se comenzó a entender qué era. Estos años ha logrado que nadie dude de las capacidades de la IA y de todo lo que puede hacer y, prácticamente, todo el mundo está de acuerdo en que una de las áreas donde más impacto va a tener es en el trabajo.

Esto es porque es la primera tecnología que tiene y puede replicar las capacidades humanas para realizar las tareas que tenemos que hacer en nuestro día a día. Sin embargo, la adopción de la IA en las empresas no está siendo un camino de rosas, por los problemas que hay a la hora de introducirla en los flujos de trabajo.

Según el informe *The GenAI Divide*, publicado por el MIT, las empresas han invertido entre 30.000 y 40.000 millones de dólares en estas innovaciones, sin embargo, siete de los nueve grandes sectores económicos analizados por los expertos no muestran cambios estructurales.

El problema, según señalan los investigadores, "no es la tecnología, que ya está lista para ser útil, sino la forma que tienen de implementarla las organizaciones" debido a la capacidad de aprendizaje y de adaptación de la tecnología en las empresas.

La mayor fuerza laboral, pero del futuro

Pero este no es el único reto que tiene esta tecnología para hacerse un hueco en el mercado, y es que, aunque pueda estar capacitada para realizar una labor, esta no es completamente fiable. El estudio realizado por Cloudera resalta esta idea, afirmando que el 96% de los responsables IT a nivel global aseguran que la IA está integrada en sus organizaciones, no obstante, solo el 9% reconoce que sus datos están preparados y son accesibles para tareas con esta tecnología.

La falta de regulación y vacíos legales también contribuyen a que las organizaciones pueden tardar más tiempo en adoptar soluciones IA. Esto se debe a que las organizaciones deben evaluar riesgos, adaptar procesos y superar barreras regulatorias internas como los procedimientos del cumplimiento normativo, sin olvidar que la Unión Europea es muy estricta en estas materias.

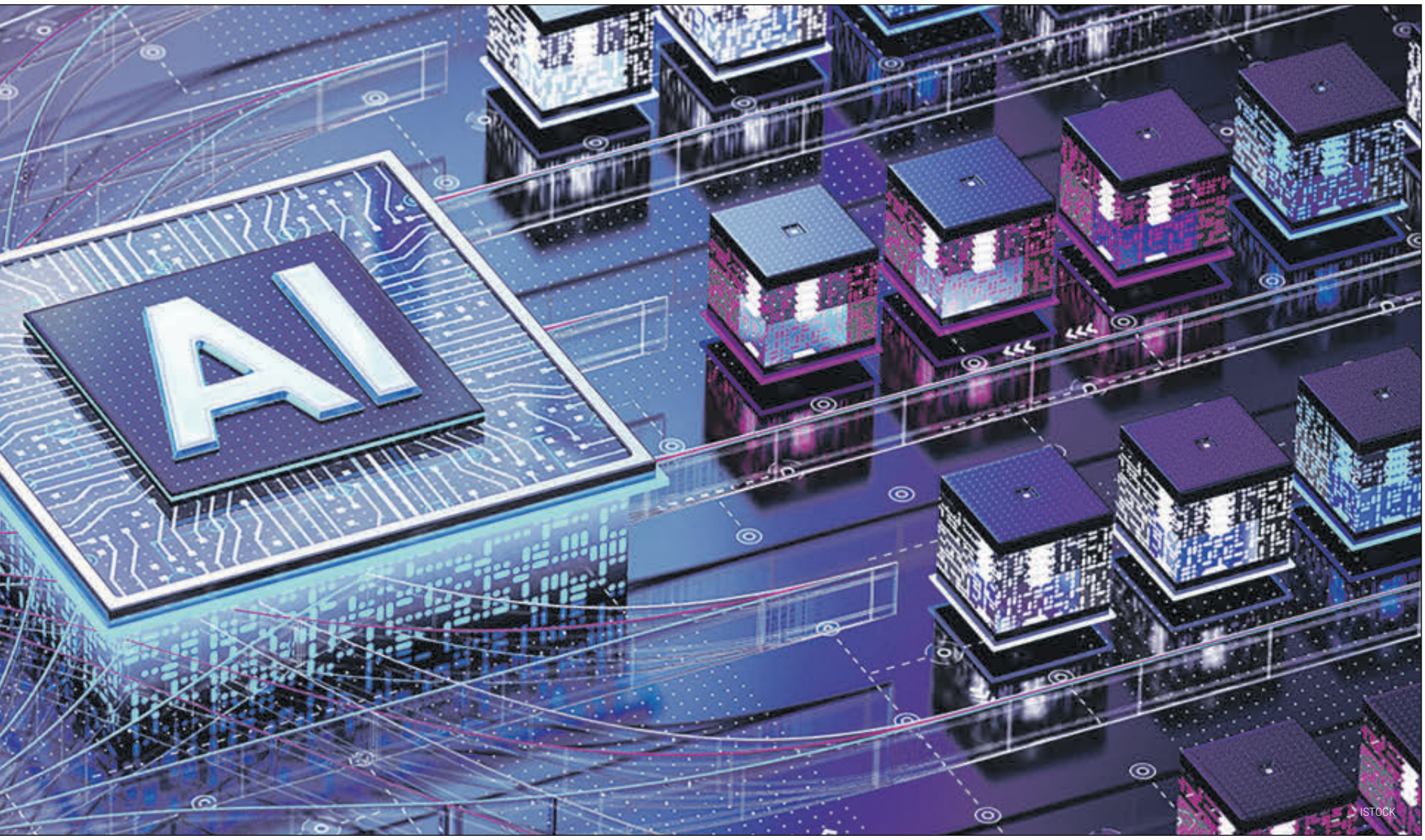
Aun así, no se puede negar (aunque se trate de esconder) que los empleados utilizan la IA en sus trabajos de diversas maneras. Pero el uso de esta tecnología no es lo que genera inquietud, sino que al no poder usar los servicios que las empresas están integrando porque no están preparadas, los trabajadores usan chatbots de IA generativa comunes como ChatGPT, Gemini o Microsoft Copilot.

A esto se le conoce como Shadow IA, una práctica que el 45% de los empleados de grandes empresas practica y que tiene como consecuencia que el 40 % de los documentos subidos a sitios de IA generativa contengan información sensible, según Layer X.

Esta práctica, que como decimos es cada vez más común, resulta en que estas plataformas de IA generativa son las responsables de, aproximadamente, el 14% de todas las fugas de datos de las empresas.

Esto supone un serio peligro para las organizaciones, sobre todo aquellas que tratan con datos sensibles y que pueden ser objetivo de ciberataques, además de que los informes señalan que más de la mitad de estas aplicaciones pueden ser manipuladas para ofrecer respuestas erróneas o problemáticas. "Esta situación subraya la necesidad de establecer marcos éticos y técnicos más sólidos en el diseño y despliegue de modelos generativos", señalan desde PaloAlto Networks.

"El hecho de que la gente las use de forma individual revela que aporta valor de verdad", defien-



ISTOCK

de Nacho Mateo, CEO del foro de innovación y emprendimiento South Summit. "Solo falta que esta tecnología se incorpore de forma segura en las empresas. Pero las corporaciones van a ser siempre muy cautas con eso, así que será un proceso lento".

Él mismo defiende que esta situación no significa para nada que la aplicación en estos primeros años haya sido un fracaso, sino que se trata de un proceso natural que ha ocurrido con numerosos avances tecnológicos en el pasado como con el *blockchain* o la realidad aumentada. "Al principio, todo el mundo invierte entusiasmado, luego la tecnología se va puliendo y se ve dónde es realmente útil".

Por otro lado, una de las primeras ideas y puntos a favor de la integración de la IA en el trabajo era que supondría la eliminación del "error humano", aunque no hay que olvidar que las máquinas también fallan.

Y a diferencia de las personas, la IA siempre cree que tiene razón y no duda de lo que dice o hace hasta que un humano le señala su fallo, por lo que la supervisión humana es más que necesaria, sobre todo en esta primera etapa de introducción en las empresas.

Por último, otro bache al que se están enfrentando las organizaciones con la IA es la huella medioambiental que tiene. Desde la ONU señalan que "a nivel mundial, la infraestructura relacionada con la IA pronto podría consumir seis veces más agua que Dinamarca, un país de 6 millones de habitantes". Un ejemplo que llama mucho la atención es que generar una imagen con IA tiene el coste energético comparable a cargar un *smartphone* en algunos modelos y el gasto de agua de entre 0,5 y 5 litros por imagen.

A parte del consumo de agua y el energético, el diseño y construcción de la infraestructura y los chips necesarios para impulsar la IA requieren el uso de elementos de tierras raras, que a menudo se extraen de formas destructivas para el medio ambiente. Lo que choca con los esfuerzos medioambientales que cada vez más empresas están llevando a cabo.

Pero lo cierto es que solo el 12% de los ejecutivos que utilizan IA generativa reconoce que su organización mide la huella medioambiental de su uso y, de hecho, únicamente el 38% afirma ser consciente de ese impacto medioambiental, que a medida que la adopción de esta tecnología crezca, va a ser cada vez más alto.

Esta situación choca con los esfuerzos medioambientales que cada vez más empresas están llevando a cabo, y se va a acabar convirtiendo en un caballo de Troya para estas mientras no se busquen soluciones más sostenibles.

El futuro es prometedor

Pese a todo lo que se ha avanzado, la IA todavía se encuentra en una etapa muy temprana de adopción en las empresas, y en general en el mundo, ya que para la mayoría de las personas sigue siendo una tecnología desconocida que ven como lejana.

Pero las ganas de introducirla en el día a día de las empresas lo antes posible, a pesar de que todavía no está dando resultados, señala la clara apuesta por la IA y la confianza en que va a ser el motor de las economías de cara al futuro.

Las inversiones en IA por parte de las empresas no dejan de crecer, el informe publicado por Capgemini señala que, en los últimos 12 meses, nueve de cada 10 organizaciones han aumentado la inversión en Gen AI y de esas un 79% está satisfecha con los resultados obtenidos hasta el momento.

Este mismo estudio ha descubierto a su vez que seis de cada 10 organizaciones esperan que la IA

> Solo el 9% de las empresas reconoce que sus datos están preparados y son accesibles para tareas con esta tecnología

sea un miembro activo del equipo o supervise a otras IA en los próximos 12 meses a medida que los trabajadores reciban la formación y herramientas necesarias para hacerlo, al mismo tiempo que la IA se desarrolle y esté mejor adaptada a las necesidades de esto.

Y todavía queda el plato fuerte por venir, ya que cada vez estamos más cerca de las IA General (AGI), que supone un paso más hacia delante al ser una IA que tendría la capacidad de comprender, aprender y aplicar conocimientos en una amplia variedad de tareas a un nivel comparable al de un ser humano, es decir, que pudiera razonar, resolver problemas e incluso transferir conocimientos, lo que elevaría todavía más las capacidades y potencial de esta tecnología.

Cada vez más investigaciones señalan que estamos más cerca de alcanzarla, como la prueba que OpenAI, empresa creadora de ChatGPT, elaboró llamada GPDval, un test que evalúa lo cerca que está la IA actual de convertirse en AGI.

Este examen hace el cálculo en base a la cantidad de trabajos en los que la IA ya supera a los humanos. Durante este, se pusieron a prueba hasta 44 profesiones de nueve sectores diferentes como farmacéuticos, periodistas, abogados, programadores, asistentes sociales y vendedores, entre otros.

Según los resultados publicados por la compañía, la IA ya nos iguala o supera en el 49% de las 44 profesiones estudiadas. En los casos en los que la máquina saca una puntuación de 50% o superior, quiere decir que la IA realiza un trabajo igual o mejor que el humano en la mayoría de las tareas a las que se le expuso, pero lo cierto es que solo tres labores (gestión de proyectos, desarrollo de *software* y producción y dirección de contenidos audiovisuales) superaron este umbral.

Ferran García Rigau Responsable del Centro de Excelencia de Datos e Inteligencia Artificial en Iberia

"La IA generativa nos ha permitido llegar mejor a nuestros clientes"

"A través de los datos queremos crear casos de uso de IA en todas las áreas de la compañía"

"Los datos nos dieron seguridad y nos ayudaron a saber cómo debíamos avanzar"

"A nivel interno, la IA generativa nos ha ayudado a aumentar la productividad y la creatividad"

EcoBrands MADRID

El sector aéreo se enfrenta a retos relacionados tanto con la tecnología como con la sostenibilidad, lo que se traduce en competitividad. En este contexto, Iberia se ha posicionado como una de las aerolíneas más fuertes del mercado, llevando a cabo proyectos innovadores. Ejemplo de ello, es la utilización de la inteligencia artificial generativa para hacer frente a la obsolescencia de la flota, mejorar la calidad del servicio a los clientes o ser más respetuosa con el medioambiente.

¿En qué consiste su puesto? ¿Qué aporta su perfil en una compañía como Iberia?
Soy el responsable del Centro de Excelencia de Datos e Inteligencia Artificial de Iberia, en el que tenemos dos objetivos principales: tener una plataforma moderna de datos que centralice una única fuente de datos de la compañía, con todos los KPIs principales para medir nuestra actividad; y la segunda es, a través de estos datos, crear casos de uso de IA en todas las áreas de la compañía, desde la operación hasta la experiencia de cliente, para ayudar en la transformación de Iberia.

¿Qué tipo de proyectos y actividades desarrolla en su departamento?
En el primer ámbito, son proyectos de gobierno del dato y organización de la información, con creación de reportes y herramientas de ayuda a la decisión. Y en el segundo es esencialmente crear modelos de Inteligencia Artificial.

¿Cómo ha evolucionado el área de datos en Iberia desde que se empezó a aplicar la inteligencia artificial? ¿Cuál fue el punto de inflexión para dar el paso?
En 2019 creamos el Centro de Excelencia de Datos como parte de nuestro plan de transformación. Un punto de inflexión muy relevante fue la pandemia, que ocurrió al año de haber creado este centro, y los datos nos dieron seguridad y nos ayudaron a saber cómo debíamos avanzar. Esto nos confirmó que la creación de este departamento había sido un acierto y seguimos invirtiendo en él según nos fuimos recuperando después de la pandemia.

En Iberia continúan reinventándose. De hecho, hace poco implantaron la IA generativa. ¿En qué ha consistido este proceso? ¿Cómo se está materializando esta innovación en la práctica?
En Iberia llevamos invirtiendo en Inteligencia Artificial desde 2019. Cuando empezamos a invertir en la IA generativa, teníamos ya más de 50 modelos en producción. Pero es cierto que la IA generativa nos ha permitido llegar mejor a nuestros clientes, con soluciones como el asistente que tenemos en nuestra web y en el canal de WhatsApp. A nivel interno, nos ha ayudado a democratizar el uso de la generativa también por parte de nuestros empleados para aumentar la productividad, la creatividad y la reducción del temor al uso de esta tecnología con tanto potencial.

E.E

Iberia utiliza la IA para optimizar la distribución del peso de la bodega y reducir así el consumo. E.E

Los clientes son el motor de la compañía. ¿Cómo ha cambiado la relación con ellos gracias al uso de la IA y de los datos?
Hasta la irrupción de la IA generativa lo más relevante que hacíamos con los clientes a través del dato y la IA era la personalización. Por un lado, entender lo que quieren nuestros clientes a través de las casi 300.000 encuestas que rellenan nuestros clientes anualmente y también hacer que su experiencia digital fuera más personalizada. Con la IA generativa hemos podido ir un paso más allá porque con la experiencia conversacional el nivel de personalización es mucho mayor. Por ejemplo, el nuevo asistente de nuestra web recomienda destinos, nos ayuda a planificar viajes y hace la búsqueda de vuelos mucho más dinámica.

Uno de los retos actuales del sector aéreo es reducir el desperdicio alimentario a bordo. ¿Cómo está ayudando la inteligencia artificial a conseguirlo en Iberia?
Sí, en este caso usamos el dato en tiempo real y esperamos casi al último minuto para cargar los menús imprescindibles. Por un lado, evitamos desperdiciar comida que no se consume y, por otro, es peso que no se carga en el avión y se reduce el consumo de combustible. Además, en los vuelos de largo radio, cuando sobra comida, nuestras tripulaciones ofrecen a los clientes la posibilidad de repetir para evitar ese desperdicio alimentario, ya que esos menús habría que tirarlos.

Además, también es uno sobre los que más se ejerce la presión medioambiental, ¿cómo contribuyen los datos y la IA a la sostenibilidad de la compañía?
La IA nos ayuda a optimizar la manera en la que llenamos nuestros aviones. Utilizamos la IA para asignar asientos a todos nuestros clientes, teniendo en cuenta por un lado sus preferencias y por el otro el balanceo óptimo del avión. Lo ajustamos también con el peso de la bodega en función de las maletas o las mercancías que llevemos en cada vuelo. Este proceso optimiza el centrado del avión en cada vuelo y prácticamente en tiempo real para tener en cuenta cualquier cambio de último minuto. Esto se traduce en una reducción de combustible y, por lo tanto, en menos emisiones y una operativa más sostenible.

"El nuevo asistente recomienda destinos y nos ayuda a planificar viajes"

"Para reducir el desperdicio alimentario usamos el dato en tiempo real para los menús"

"Integrar la IA en todas las áreas operativas garantiza que los sistemas sean robustos"

¿Qué casos de éxito podría compartir que haya ayudado a Iberia a ser más eficiente, ya sea en la operativa o en la gestión de la flota?
Un caso de éxito es el uso del dato para optimizar el reparto de nuestra flota. Es una especie de Tetris que nos ayuda a decidir qué avión mandamos a qué ruta. En Iberia hacemos un seguimiento continuo de la demanda de nuestras rutas para adaptar el tipo de avión a lo que necesita cada una, ya sea por un aumento de demanda, por una cancelación o por un problema con la meteorología. Si, por ejemplo, tenemos que cancelar un vuelo (por causas técnicas o de meteorología), cambiamos el tipo de avión por uno más grande para tratar de regularizar esos traslados lo antes posible. Es una especie de sudoku continuo con el que tratamos de mejorar al máximo la operativa de cada día en tiempo real. Otro ejemplo llamativo es que predecimos en tiempo real posibles pérdidas de conexión de nuestros clientes en función del estado de sus vuelos, pero también de las características de su conexión. Así, si vemos que podrían tener riesgo de perder esa conexión, les buscamos una solución de forma proactiva y anticipada para minimizar la incertidumbre que ellos podrían sufrir.

En una compañía tan grande como Iberia, ¿cuáles diría que son los mayores retos que se ha encontrado?
En una compañía tan grande como Iberia, uno de los mayores retos está siendo la adopción a gran escala de la inteligencia artificial generativa. La transformación digital implica cambiar procesos y mentalidades, lo que requiere una labor importante de formación y sensibilización dentro de la organización. Además, la integración de la IA en todas las áreas operativas supone garantizar que los sistemas sean robustos, seguros y capaces de adaptarse en tiempo real a las necesidades cambiantes de nuestra operativa diaria.

¿Podría adelantarnos cuál será el siguiente paso que decida Iberia en materia de IA?
En Iberia estamos en constante análisis de las novedades y tendencias del mercado en materia de inteligencia artificial, porque somos conscientes de que el sector evoluciona a gran velocidad. Nos gustaría seguir potenciando aún más la integración de la IA generativa en áreas clave de nuestra operativa, con el objetivo de mejorar la eficiencia y la experiencia de viaje de nuestros clientes.

Tecnología

España registra, de media, 1.951 ciberataques a la semana. EE

La educación, los gobiernos y la sanidad lideran los ciberataques

En España, según datos del Instituto Nacional de Ciberseguridad, se registraron 42.136 casos de 'malware', incluyendo virus y otros 'softwares' maliciosos que afectan a dispositivos. De estos, 357 fueron ataques de 'ransomware', donde los ciberdelincuentes bloquean sistemas o archivos, exigiendo rescates económicos

Judith Arrillaga Pérez

España registra, de media, 1.951 ciberataques a la semana, lo que supone un incremento del 1% con respecto al año anterior y confirma el panorama global de amenazas continúa en niveles históricamente elevados, según datos de Check Point.

Y aunque no hay ningún sector ni empresa que sea inmune a esta clase de ataques, sí que existen unas industrias más atacadas que otras. "La tendencia está en que aquellos sectores con más usuarios son los que reciben más ataques", explica a elEconomisa.es Eusebio Nieva, director técnico de Check Point Software para España y Portugal. El *ranking* lo lideran la educación, las instituciones públicas y la sanidad. "El sector de la educación es uno de los más atacados porque es de los que más usuarios tiene, el gubernamental es otro de los más afectados. Pero el resto de los sectores no pueden decir que no están siendo atacados porque todos tienen un nivel bastante alto de frecuencias de ataque", apunta el experto.

Hay otro factor que explica la popularidad de unos sectores por encima de otros: la información que manejan. "Uno de los más atacados tradicionalmente es el financiero porque tiene algo que todo el mundo quiere: dinero".

En una línea muy similar se pronuncia José de la Cruz, director técnico de Trend Micro, que alerta de la alta exposición que sufren los sectores público, sanitario e industrial. "Estos sectores manejan información altamente confidencial, a menudo de carácter personal y sujeta a estrictas regulaciones. Este tipo de datos resulta especialmente valioso para los atacantes, ya que puede ser aprovechado en fases posteriores del ataque, como la extorsión o los movimientos laterales dentro de la red comprometida", detalla a este medio.

Evolución de los ataques

El año pasado, en España, según datos del Instituto Nacional de Ciberseguridad, se registraron 42.136 casos de *malware*, incluyendo virus y otros *softwares* maliciosos que afectan a dispositivos. De estos, 357 fueron ataques de *ransomware*, donde los ciberdelincuentes bloquean sistemas o archivos, exigiendo rescates económicos. El fraude online, con más de 38.000 incidentes, representó el 43,2% del total. El phishing lidera esta categoría con 21.571 casos, como correos falsos simulando ser bancos o empresas conocidas para robar datos personales. Además, se identificaron 7.470 intrusiones e intentos de acceso no autorizados a información de redes o sistemas informáticos de empresas y hogares, como el hackeo de una red doméstica que expone datos familiares.

"El *ransomware* continúa encabezando la lista de los ataques más comunes, debido a su alta probabilidad de éxito y gran rentabilidad económica para los ciberdelincuentes. Cabe destacar que el *ransomware* ha evolucionado notablemente. Ha pasado de ser un simple tipo de ataque a convertirse en una campaña de *hacking* avanzada, donde los atacantes combinan múltiples vectores de intrusión con técnicas cada vez más sofisticadas", argumenta el experto de Trend Micro.

El *phishing* ha sido, tradicionalmente, el tipo de ataque más utilizado. Este consiste en engañar al usuario para que instale algo malicioso o que pinche en un enlace que lleva a una página web que intenta robar sus credenciales. Sin embargo, esto está cambiando. "Esto se ha equilibrado hacia el aprovechamiento que hacen de las vulnerabilidades existentes en el *software*. Por eso insistimos en la necesidad que hay de parchear los sistemas, es fundamental para no caer en este ataque que cada vez es más habitual. Eso sí, una vez dentro de los sistemas, el *ransomware* sigue siendo el más habitual", apunta a este respecto el experto de Check Point.

En septiembre se denunciaron públicamente 562 ataques de *ransomware* en todo el mundo, lo que representa un aumento interanual del 46%. Norteamérica volvió a ser la región más afectada, concentrando el 54% de los casos registrados, la mayoría de ellos en Estados Unidos (52% del total global). En segundo lugar, se situó Europa, que representó casi una quinta parte de los incidentes (19%), mientras que Corea del Sur y Reino Unido registraron un 5% y un 4%, respectivamente.

> En septiembre se denunciaron públicamente 562 ataques de 'ransomware' en todo el mundo

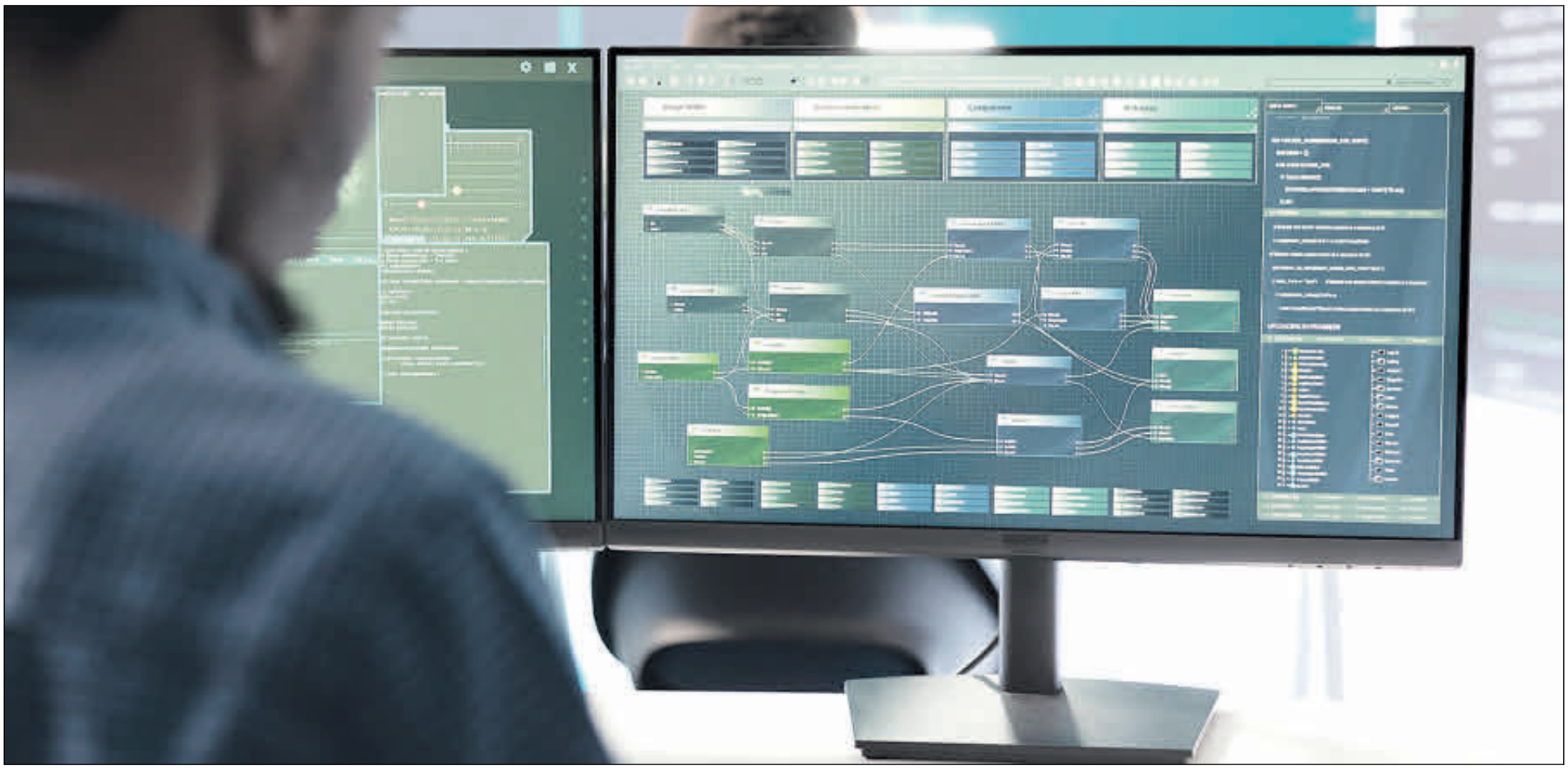
La IA, ¿amigo o enemigo?

La irrupción de la inteligencia artificial está provocando una revolución en el sector de la ciberseguridad. Por un lado, ha mejorado los sistemas de defensa de las empresas, pero por otro, también ha sofisticado los ataques que sufren. "Se ha convertido en una herramienta de doble filo dentro del ámbito de la ciberseguridad. Por un lado, los ciberdelincuentes la emplean para optimizar y sofisticar sus ataques. Por otro lado, los fabricantes de soluciones de seguridad también se apoyan en esta tecnología para desarrollar un modelo de defensa proactiva, capaz de anticipar, detectar y bloquear amenazas antes de que causen impacto", explica el representante de Trend Micro.

También hay que tener en cuenta que existen dos tipos de inteligencia artificial, la IA Generativa y la IA Discriminativa. "Esta última es capaz de hacer diagnósticos, diferenciar si algo es bueno o malo. La estamos utilizando desde hace muchísimos años y es una de nuestras grandes bazas contra los atacantes", añade. "Estamos viendo que para refinar esos ataques están usando todas esas inteligencias artificiales regenerativas para que sean más verosímiles", denuncia el experto de Check Point.

El mejor ejemplo de ello es lo que se llama la estafa del CEO que tiene como objetivo engañar a empleados que tienen acceso a los recursos económicos de la empresa para que paguen una factura falsa o haga una transferencia desde la cuenta de la compañía. Un estafador llama o envía correos electrónicos haciéndose pasar por un alto cargo de la compañía.

"Hay casos en los que se ha utilizado la falsificación de imágenes, de voz o de vídeo. En una ocasión, un empleado se vio en una videoconferencia para una adquisición de una compañía con todos sus jefes. Y luego se descubrió que todos los integrantes de esa videollamada estaban creados con inteligencia de efectivo o estaban falsificados", detalla Nieva.



La tasa de empresas víctimas del cibercrimen ronda el 23%. EE

Un tercio de las pymes españolas temen cerrar si sufren un fraude digital

La ciberdelincuencia no es solo una amenaza para la economía de una empresa, sino también para su supervivencia. De hecho, para las pymes un ataque de este calibre puede llegar a tener un coste medio de hasta 75.000 euros, sin contar lo daños colaterales, como la pérdida de clientes

María Juárez

Los ciberataques parecen cosa de las películas; pero es que una de cuatro pymes ha sido víctima de uno de estos ataques, según el nuevo estudio de Mastercard, realizado a más 1.800 empresarios de pymes en Europa. Por ello, un tercio de las pymes españolas temen cerrar sus negocios si sufren un fraude digital. Actualmente, y como señala el informe, la tasa de empresas víctimas de estafadores ronda el 23%, por debajo de la media europea, ya que países como Irlanda, Dinamarca y Francia superan el 30%.

La ciberdelincuencia no es solo una amenaza para la supervivencia de las empresas, sino que también pone en riesgo la expansión del negocio. "En pymes vemos cinco vectores de ataque dominantes: *phishing/BEC, ransomware*, fuga de datos por terceros, robo de credenciales y fraudes de pago (suplantación en cadena de suministro)", expresa Manuel Huerta, CEO de Lazarus. De hecho, casi el 70% de los emprendedores españoles alegan que el miedo a un posible fraude les hace ser cautelosos a la hora de crecer.

En España, la ciberseguridad supone uno de los mayores retos para las pymes. Y es que no es de extrañar pues tiene grandes consecuencias, como, por ejemplo, la pérdida de clientes tras una estafa, algo que han vivido el 7% de estas empresas, o la pérdida de dinero, sufrida por el 13%. En relación con esto, la compañía tecnológica Zerod considera la ciberseguridad "una necesidad" para el tejido empresarial. Según sus datos, las campañas de *phishing* aumentaron en España un 35% durante 2024 respecto al año anterior, lo que podría elevar los costes derivados de los ciberataques por encima de los 20.000 millones de euros anuales de cara a 2025. Una cifra que, alertan desde la empresa, "subraya la gravedad del problema". Es interesante destacar que esta preocupación aumenta en las generaciones más jóvenes. Tal y como demuestra el informe de Mastercard, el 36% de los empresarios de la *Generación Z* se preocupa a diario por ser víctima de la ciberdelincuencia, frente al 27% de los *millennials* y el 25% de la generación *BabyBoom*.

Otro de los grandes problemas a los que se enfrentan las pymes es cómo protegerse. "El modelo de ciberseguridad recomendado debe apoyarse en múltiples frentes: protección de dispositivos *(endpoint)*, seguridad en redes y comunicaciones, seguridad en el diseño de aplicaciones y una gestión sólida de identidades", comenta Martín Brea, *cofounder* de Darkdata. Y añade que "a estas capas se suman las copias de seguridad, fundamentales para garantizar la recuperación ante ataques como el *ransomware*; las simulaciones de ataques; y la formación del personal. La combinación de estas medidas reduce el riesgo".

> Las campañas de 'phishing' han aumentado en España un 35% durante 2024 respecto al año anterior

Huerta puntualiza que "las pymes más vulnerables son las de sectores como sanidad, legal, educación o logística, especialmente si están digitalizadas, pero sin medidas de ciberseguridad. También las que usan servicios en la nube sin configuraciones seguras, no tienen políticas internas ni responsables de TI, y dependen de herramientas como WhatsApp o correos personales para su operativa diaria".

¿Cuál es el coste?

"La mayoría de las pymes no aguantarían ni 48 horas sin sistemas. Algunas, ni 8 horas. Y lo más grave: muchas tardarían días en detectar el ataque. Hoy, el tiempo de reacción lo es todo, y sin monitorización ni protocolos claros, el daño crece por minutos", decreta el directivo de Lazarus. Para las pymes un ataque de este calibre puede llegar a tener un coste medio de hasta 75.000 euros.

Ahora bien, esto no queda aquí y a esta cifra hay que sumarle los daños colaterales, como la pérdida de clientes y de confianza, así como el deterioro de la reputación corporativa que conlleva una brecha de seguridad. "Un *ransomware* con exfiltración y parada operativa puede ser existencial para una pyme: no solo por el rescate, sino por sanciones, pérdida de clientes y ruptura de la cadena de cobro", explica Huerta.

En España, según datos de Ayesa, proveedor global de servicios de tecnología e ingeniería, cerca del 80% de las pymes presentan una alta vulnerabilidad frente a las amenazas digitales. La causa principal es la falta de sistemas preventivos sólidos que permitan anticipar o mitigar este tipo de riesgos. Ante este nuevo escenario la administración pública también juega un papel de protección. "Organismos como el Centro Criptológico Nacional y el INCIBE-CERT ya realizan una labor destacada", dice Brea y añade que "actualmente ya existen organismos que desempeñan un papel clave en el cumplimiento normativo en ciberseguridad, impulsando marcos regulatorios como NIS2, DORA, MiCA, la Ley PIC y la normativa de Protección de Datos. Estas regulaciones establecen estándares para la gestión de riesgos, resiliencia operativa y protección de infraestructuras críticas, obligando a las empresas a adoptar medidas robustas".

Tecnología

Cibercrimen para 'dummies': así se puede delinquir sin ser profesional

En una era en la que se puede pagar por casi todo, el ciberdelito no es una excepción. Gracias al 'Crimen as a Services', prácticamente cualquiera puede perpetrar un ciberdelito por menos de 100 euros y sin tener conocimientos para ello

Isabel Gaspar

El pasado mes de octubre se conocía que la Guardia Civil había desarticulado una red de *phishing* (ciberataque en el que los delincuentes se hacen pasar por una entidad de confianza) que ha causado millones de euros en pérdidas y cientos de denuncias. Si bien esta es una noticia lamentablemente recurrente, una de las particulares de este caso, cuyo cerebro es un joven brasileño de 25 años, es que operaba a través de un modelo *Crime as a Service* (CaaS).

En tecnología el concepto *as a Service* hace referencia al pago por servicio, similar, por ejemplo, a alquilar una casa para las vacaciones o un coche para un viaje. Y eso es, precisamente, lo que se hace con el modelo CaaS, pagar por servicios para delinquir. "Surge porque el cibercrimen se ha profesionalizado y los criminales están buscando nuevas maneras de monetizar su conocimiento. Por ello, ha aparecido este tipo de servicios en la *Dark Web* que ofrecen herramientas listas para usar, igual que un *software* comercial. Por ejemplo, por menos de 100 euros se pueden comprar kits de *ransomware* o bases de datos robadas", señala Andrés de Benito, director y responsable de Ciberseguridad de Capgemini en España.

En otras palabras, prácticamente cualquiera puede perpetrar un ciberdelito. Esta es, justamente, la clave del éxito de este modelo. Ya no es necesario tener los conocimientos suficientes para lanzar ciberataques, democratizando el acceso al cibercrimen. Como subraya Eusebio Nieva, director técnico para España y Portugal en Check Point Software, "los atacantes ya no necesitan ser expertos técnicos: pueden comprar, alquilar o suscribirse a servicios listos para usar, como rans*omware*, kits de *phishing* o *botnets*. Esta modalidad, reduce las barreras de entrada y aumenta el alcance y la frecuencia de los ataques".

A este respecto, el CaaS se está convirtiendo en uno de los principales motores del crecimiento del cibercrimen global. Si bien no existen datos exactos, los expertos consultados coinciden en que este negocio está en continua expansión y es el motor de la industrialización del cibercrimen, moviendo miles de millones de euros al año. "El auge de plataformas de *Ransomware as a Service* (RaaS) o *Phishing as a Service* (PhaaS), junto con la automatización de procesos, tecnologías como la inteligencia artificial o el uso de criptomonedas para el pago anónimo, han facilitado una expansión muy rápida del CaaS. En la práctica, estamos ante un ecosistema maduro, comparable en escala y sofisticación al de las empresas legítimas y estables, pero orientado al delito", reconoce Antonio Villalón, *Chief Security Officer* en S2GRUPO.

En este sentido, según las estimaciones de NTT Data, el coste económico global del cibercrimen alcanzará un récord de 10,5 billones de dólares anuales este 2025, un 15% más que el año anterior. "Lo significativo es que gran parte de este valor se genera explotando precisamente la vulnerabilidad de los datos en tránsito, donde las intercepciones pueden pasar completamente desapercibidas durante meses o años", indica Vanesa Díaz, CEO de LuxQuanta. Algunos análisis sugieren que el cibercrimen mueve más dinero que el tráfico de drogas, armas y trata de personas juntos.

Y en estas cifras es clave el CaaS, puesto que está permitiendo que el acceso a este mercado sea más fácil que nunca.

En palabras de Doris Seedorf, CEO de Softtek para España, hoy en día los ataques "responden a una estructura empresarial bien definida. Existen desarrolladores que crean el *software* malicioso, distribuidores que lo comercializan y afiliados que lo ejecutan contra las víctimas. Este sistema modular permite que los ataques se multipliquen con facilidad y que los delincuentes mantengan su anonimato".

Como explica esta experta, uno de los ejemplos más conocidos en este campo es el de los grupos de RaaS, como LockBit, que alquilan su infraestructura a terceros a cambio de una parte del rescate pagado por las víctimas. Según Europol, el CaaS ha aumentado la frecuencia de ataques de *ransomware* en más de un 30% en los últimos años.

Los desarrolladores de *ransomware*, también llamados operadores RaaS o grupos RaaS, desarrollan y mantienen las herramientas y la infraestructura del *ransomware*. Agrupan sus herramientas y servicios en kits RaaS que venden a otros hackers, conocidos como afiliados RaaS.

Según explica IBM, la mayoría de los operadores de RaaS utilizan uno de estos modelos de ingresos para vender sus kits: la suscripción mensual, pagando una cuota periódica que puede ser tan baja como 40 dólares al mes; la tarifa única para comprar el código *ransomware* directamente; los programas de afiliados en los que se paga una cuota mensual y se comparte un pequeño porcentaje de los pagos del rescate; y el reparto de beneficios, por el que los operadores no cobran nada por adelantado, pero se llevan una parte importante de cada rescate que recibe el afiliado, a menudo entre el 30% y el 40%.

En el caso del *Phishing como Servicio*, los precios, por un pago único, pueden oscilar de 25 a 50 dólares por plantillas básicas para imitar marcas conocidas, a entre 200 y 900 dólares por páginas más convincentes, que evaden mejor los sistemas de detección y, a veces, cuentan con soporte técnico, según Kaspersky.

Una de las mayores plataformas de PhaaS, desarticulada el año pasado en una acción internacional conjunta, fue LabHost. De media, por un pago mensual de 249 dólares, los afiliados tenían acceso a una plataforma personalizable con más de 170 plantillas de sitios web falsos que imitaban a bancos, servicios postales y empresas de telecomunicaciones. Se estima que facilitó el robo de más de un millón de credenciales de usuario y cerca de 500.000 tarjetas de crédito.

Así, a diferencia de otro tipo de ataques, el cibercrimen como servicio "es un modelo más accesible, escalable y profesionalizado, funcionando como una plataforma donde distintos servicios criminales se venden o alquilan a terceros, algo que no ocurre en ciberataques más aislados o hechos por actores con recursos limitados. Además, el CaaS tiende a operar con estructuras empresariales clandestinas más organizadas, con soporte al cliente/delincuente, pagos en criptomonedas y marketing tanto dentro de la *Dark Web* como en foros en la web abierta, a diferencia de los ataques independientes o improvisados de otros cibercriminales", sostiene Josep Albors, director de Investigación y Concienciación de ESET España.

Por su parte, Andrés de Benito recuerda que "este modelo de negocio exige de una profesionalización importante, viéndose en este mercado que estas "empresas" ofrecen al final características muy similares a las de otras empresas legales, tales como soporte técnico, con atención al cliente y programas de afiliación incluidos".

Todos los expertos consultados por este medio coinciden: la gran ventaja del CaaS para los delincuentes es la accesibilidad, la escalabilidad, el bajo riesgo, el anonimato y la alta rentabilidad.

Más ataques y más sofisticados

Los datos son el activo de más valor para el crimen y si hay organizaciones donde abundan los datos esas son las empresas. Según el Índice Global de Amenazas del mes de septiembre, elaborado por *Check Point Research*, las organizaciones de todo el mundo se enfrentaron a una media de 1.900 ciberataques semanales por compañía. En el caso de España, las compañías sufrieron 1.951 ataques semanales de media, un 7% más que en el mismo mes de 2024.

> Sólo el 6% de las empresas se ve preparada para combatir todas las amenazas del cibercrimen

A este respecto, este modelo de cibercrimen supone una importante amenaza a nivel empresarial. "Las empresas ya no se enfrentan a atacantes individuales, sino a ecosistemas criminales completos, automatizados y globalizados. Esto implica que los ataques son más constantes, más sofisticados y difíciles de atribuir", apunta Eusebio Nieva. Además, como recalca Josep Albors, "la profesionalización y especialización de estos servicios criminales permite ataques más efectivos, rápidos y con mejor soporte técnico que pueden llegar a evadir las defensas tradicionales".

Por tanto, tal y como sostiene Doris Seedorf, "las medidas tradicionales, como los antivirus o los cortafuegos, resultan insuficientes frente a amenazas que cambian de forma constantemente". Ante esto, Vanesa Díaz alerta también de que "mientras las organizaciones invierten en *firewalls* y antivirus, los atacantes explotan el eslabón más débil: el canal de comunicación desprotegido".

¿Qué se puede hacer al respecto? Andrés de Benito lo tiene claro: "Las empresas deben invertir más en detección temprana, inteligencia de amenazas y, como siempre, en capacitación del personal". En esta línea, Josep Albors indica que "la lucha eficaz exige anticipación, educación, tecnología y cooperación constante en un entorno dinámico y desafiante". A tenor de los datos recopilados por el estudio *Global Digital Trust Insights 2026*, de PwC, sólo el 6% de las empresas se ve preparada para combatir todas las vulnerabilidades en materia de ciberseguridad.

Para Antonio Villalón, enfrentarse al CaaS requiere una respuesta coordinada en tres niveles: tecnológico, organizativo y legislativo. A nivel tecnológico, es fundamental, "reforzar las capacidades de detección y neutralización para hacerlas más robustas y ágiles, por ejemplo, mediante inteligencia artificial o ciberinteligencia avanzada, entre otros". A nivel organizativo, hay que "garantizar la agilidad de la detección y la respuesta, lo que puede introducir cambios para engranar mejor a diferentes departamentos internos, o incluso puede implicar la contratación, o el refuerzo, de servicios externos especializados". Finalmente, en el ámbito legislativo, son indispensables leyes "que aborden el problema global, así como el refuerzo de la cooperación internacional para desmantelar las infraestructuras criminales y perseguir a los responsables". En su caso, Vanesa Díaz indica que el CaaS es "el síntoma definitivo de que la ciberseguridad tradicional ha alcanzado sus límites".

A todo ello, Doris Seedorf añade la formación y la concienciación de los usuarios. "En un mundo donde el crimen digital se ha convertido en un servicio más, la prevención y la información son las herramientas más poderosas para evitar ser la próxima víctima". Como recuerda Eusebio Nieva, "un 60% de los ataques están causados por una acción u omisión humana".

ISTOCK

Tecnología

Europa debe invertir 300.000 millones para lograr su soberanía tecnológica

El 80% de la infraestructura digital europea se basa en tecnologías importadas de otros países fuera de Europa. Por ello, para cambiar esta situación se invertirán 300.000 millones de euros en los próximos diez años

María Juárez

La inteligencia artificial (IA) y las nuevas tecnologías son un motor clave en la transformación en la economía de los países. El problema es que más del 80% de la infraestructura digital en Europa se sustenta en tecnologías importadas, lo que evidencia la urgencia de desarrollar un ecosistema de inteligencia artificial propio que fortalezca su autonomía digital y su capacidad competitiva. Es en este contexto en el que surge el EuroStack, creada por un consorcio de instituciones europeas, incluyendo la Bertelsmann Stiftung, CEPS y la UCL Institute for Innovation and Public Purpose. Esta es una iniciativa estratégica diseñada para impulsar la soberanía digital europea gracias al desarrollo de infraestructuras tecnológicas propias. Para llevar a cabo todo esto, EuroStack impulsa un marco regulatorio y financiero destinado a fomentar el desarrollo de soluciones tecnológicas escalables y sostenibles. La cooperación entre gobiernos, empresas y centros de investigación se perfila como un factor decisivo para que Europa conserve su liderazgo en el entorno digital.

Pero ¿por qué es necesario apostar por la independencia tecnológica? Europa siempre ha estado atada por una dependencia a proveedores extranjeros para infraestructuras digitales. De hecho, y tal y como destaca el proyecto EuroStack, desde 2017 el 70% de los modelos fundamentales de IA se han desarrollado en Estados Unidos, mientras que el 15% procede de China. Todo esto refleja la necesidad inminente de Europa de fortalecer las capacidades locales y consolidar un ecosistema de IA propio, con una inversión de, aproximadamente, 300.000 millones de euros durante la próxima década.

La transformación digital europea no es solo una aspiración, sino una realidad que se sostiene en cifras y en un proyecto a largo plazo. Las proyecciones indican que el mercado de la IA en Europa alcanzará los 50.000 millones de euros para 2030, impulsado por la soberanía digital y por iniciativas como EuroStack. Sin embargo, la brecha en innovación sigue siendo evidente. Este desequilibrio pone de relieve la urgencia de consolidar un ecosistema de investigación y desarrollo propio que permita a la región avanzar con independencia tecnológica y liderazgo global.

Ante esto, los Estados miembros de la Unión Europea han apostado por EuroStack, como un pilar central para reducir la dependencia de proveedores externos, impulsar la innovación y garantizar el desarrollo tecnológico europeo. En términos generales, estos esfuerzos pretenden no solo cerrar la brecha digital, sino transformar a Europa en un referente mundial de tecnología responsable y soberana.

EuroStack es la gran apuesta de Europa para lograr la soberanía digital. ISTOCK

Desafíos y riesgos

Ahora bien, no todo es un camino de rosas y son varios los desafíos que hay. Uno de los principales obstáculos es la dependencia de la financiación pública. A pesar de la inversión prevista, una gran parte de los recursos proviene de fondos europeos y programas gubernamentales. Esta dependencia hace que la ejecución de EuroStack esté sujeta a cuestiones políticas. Por otro lado, está la competencia. El ecosistema digital actual está dominado por empresas estadounidenses y chinas con una capacidad de inversión privada y una infraestructura de innovación muy superiores. Si EuroStack no logra atraer capital del sector privado y consolidar alianzas estratégicas con la industria europea, corre el riesgo de quedar rezagado.

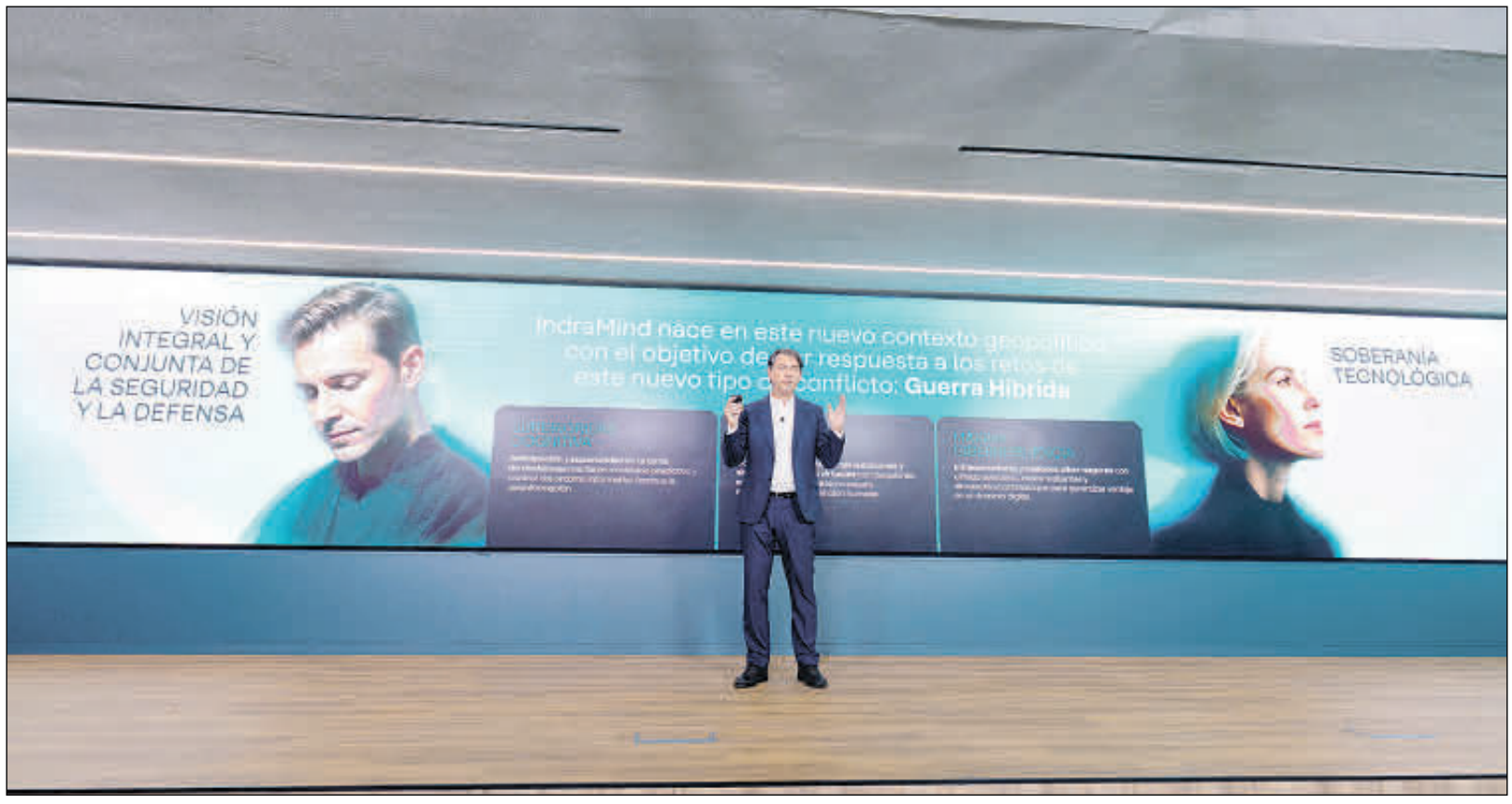
A ello se suma el reto de la adopción y compatibilidad tecnológica. Aunque la iniciativa promueve soluciones soberanas, estas deben coexistir en un mercado, donde muchas empresas ya dependen de infraestructuras tecnológicas establecidas. La implementación efectiva de los componentes tecnológicos –como SovereignAI, EuroChips o SovereignCloud– también representa un punto crítico. Su éxito dependerá de la capacidad de Europa para desarrollar y fabricar estas tecnologías.

> Desde el año 2017 el 70% de los modelos fundamentales de IA se han desarrollado en Estados Unidos

Asimismo, la atracción y retención de talento es un gran reto. El liderazgo en IA requiere profesionales cualificados; sin embargo, Europa continúa perdiendo talento hacia Estados Unidos y Asia, donde las oportunidades laborales y los incentivos económicos son mayores. Sin políticas eficaces que fomenten la formación, la movilidad interna y la competitividad salarial, EuroStack podría enfrentarse a una brecha de capacidades difícil de cerrar. Por último, algunos expertos advierten sobre las posibles implicaciones políticas y éticas de la iniciativa.

Aunque EuroStack se presenta como un instrumento para fortalecer la soberanía digital, existen preocupaciones en torno al control gubernamental. La introducción de herramientas como la Digital ID Wallet o el Euro Digital despierta debates sobre la privacidad, la centralización de la información y el riesgo de un proteccionismo digital que limite la competencia y la colaboración internacional. Si no se gestiona con transparencia y equilibrio, la búsqueda de soberanía tecnológica podría derivar en un exceso de control estatal y en una menor apertura del mercado europeo, afectando la innovación que precisamente pretende impulsar.

En definitiva, EuroStack representa una apuesta decisiva por la soberanía digital europea, pero su éxito dependerá de equilibrar independencia, innovación y colaboración. Europa tiene ante sí un gran reto. Si logra combinar inversión, talento y visión estratégica, podrá consolidarse como un referente tecnológico sostenible y autónomo. Así, este proyecto es un intento de equilibrio entre independencia y cooperación, entre competitividad y responsabilidad.



Ignacio Martínez, director de IndraMind, durante la presentación de esta iniciativa de Indra Group.

Así es IndraMind, el 'cerebro' digital de Indra Group para combatir la guerra híbrida

Se trata de la primera iniciativa tecnológica española que desarrolla IA soberana en un entorno ciberresiliente y que constituye un paso decisivo hacia la soberanía tecnológica

EcoBrands

Los conflictos actuales ya no distinguen entre lo civil y lo militar, ni entre lo físico y lo digital. Las fronteras se han desdibujado completamente". Estas palabras de Ignacio Martínez, director de IndraMind, ponen sobre la mesa por qué la seguridad y la defensa exigen una visión unificada en la que las tecnologías de uso dual son necesarias para dar respuesta a cualquier tipo de amenaza. En este sentido, como recuerda Martínez, "la soberanía tecnológica deja de ser una opción para convertirse en la base de nuestra autonomía". Y es que las amenazas a la seguridad nacional ya no operan en silos. Un ataque puede combinar simultáneamente el ciberespacio, las infraestructuras críticas y los servicios públicos, difuminando los límites entre la seguridad civil y la defensa militar.

Para dar respuesta a este contexto nace IndraMind, un *cerebro* para la protección integral de ciudadanos, territorios, infraestructuras y activos críticos físicos y digitales, desarrollado por Indra Group. Se trata de la primera iniciativa tecnológica española que desarrolla IA soberana en un entorno ciberresiliente y que constituye un paso decisivo hacia la soberanía tecnológica y la superioridad estratégica.

Con operaciones con un volumen de ventas superior a los 300 millones de euros y una plantilla compuesta por 3.000 profesionales altamente cualificados, este proyecto de Indra Group ofrece un enfoque integral en seguridad y defensa, aplicando soluciones tecnológicas duales orientadas a asegurar tanto la ventaja operativa en situaciones críticas como la capacidad de disuasión.

Para Ángel Escribano, presidente ejecutivo de Indra Group, "es la respuesta que damos ante una nueva situación, utilizando nuestro conocimiento para, de manera inmediata, impulsar la soberanía tecnológica en España y Europa". Así, IndraMind se construye sobre más de dos décadas de conocimiento, experiencia y capacidades de la compañía en materia de ciberseguridad, ciberdefensa, guerra electrónica, inteligencia artificial, plataformas autónomas (drones y antidrones), gestión masiva de datos y sistemas de mando y control.

"En los últimos meses hemos consolidado el posicionamiento comercial alineado con tres tendencias clave del mercado de seguridad y defensa: superioridad cognitiva –inteligencia y decisión–, operaciones autónomas y resiliencia ciber", destaca José Vicente de los Mozos, consejero delegado de Indra Group.

Las capacidades de IndraMind permiten atender a situaciones tanto en el ámbito civil como militar. "Hablamos de situaciones como la vigilancia de fronteras, gestión de emergencias, protección de infraestructuras críticas frente a ataques físicos y digitales. Y hablamos de soberanía tecnológica, no solo en los datos, también en los algoritmos, la IA, el *software* y la infraestructura sobre la que se sustenta todo", explica Martínez.

Vanguardia digital

IndraMind es una solución que no solo responde a los retos actuales, sino que se adelanta a los desafíos futuros, con una visión centrada en la inteligencia como motor de transformación.

Su capacidad para aprender, adaptarse y operar de forma autónoma en tiempo real la convierte en una herramienta clave para la nueva era de los sistemas críticos. A este respecto, tiene la capacidad para procesar grandes volúmenes de datos en tiempo real y esto permite anticipar las amenazas y responder adecuadamente. Una ventaja más que relevante teniendo en cuenta que la velocidad es fundamental en misiones críticas, ya que permite que agentes inteligentes, como drones y sistemas autónomos con IA, actúen de forma coordinada. Por eso es clave la optimización de la toma de decisiones y la automatización.

"La inteligencia artificial y el *software* avanzado están transformando el mercado de la seguridad y defensa. IndraMind se posiciona como un especialista único en el mercado porque integra toda la cadena de valor con productos propios de nueva generación", subraya el director general de IndraMind.

IndraMind Marca un hito clave hacia la soberanía tecnológica de España y Europa

Para Óscar López, ministro de Transformación Digital y de la Función Pública, Indra y España han marcado "un momento de inflexión en el calendario de la soberanía digital europea. La tecnología de IndraMind no solo supone un enorme activo en la protección integral de nuestros ciudadanos, territorios e infraestructuras. También supone un salto cuántico en la carrera geopolítica de la ciberdefensa. Cuando una infraestructura estratégica se moderniza, las empresas y las instituciones podemos tomar mejores decisiones y hacerlo más rápido".

Así, esta propuesta refuerza el liderazgo de la compañía en innovación y en el desarrollo de soluciones tecnológicas que sitúan a nuestro país a la vanguardia de la transformación digital de los sistemas críticos.

Tecnología

La guerra de los chips: el constante tira y afloja entre China y Estados Unidos

El líder asiático y la potencia norteamericana continúan la pugna por encabezar la soberanía tecnológica. Mientras, el resto de actores, se alertan por la interrupción de suministros

Pilar Ceballos

La agenda y la actualidad geopolíticas han estado marcadas durante las últimas semanas por la tensión entre China y EEUU. Las grandes potencias continúan luchando por dominar el sector de los microchips y planificando encuentros cara a cara.

Hasta ahora los verdaderos protagonistas habían sido los mandatarios de los respectivos territorios, Donald Trump y Xi Jinping, no obstante, la complejidad de las relaciones internacionales, ha provocado que se ponga el foco en otros actores como Europa.

Entre los últimos movimientos, destaca la reunión de principios de noviembre, cuando la Administración del presidente estadounidense, Donald Trump, indicó que "como parte del acuerdo comercial con China, el Gobierno de Pekín permitirá a la tecnológica Nexperia reanudar las exportaciones de sus chips fabricados en territorio chino, clave para las cadenas de suministro globales", según informó la Agencia EFE.

Este encuentro se dio después de que el gobierno neerlandés interviniese a Nexperia, filial europea de la empresa china Wingtech Technology, suspendiendo al propietario de la tecnológica y colocando sus acciones bajo administración indepediente, a través del Tribunal de Apelación de Ámsterdam. Todo ello porque "sospechaba que la empresa propietaria china Wingtech Technology, estaba robando secretos industriales de una planta británica para poder llevarse esta actividad a su territorio", explica José Luis Costa-Krämer, investigador y experto en el PERTE Chip en IMN-CSIC (Instituto de Micro y Nanotecnología-Consejo Superior de Investigaciones Científicas). Al día siguiente, "China inmediatamente dejó de mandar chips a Europa y denunció daños económicos y reputacionales", relata el especialista.

"Nexperia cuenta con cerca del 40% del suministro mundial de semiconductores básicos para automoción y representa un eslabón crítico, cuyo parón afecta directamente a Volkswagen, BMW, Mercedes-Benz, Stellantis, Renault, que ya evalúan paradas de producción por falta de stock", estima David Ortega, profesor de EADA y consultor en movilidad y reindustrialización. Y agrega que "la actual crisis va mucho más allá de la tecnología y afecta a toda la estructura industrial europea".

> El 70% de las tierras raras a nivel global pertenecen al 'gigante' asiático, claves para fabricar semiconductores

Esto no es nada nuevo. La guerra comercial entre China y EEUU se intensificó en 2018, cuando Trump impuso medidas arancelarias al otro *gigante*. Desde entonces, la relación entre ambas potencias ha sido un constante tira y afloja, con restricciones que han llegado hasta tres dígitos en alguna ocasión.

Pero ¿cuál es el núcleo del enfrentamiento? Para Alfonso Gabarrón, gerente de la AESEMI (Asociación Española de la Industria de Semiconductores), es una pugna que "combina tecnología, propiedad intelectual, suministro de materias primas y control geopolítico de las cadenas de valor".

Diferentes estrategias

Con respecto a China, Costa-Krämer resalta que "hay mucha interdependencia, no solo tecnológica sino mercantil y financiera". No obstante, en lo que a materia prima se refiere, el *gigante* asiático va sobrado. De hecho, según la Agencia Internacional de la Energía, en la actualidad, domina el 70% de las tierras raras a nivel global, materiales críticos imprescindibles para la fabricación de semiconductores.

En su caso, Ortega apunta a que "busca autosuficiencia tecnológica completa: inversión masiva en diseño, fundición y *packaging* para reducir su dependencia de proveedores occidentales y usar el control sobre los nodos maduros como palanca diplomática". Pese a ello, Costa-Krämer, de IMN-CSIC, califica a China como un "competidor formidable", debido a su gran inversión pública en fabricación de chips y a su "ventanilla única". Aun así, "necesita el mercado estadounidense y ciertas tecnologías en las que está retrasada", añade.

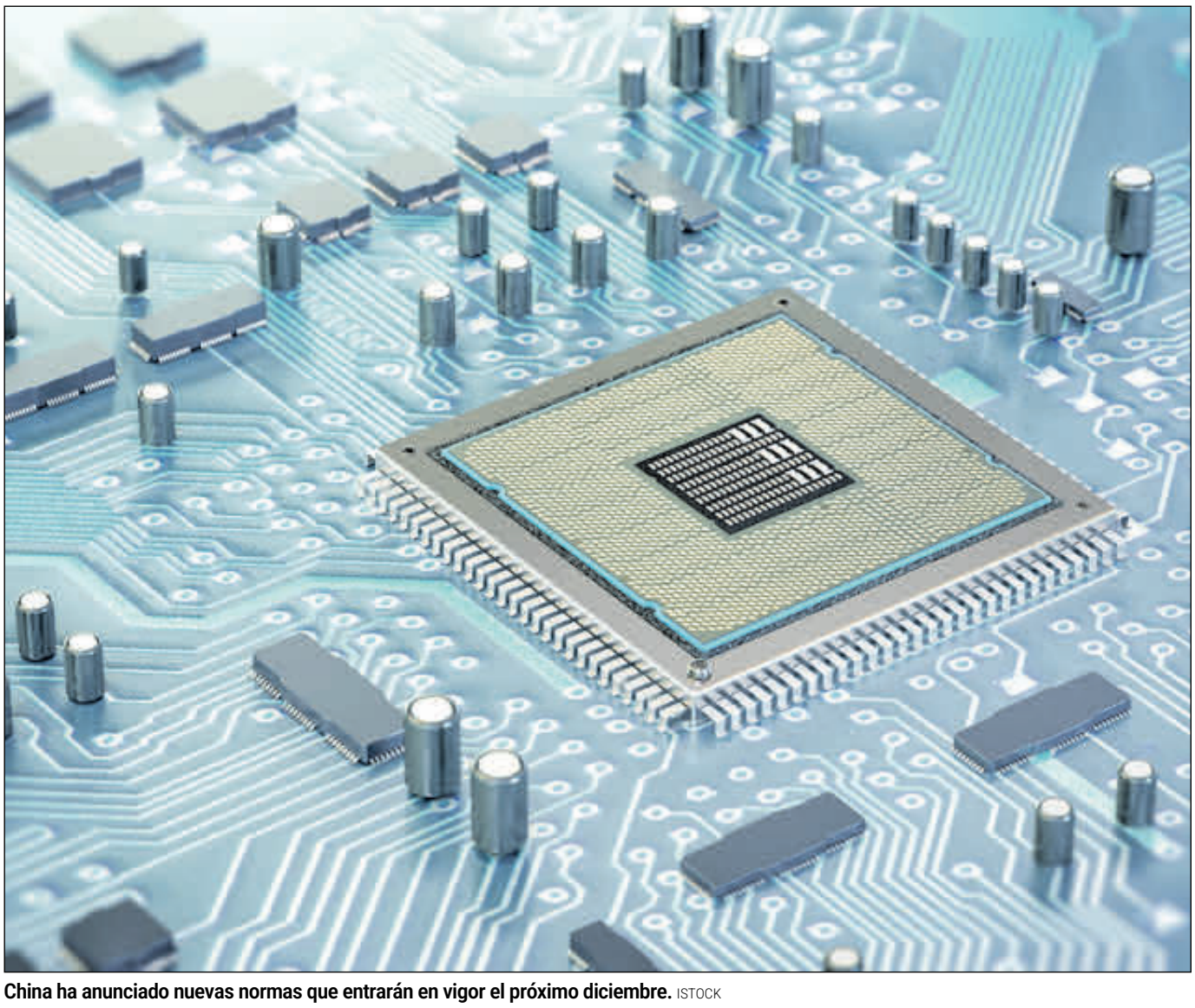
EEUU, por su parte, "ha sido el padre de la tecnología, con la invención del circuito integrado, su desarrollo y aplicación y con empresas líderes en el mercado de fabricación como Nvidia y ávidas de la tecnología como Apple", asegura el experto en PERTE Chip.

Según Gabarrón, de AESEMI, su estrategia se centra en "intentar posicionarse restringiendo exportaciones, financiando nuevas fábricas nacionales y promoviendo alianzas con socios estratégicos".

Con la mirada puesta en el futuro y la incertidumbre de lo que pueda pasar hasta entonces, China ha anunciado nuevas normas que entrarán en vigor el próximo diciembre. Esta consta de dos fases, aunque la fecha de su aplicación va variando después de cada reunión, por lo que son ambiguas. La que trataba de controlar las exportaciones de tierras raras y chips, en forma de licencias, parece haberse aplazado durante 12 meses. Cada producto o artículo fabricado con materiales o tecnologías *made in china*, deberán obtener una licencia de exportación. Todo ello con el fin de controlar las cadenas de suministro.

¿Qué reacción se espera de EEUU? Tras la puesta en marcha de las nuevas reglas chinas, Gabarrón de AESEMI cree que "llevará a cabo más controles, incentivos a la fabricación local y presión diplomática hacia los aliados para desacoplar cadenas críticas de suministro del entorno chino". Además, agrega que "endurecerá las reglas comerciales y pondrá nuevos vetos tecnológicos, complejizando las alianzas e industriales globales en un ecosistema ya altamente fragmentado".

Por otro lado, ¿cuál está siendo el papel de Europa en este duelo? Según el profesor de EADA, Ortega, "Europa se ve obligada a equilibrar su dependencia comercial con su necesidad de seguridad industrial". Pese a que la soberanía es prácticamente imposible, Costa-Krämer propone "atraer fábricas de última generación, establecer un ecosistema de confianza y un plan de contingencias para asegurar el suministro de chips", concluye.



China ha anunciado nuevas normas que entrarán en vigor el próximo diciembre. ISTOCK

El sector empresarial está aumentando su inversión en ciberseguridad. ISTOCK

El mercado de ciberseguros se multiplica por 50 en una década y rozará los 43.000 millones

Según las estimaciones del bróker Howden, estas pólizas llevan más de un año con tarifas a la baja, con una caída en el tercer trimestre del año de un 15% de media. Europa es de los mercados con un crecimiento más elevado y representará el 25% de las primas globales hasta 2030

Aitor Caballero Cortés

El mercado de los ciberseguros alcanzará los 50.000 millones de dólares de volumen de ingresos por primas (algo más de 43.000 millones de euros según el tipo de cambio actual) a finales de año a nivel global, según las últimas estimaciones de la correduría de seguros multinacional Howden.

En tan solo diez años, estas pólizas han pasado de ser prácticamente insignificantes para el negocio asegurador a ser un producto el cual es difícil no encontrar en los catálogos de las compañías. Y es que el crecimiento del mismo en esta última década se ha multiplicado por 50. Si lo comparamos con otras pólizas no tan generalistas, como los seguros D&O (productos aseguradores que protegen a los directivos y altos cargos de las compañías), el incremento de estos se ha multiplicado por diez, y prácticamente se igualarán en volumen de primas a cierre de año.

Todo ello gracias a un empuje en la contratación de estos seguros especialmente en Estados Unidos y Europa, porque los índices tarifarios incluso son negativos si se hace la comparación interanual. Al contrario que sucede en otros ramos generalistas como autos o salud, donde la inflación supone una parte importante del crecimiento del volumen de negocio y no tanto la adhesión de nuevos clientes, los ciberseguros llevan desde finales de 2023 e inicios del pasado ejercicio con primas a la baja.

Y es que, pese a que el sector empresarial está aumentando su inversión en ciberseguridad y, por ende, presiona la demanda también a la hora de contratar ciberseguros, eso también se tradujo en una menor siniestralidad, lo que permite a las entidades obtener retornos de su servicio. Esta menor frecuencia ha supuesto la entrada de nuevos jugadores en el mercado, lo cual está presionando incluso más que la demanda de las compañías.

En concreto, las tarifas de los seguros cibernéticos disminuyeron durante el primer semestre de 2025 entre un 10% y un 15%, aunque según Howden, en algunos casos llega hasta un 30%. En general, hasta el 63% de los clientes de este tipo de pólizas reportaron un descuento en sus primas "considerablemente superior en comparación con el primer semestre del mismo periodo del año anterior", se explica en el informe. En este tercer trimestre ya cerrado, las primas medias aceleraron su descenso en torno a otro 15%, aunque este indicador también varía en función del sector que contrate este seguro.

> El grado de penetración de los ciberseguros en las pequeñas y medianas empresas apenas llega al 15%

Más garantías

Con este contexto, las compañías "están aprovechando el mercado en recesión (de precios) para mejorar sus límites de cobertura y ajustar sus niveles de retención. Incluso están eliminando límites de cobertura a medida que mejora la calidad del riesgo, volviéndose las aseguradoras más flexibles", detalla Howden. No obstante, esta permisividad de las aseguradoras no está siendo en vano, ya que las entidades financieras cada vez están demandando mayores elementos de ciberseguridad a la compañía contratante. Según el informe *CyberArk Identity Security Landscape Report 2025*, se muestra que hasta el 88% de las organizaciones afirman que sus aseguradoras exigen controles de ciberseguridad avanzados.

El problema de ofrecer esas garantías es que no tienen, precisamente, un bajo coste. Y comprendiendo que el 99% de las empresas que hay en Europa son pymes, hace que los presupuestos estén más ajustados que en las grandes compañías. Por ello, el índice de penetración de los ciberseguros en el terreno pyme es apenas del 15%, por lo que la brecha en cuanto a contratación de estos productos se estimó, en 2023, en más de 900.000 millones de dólares (777.000 millones de euros), con Europa representando el 23% de ese total (178.742 millones de euros).

El incidente de CrowdStrike

Según Marsh, el número de incidentes cibernéticos en Europa continúa creciendo, aumentando un 61% en 2024 respecto al año anterior. Esto se debió al impacto de las reclamaciones fruto del incidente con CrowdStrike, que supuso reclamaciones de millones de usuarios de todo el mundo. En total, las reclamaciones por este hecho fueron finalmente menos costosas de lo esperado: frente a las estimaciones que rondaban los 1.000 millones de dólares, resultó en un coste de aproximadamente 500 millones de dólares. Sin embargo, incluso descontando dicho siniestro, las denuncias por ciberataques aumentaron un 43%.

Mercadona invierte 250 millones de euros para la transformación digital

Mercado IT es el departamento que se encarga de crear soluciones tecnológicas y gestiona alrededor de 300 aplicaciones y procesos en continua evolución

EcoBrands

La transformación digital está ganando cada vez más peso dentro de las compañías y se ha convertido en un pilar fundamental. En este contexto, Mercadona refuerza su compromiso con el impulso del desarrollo tecnológico y la innovación mediante el lanzamiento de un ambicioso Plan de Excelencia Digital. Este programa, que cuenta con una inversión superior a los 250 millones de euros para el periodo 2025-2028, permitirá a la compañía continuar avanzando en la reingeniería tecnológica de sus diferentes procesos de negocio, con el objetivo de mejorar la agilidad y optimizar la eficiencia operativa.

Mercadona IT es el departamento que se encarga de crear soluciones tecnológicas. Esta área gestiona alrededor de 300 aplicaciones y procesos en continua evolución tecnológica. "Adoptamos tecnologías, arquitecturas y lenguajes de vanguardia que nos permiten avanzar en agilidad y eficiencia, con el propósito de responder a las nuevas demandas de Mercadona y de nuestros clientes, para quienes aspiramos a seguir siendo un referente", subraya Patricia Tobía, directora general del Departamento de Informática (CIO) de la compañía.

Así, y gracias a la innovación tecnológica, la compañía ha podido agilizar la toma de decisiones y fomentar la innovación de producto; desarrollar sistemas inteligentes y eficientes orientados a optimizar costes y reforzar la productividad en sus bloques logísticos; digitalizar la trazabilidad de los productos para garantizar en todo momento la seguridad alimentaria y la calidad; mejorar la experiencia de compra en tienda mediante espacios más acogedores y sostenibles, con un ahorro energético de hasta el 40 % en iluminación; y crear soluciones informáticas específicas para nuevas líneas de negocio, como la sección *Listo para Comer*, entre otras iniciativas.

En definitiva, la propuesta de valor de Mercadona se sustenta en tres pilares esenciales: la participación en proyectos de gran impacto impulsados por tecnología de vanguardia; la posibilidad de crecer en un entorno que promueve el desarrollo personal y profesional, respaldado por un plan de carrera sólido y atractivo; y la oportunidad de integrarse en un equipo altamente especializado y experimentado, referente en su ámbito.

Una plantilla con mucho talento

En los últimos años, Mercadona IT se ha consolidado como el motor interno de la estrategia de modernización digital del grupo. Este impulso ha supuesto un notable crecimiento y expansión. De hecho, en el último ejercicio fiscal, 120 personas se han incorporado al equipo especializado en el desarrollo de *software* y aplicaciones, encargado de diseñar y construir soluciones que mejorar procesos clave de la empresa.

Esta área ha ido creciendo hasta conformar un equipo de 1.200 profesionales tecnológicos especializados en áreas como desarrollo y arquitectura de software, ciberseguridad, *DevOps*, gestión del dato, *product management*, *cloud*, infraestructura IT, diseño UX/UI, gestión de dispositivos y adquisición de software informático, entre otras disciplinas. Todo esto ha permitido a la compañía ser más ágil en la toma de decisiones y tener trazabilidad del desarrollo profesional de los integrantes de la plantilla.

Asimismo, la compañía cuenta con un modelo de innovación propio transversal con el que contribuye a impulsar los Objetivos de Desarrollo Sostenible (ODS) del Pacto Mundial de la Organización de las Naciones Unidas. En este sentido, Mercadona ha invertido 72 millones de euros en la transformación digital, incluyendo Mercadona Online.

En las tiendas, ha incorporado tecnologías de predicción de fallos, una herramienta que permite anticipar incidencias y reforzar la automatización operativa, aumentando así la eficiencia y reduciendo tiempos de respuesta. La digitalización se ha extendido a prácticamente todos los ámbitos: desde la gestión del surtido y las herramientas de diseño de gastos, hasta la implantación del sistema multidivisa en todos los sistemas financieros, que facilita la operativa en diferentes entornos económicos y simplifica las transacciones internacionales.

El área informática también ha vivido una profunda transformación con el desarrollo de nuevas aplicaciones propias, diseñadas para agilizar los procesos y responder de manera más rápida a las necesidades del negocio. Entre estas soluciones, destaca una nueva herramienta para dietas y liquidaciones de gastos, que permite gestionar de forma más eficiente los desplazamientos y los reembolsos de los trabajadores. Asimismo, se ha puesto en marcha una aplicación específica para conocer los gastos certificados por tienda, lo que mejora la transparencia y el control financiero de cada establecimiento. La digitalización de herramientas clave ha continuado con la gestión de actas de Sanidad y la carpeta de registros del sistema APPCC (Análisis de Peligros y Puntos de Control Críticos), esenciales para garantizar la seguridad alimentaria.

> La compañía ha destinado 72 millones a impulsar Mercadona Online

Uno de los avances más significativos ha sido la evolución del Portal Tornillo, una herramienta interna que centraliza la información de productos, surtido, proveedores y precios. Su reciente actualización ha mejorado la usabilidad y las funcionalidades tanto en formato web como móvil, consolidándose como la fuente principal de datos actualizados para toda la compañía. En la misma línea, la herramienta Ciclo de Vida facilita la gestión integral de los productos, permitiendo dar altas, bajas o modificaciones de manera sencilla y eficiente a lo largo de toda la cadena de suministro.

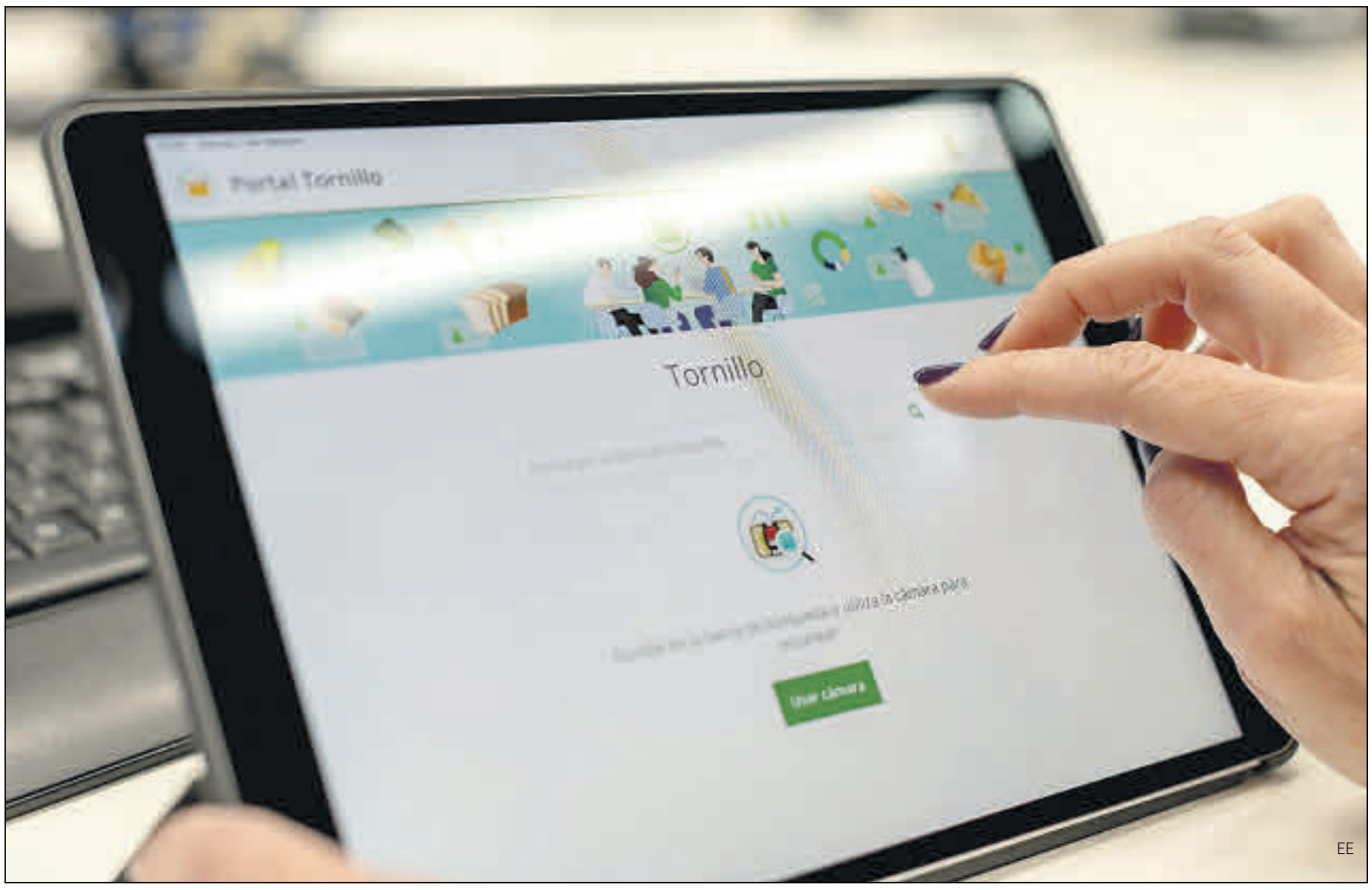
La transformación digital también ha alcanzado los ámbitos de recursos humanos, con la implantación de la herramienta Emplea_2, pensada para gestionar el día a día de los trabajadores, y de procesos logísticos y de mantenimiento, donde la automatización y la trazabilidad digital están optimizando el rendimiento. Además, la gestión de planos e inventario de medios físicos en tienda y del stock en tiempo real se ha modernizado con sistemas digitales que aportan mayor control y precisión.

En el plano administrativo y comercial, Mercadona ha impulsado la firma digital de contratos y condiciones con proveedores mediante la herramienta Gefidocom, así como el desarrollo de Factura-Me, un sistema de facturación e información que mejora la comunicación entre proveedores y responsables de área. La compañía incluso ha incorporado inteligencia artificial generativa para el procesamiento automático de facturas, una innovación que acelera tareas y reduce errores.

Infraestructura tecnológica

La compañía ha puesto en marcha la renovación de la infraestructura tecnológica de sus Centros de Procesamiento de Datos (CPD) ubicados en Albalat dels Sorells (Valencia) y Villadangos (León), un proyecto estratégico valorado en 20 millones de euros. Para su desarrollo, Mercadona colabora con aproximadamente 15 proveedores nacionales e internacionales.

Los CPD son instalaciones diseñadas para albergar, gestionar y operar los sistemas de información y comunicaciones que permiten el funcionamiento diario de las más de 1.670 tiendas de la cadena. Estas infraestructuras están preparadas para resistir a catástrofes naturales, incorporan sistemas de refrigeración redundantes y cuentan con acceso mediante análisis biométrico, garantizando la máxima seguridad y disponibilidad operativa.



EE

Mercadona renueva sus centros de datos cada seis años, un proceso que implica la migración de más de 300 aplicaciones críticas, con el objetivo de mantenerse siempre a la vanguardia tecnológica. "El diseño y la implementación de este proyecto, de gran impacto para la organización, están siendo desarrollados por perfiles altamente especializados de Mercadona IT, como administradores de redes, sistemas, bases de datos, *cloud* o ciberseguridad", explica Juanjo López, coordinador de Seguridad e Infraestructura Informática de la compañía.

Entre las principales mejoras destacan la automatización de procesos, el incremento de la resiliencia y el control de entornos, la potenciación de la ciberseguridad y la ampliación de la capacidad de cómputo, equivalente –en el caso de los nuevos CPD– al almacenamiento digital de todos los libros, revistas, periódicos y manuscritos publicados. Además, esta infraestructura refuerza la apuesta por la nube híbrida, evita la obsolescencia tecnológica y proporciona mayor seguridad y control sobre los sistemas.

Actualmente, ya se han completado las fases de diseño y adquisición del equipamiento, y antes de finalizar el año se llevará a cabo el montaje de las nuevas máquinas, en paralelo al funcionamiento de los CPD actuales. La migración de aplicaciones a los nuevos equipos está prevista para 2026.

Otros avances

Asimismo, Mercadona ha llevado a cabo otros avances notables que incluyen la digitalización de los procesos de gestión inmobiliaria a través de la herramienta Real Estate, y la implantación de un sistema digital para coordinar y registrar las donaciones en todas las tiendas de España, reforzando el compromiso social de la cadena. Pero la innovación no se limita al ámbito tecnológico, pues ha extendido su cultura innovadora a otros frentes estratégicos que abarcan el producto, la sostenibilidad social y la colaboración empresarial.

En innovación de producto, Mercadona ha consolidado su Modelo de Coinnovación, con 20 centros especializados donde los "Jefes" –como la empresa denomina a sus clientes– comparten experiencias y sugerencias que sirven para desarrollar productos ajustados a sus necesidades, con la máxima calidad y precios competitivos. Gracias a este modelo, la compañía ha logrado 220 mejoras en el surtido, 330 novedades y 23 innovaciones, fortaleciendo su liderazgo en la distribución alimentaria.

También ha logrado 220 mejoras en el surtido, 330 novedades y 23 innovaciones

En el ámbito de la innovación social, ha impulsado proyectos de integración y sostenibilidad. Asimismo, cuenta con 22 tiendas que incorporan jardines urbanos en sus cubiertas y fachadas, una iniciativa que contribuye al bienestar ambiental. Mercadona también colabora en campañas solidarias de recaudación en favor de entidades sociales reconocidas, permitiendo que los clientes realicen donaciones directamente en caja. Además, la compañía ha desarrollado la Tarjeta Sociedad, una herramienta dirigida a Administraciones públicas y entidades sociales para canalizar ayudas hacia colectivos vulnerables, otorgando a los beneficiarios la libertad de elegir los productos que necesitan y dignificando su proceso de compra.

Por último, en materia de innovación abierta y colaborativa, mantiene alianzas con cinco organizaciones que promueven el avance tecnológico y empresarial: la Fundación COTEC para la Innovación, el Foro de Empresas Innovadoras, la CEOE, AECOC y AINIA. Además, participa activamente en el Programa Corporate Lanzadera-Mercadona, que impulsa proyectos con siete *startups* –Sensei, Hoop Carpool, Midsaic, Invofox, Busup, Kleta y Okticket– dedicadas a desarrollar soluciones tecnológicas aplicadas a la movilidad, la sostenibilidad y la digitalización de procesos.

Con este conjunto de iniciativas, Mercadona no solo moderniza su infraestructura tecnológica y operativa, sino que consolida un modelo integral de innovación, abierto, sostenible y centrado en las personas, que refuerza su posición como referente en eficiencia, compromiso social y transformación empresarial.

Tecnología

El euro digital entra en su fase final y Europa ultima su llegada en el año 2029

El pasado mes de octubre concluyó la fase de preparación y ahora el organismo europeo está trabajando para que el proyecto pueda ver la luz dentro de tres años. Antes, se realizarán pruebas piloto

Judih Arrillaga Pérez

En un mundo marcado por la digitalización en el que cada vez son más comunes los términos criptomonedas, *blockchain*, pagos NFC o *contactless*, la Unión Europea ha dado un paso en esa dirección y está trabajando en el lanzamiento del euro digital, su propia moneda digital soberana (CBDC por sus siglas en inglés). Pero, ¿en qué consistirá?

Se va a tratar de dinero emitido por los bancos centrales del Eurosistema, es decir, será como el efectivo, pero en versión digital. Está pensado para ser una opción de pago electrónico adicional a las ya existentes, complementando así al efectivo y los medios de pago privados. "Actualmente no existe ninguna opción de pago digital europea que abarque toda la zona del euro, y 13 de los 20 países dependen de esquemas internacionales para los pagos con tarjetas. El euro digital será un medio de pago electrónico europeo accesible y aceptado en todos los países de la zona del euro", justifica el BCE.

> Será un medio de pago electrónico europeo accesible y aceptado en todos los países de la zona del euro

Fue el 14 de julio de 2021 cuando el Banco Central Europeo aprobó el proyecto que ponía en marcha esta nueva divisa. En estos cuatro años se ha llevado a cabo el trabajo de campo. Fue el pasado mes de octubre cuando acabó la fase de preparación, tras 24 meses, y ahora el Consejo de Gobierno del BCE evaluará los resultados y decidirá si se inicia la siguiente fase. "Se espera que el reglamento que regulará el uso del euro digital pueda aprobarse hacia el segundo trimestre de 2026. Durante la fase de preparación se han definido los requisitos técnicos, opciones de diseño, normativas operativas, pruebas, selección de proveedores, casos de uso, etc.", explica a *elEconomista.es* Gorka Briones, socio de Monitor de Deloitte.

Según las estimaciones del BCE, esperan estar preparados para una posible primera emisión del euro digital en 2029, suponiendo que se adopte la legislación necesaria de la Unión Europea en 2026. "Lo que acaba de pasar es lo que llaman fase preparatoria, que empezó en 2023. Se ha iniciado hace poco la fase más técnica, la que establecerá las normas de funcionamiento. A partir de ahí ya iremos conociendo cómo lo piensan articular, como van a seleccionar los proveedores de tecnología para que esto funcione. También habrá un tanteo a los ciudadanos, que por ahora hay bastante escepticismo. Y luego se hará algún tipo de prueba piloto y simulaciones. Será en 2028 o 2029 cuando entre ya en vigor", detalla Patricia García Sánchez de la Barreda, directora del Máster en Dirección Financiera de ESIC Business & Marketing School.

> El BCE ha diseñado el proyecto como una alternativa al dinero en efectivo, nunca para que acabe sustituyéndolo

"Para hacer realidad esta ambición compartida, el Eurosistema se centrará en tres líneas de trabajo principales: impulsar la preparación técnica, profundizar la participación del mercado y apoyar el proceso legislativo. Esto incluirá comenzar a desarrollar las bases técnicas del euro digital y validar sus funcionalidades básicas mediante proyectos piloto; colaborar estrechamente con los proveedores de servicios de pago, los comercios y los representantes de los consumidores para realizar pruebas progresivas y prepararse para la primera emisión; y mantener una estrecha colaboración con los colegisladores, las instituciones y las autoridades de la UE en el proyecto del euro digital para seguir aportando conocimientos técnicos durante todo el proceso legislativo", explica el organismo.

¿La sociedad está preparada?

La idea es que el euro digital se utilice en los pagos pequeños del día a día. "Con el monedero en euros digitales podrías pagar el café de la mañana o a la persona que cuida de tus hijos por la tarde. El euro digital estaría disponible para cualquier pago electrónico en tiendas físicas, a través de internet o entre particulares", detalla la institución. Una de las mayores ventajas de esta nueva divisa será a la hora de viajar por los países de la Unión Europea ya que de esta forma no será necesario disponer de dinero en efectivo y se podrá pagar en cualquier establecimiento sin costes adicionales.

"Cuando tú tienes una tarjeta en el banco, este te cobra una comisión, esta es una ventaja con la que parte el euro digital. Tampoco va a ser necesaria una conexión a internet. El día del apagón, por ejemplo, todos necesitábamos efectivo porque no funcionaban ni los datáfonos ni los cajeros. El BCE lo vende como una ventaja respecto a la posibilidad de estar en un sitio sin cobertura", argumenta García Sánchez de la Barreda.

Pese a que sobre el papel su uso parece claro, todo hace indicar que su aceptación por parte de la sociedad será mucho más paulatina. "El nivel de adopción natural de un euro digital sería muy bajo puesto que, en su configuración actual, el euro digital no cubre ninguna necesidad insatisfecha. Es cierto que aspira a tener atributos de anonimidad en un medio de pago digital, espacio que no cubre actualmente ningún medio de pago, pero los ciudadanos no acaban de comprar el concepto de un anonimato real en un medio de pago público digital", declara Briones.

Un informe elaborado por Deloitte recalca que la probabilidad de adopción del euro digital por parte de los españoles es baja, posiblemente porque les cuesta conceptualizarlo y no ven su utilidad debido a la amplia oferta de medios de pago digitales disponibles. De hecho, el 61% de los usuarios preguntados por la consultora rechazan su adopción o declaran no saber si lo adoptaría. Además, el 64% considera que no tendrá amplios beneficios.

"Lo que ocurre es que la falta de un interés amplio en los usuarios plantea dudas sobre la posibilidad de lograr una adopción universal del euro digital en España. Por dar algún dato de una encuesta realizada por Monitor Deloitte recientemente, el 62% de españoles desconocen el euro digital y el 64% consideran que no tendrá amplios beneficios, el 47% tienen conocimiento de conceptos económicos clave para la comprensión del euro digital, lo que puede suponer una barrera y el nivel de satisfacción actual respecto a medios de pago actuales es del 85%", detalla el socio de Deloitte.

¿Sustituto del efectivo o los bancos?

Una de las preguntas más repetidas a la hora de hablar del euro digital es si sustituirá al dinero en

ISTOCK

efectivo o a los bancos. Una cuestión en la que el BCE es bastante tajante. "No. Sería un complemento del efectivo, no un sustituto. El euro digital existiría en paralelo al efectivo en respuesta a la creciente preferencia de los consumidores por pagar digitalmente, de manera rápida y segura. El efectivo seguiría siendo de curso legal y coexistiendo con el euro digital y con cualquier medio de pago electrónico privado actualmente en uso", explica la institución.

"El euro digital es una forma de dinero digital emitido directamente por el Banco Central Europeo, lo que lo convierte en dinero de curso legal respaldado por el Estado. En cambio, las tarjetas de crédito tradicionales no emiten dinero, sino que son un instrumento de pago que permite a los usuarios acceder a una línea de crédito otorgada por una entidad financiera privada, lo que denominaríamos dinero bancario o privado", detalla Briones.

Tampoco va a sustituir por completo a los bancos y las tarjetas de crédito porque sobre la mesa está poner un límite máximo de dinero que pagar. "Están hablando de poner un límite al monedero para rellenarlo de entre 1.000 y 5.000 euros. Esto supone que ese euro digital no va a estar para comprarse una casa", detalla la directora del Máster en Dirección Financiera de ESIC Business & Marketing School. Al establecer un límite se impide que esta nueva moneda se convierta en un instrumento para mantener activos líquidos sustanciales, es decir, no será una alternativa de inversión o de ahorro.

Entonces, ¿las tarjetas pueden verse perjudicadas en algunos escenarios? "Tal y como se está configurando, es probable que se utilice especialmente para pagos pequeños y cotidianos (como compras en comercios físicos, transporte público, etc.), donde el uso de tarjetas puede ser menos conveniente. Si el euro digital se integra eficazmente en plataformas digitales, podría competir igualmente con las tarjetas y con el resto de medios de pagos electrónicos como Bizum", augura el socio Monitor de Deloitte.

No es una criptomoneda

Pese a tratarse de un método de pago 100% online, es importante destacar que no estamos hablado ni de *stablecoins*, ni de criptomonedas. Las primeras, están creadas por empresas privadas y no están garantizadas por ningún banco central ni por ninguna autoridad pública. Su valor depende de la forma en la que la empresa gestione sus reservas y finanzas, lo que podría verse influido por factores ajenos a su control, por lo que su estabilidad no es tan segura como la del euro. En el caso de activos como el Bitcoin o el Ethereum no están respaldados por ninguna entidad y no tienen valor subyacente. Sus precios pueden subir y bajar considerablemente, y no hay ninguna organización responsable si pierde su valor.

> Podría competir igualmente con las tarjetas y con el resto de medios de pagos electrónicos como Bizum

El euro digital, por su parte, será dinero de banco central, emitido y garantizado por el Eurosistema, integrado por el Banco Central Europeo y los bancos centrales nacionales de la zona del euro. Al igual que los billetes y monedas en euros, tendría curso legal, por lo que todos los ciudadanos podrían utilizarlo para efectuar pagos. Como dinero de banco central y bien público, sería estable y fiable, con la seguridad de que un euro digital vale un euro.

Más allá de nuestras fronteras

El proyecto de contar con su propia CBDC no es exclusivo de la Unión Europea. La Reserva Federal de Estados Unidos (Fed por sus siglas en inglés) empezó hace unos años a trabajar en la creación de un dólar digital, sobre todo, después de que en 2019 Facebook decidiera lanzar su *stablecoin* Libra, un proyecto que finalmente nunca llegó a ver la luz. Sin embargo, en la actualidad el dólar digital está paralizado como consecuencia de la situación política que atraviesa el país. De hecho, Donald Trump, nada más llegar a la Casa Blanca, aprobó un decreto que prohíbe "crear, emitir o promover una moneda digital proveniente de un banco central" y ordenó "poner fin" a todo trabajo vinculado a esta posibilidad.

Donde la CBDC es una realidad es en China. El país asiático está probando el uso del yuan digital en diversas ciudades del país desde 2019. En el año 2023, se abrieron más de 15 millones de billeteras de yuanes digitales por personas físicas y más de 1,3 millones por empresas. Asimismo, se estima que más de 2,7 millones de comercios adoptaron esta moneda en 2023. Dentro de este conjunto de pruebas piloto, algunas ciudades chinas han comenzado a pagar a los empleados de organismos gubernamentales y empresas estatales con esta moneda, recibiendo su salario íntegramente en yuanes digitales.

Tecnología

Ley europea de IA: cuáles son las fechas clave los próximos meses

Los primeros pasos en esta regulación se dieron en 2021, pero no ha sido hasta febrero de este año cuando han entrado en vigor algunas prohibiciones; sin embargo, no será hasta agosto de 2027 cuando se aplique al completo esta normativa

María Juárez

El avance de las nuevas tecnologías tiene un ritmo sin precedentes. No cabe duda de todos los beneficios que traen consigo herramientas como la inteligencia artificial (IA); sin embargo, también son muchos los riesgos. En este contexto, la Comisión Europea se convierte en pionera mundial y decide impulsar una regulación que proteja los derechos fundamentales, la seguridad y la salud de los ciudadanos europeos. De hecho, esta ley de IA busca abordar riesgos como la falta de transparencia de los sistemas, las decisiones discriminatorias y la manipulación, al tiempo que establece un marco de confianza para el desarrollo y uso de la IA en el mercado único.

Pero ¿cuándo surge todo esto? Aunque fue en 2021 cuando se planteó por primera vez una regulación para la IA, no fue hasta finales de 2023 cuando el Consejo y el Parlamento Europeo alcanzaron un acuerdo provisional. Ahora bien, fue hasta un año más tarde cuando entró en vigor, aunque sin aplicarse ninguno de los requisitos. Ya en 2025, concretamente en febrero, se empiezan a aplicar las prohibiciones sobre determinados sistemas y requisitos sobre alfabetización. En paralelo, desde el Gobierno de España se aprueba el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la IA. El objetivo principal de esta medida es adaptar la legislación española a las pautas que llegan desde Europa. En agosto de 2026, se aplicará el resto de la ley de IA, salvo el artículo 6, que está relacionado con las normas de clasificación de los sistemas de IA de alto riesgo. Por lo tanto, no será hasta agosto de 2027 cuando se aplique al 100% esta regulación.

La clasificación de riesgos

La regulación europea sobre IA establece una jerarquía de riesgos para garantizar el uso seguro y ético de estas tecnologías. En el nivel más alto se encuentran los riesgos inaceptables, que corresponden a sistemas de IA directamente prohibidos. Entre ellos se incluyen aquellos que emplean la clasificación social de ciudadanos o la manipulación del comportamiento humano, prácticas consideradas contrarias a los derechos fundamentales. El segundo nivel corresponde a los sistemas de alto riesgo, que pueden afectar la salud, la seguridad o los derechos fundamentales de las personas. Este grupo abarca tecnologías aplicadas en sectores sensibles como la infraestructura crítica, la educación, el empleo, la justicia y los servicios públicos esenciales. Estos sistemas deberán cumplir con exigentes requisitos técnicos y estarán sujetos a una supervisión constante.

En términos generales, en los más altos niveles se incluyen desde herramientas para la selección de personal hasta sistemas que evalúan créditos bancarios o intervienen en ámbitos como la inmigración y la justicia. Por lo que estos usos estarán sujetos a una supervisión más estricta, dado el potencial impacto de sus decisiones y la posibilidad de que el algoritmo cometa errores o genere situaciones injustas.

En el nivel de riesgo limitado o más bien casi nulo se ubican herramientas como los *chatbots*, que deberán garantizar la transparencia, informando claramente a los usuarios que están interactuando con una inteligencia artificial. Por último, los sistemas de riesgo mínimo, como los filtros de *spam*, se consideran de bajo impacto y estarán sujetos a obligaciones regulatorias reducidas.

Tal y como señala Pablo López-Aranguren, responsable del Área Digital en Mutualidad, "según un estudio de Radar Digital Mutualidad, los objetivos del EU AI Act van más allá de una simple regulación técnica. Estamos hablando de una estrategia política, ética y económica que entendemos cuenta con múltiples capas: proteger derechos fundamentales, fomentar una IA confiable y centrada en el ser humano, evitar la fragmentación del mercado único europeo, impulsar la innovación responsable y establecer un estándar global".

Esta regulación pionera en Europa, pretende ser un referente a nivel internacional. En palabras de López-Aranguren, "se establece una base sólida para un desarrollo ético, seguro y competitivo de la IA en Europa. Las empresas que se adapten pronto no solo evitarán sanciones, sino que podrán convertir la conformidad en ventaja competitiva" y agrega que "gracias a controles más sólidos de supervisión y seguridad, las entidades se sienten más cómodas en la gestión de riesgos asociados a la IA y en la protección de los datos. Este cambio se traduce en una evolución desde casos centrados en la agregación de datos y el análisis de riesgos hacia nuevas aplicaciones como *chatbots* de atención al cliente, *copilots* de asistencia y procesos automatizados de incorporación tanto de empleados como de nuevos clientes".

Parlamento europeo. EE

La línea cronológica de la ley de IA

- **2020 Oct.** El Consejo Europeo empieza a debatir sobre la inteligencia artificial
- **2021 Abr.** La CE publica una propuesta para regular la inteligencia artificial en Europa
- **2021 Ago.** Comienza el periodo de consulta pública sobre la Ley de AI por parte de la CE. La Comisión recibió 304 propuestas
- **2021 Nov.** Surge el primer texto de compromiso sobre el proyectos con importantes cambios en los ámbitos de la puntuación social, los sistemas de reconocimiento biométrico y las aplicaciones de alto riesgo
- **2021 Dic.** Las comisiones de Mercado Interior y Libertades Civiles del Parlamento Europeo dirigirán conjuntamente las negociaciones sobre la Ley de IA
- **2022 Ene.** Se da el primer intercambio de puntos de vista sobre la propuesta de ley
- **2022 Feb.** La CE presenta una nueva estrategia de normalización en la que expone su enfoque de las normas en el mercado único y a escala mundial
- **2022 Mar.** La Comisión de Asuntos Jurídicos (JURI) del Parlamento Europeo publica sus enmiendas a la Ley de IA
- **2022 Jun.** - Fecha límite para que se presenten todas la enmiendas a la ley. En total, hubo miles de enmiendas
  - La presidencia francesa del Consejo de la UE difunde su texto de compromiso final antes de que la República Checa asuma la Presidencia
- **2022 Sep.** La Comisión de Asuntos Jurídicos (JURI) del Parlamento Europeo aprueba su dictamen sobre la Ley de IA como última comisión del Parlamento
- **2022 Dic.** El Consejo de la UE adopta su posición común ('orientación general') sobre la Ley de IA
- **2023 Jun.** El Parlamento Europeo adopta su posición negociadora sobre el Acta IA, con 499 votos a favor, 28 en contra y 93 abstenciones
- **2023 Dic.** Se llega a un acuerdo provisional entre el Parlamento y el Consejo
- **2024 Feb.** Se crea en la Comisión la Oficina Europea de Inteligencia Artificial, dependiente de la Dirección General de Redes de Comunicación, Contenidos y Tecnología, para apoyar la aplicación de la Ley de Inteligencia Artificial, especialmente para la IA de propósito general
- **2024 May.** El Consejo Europeo adopta formalmente la Ley de AI de la UE
- **2024 Jul.** La Ley de IA se publica en el Diario Oficial de la Unión Europea
- **2024 Ago.** Fecha de entrada en vigor de la Ley de IA. En esta fase no se aplica ninguno de los requisitos de la Ley, que empezarán a aplicarse gradualmente con el tiempo
- **2024 Nov.** Fecha límite para que los Estados miembros identifiquen y hagan pública la lista de autoridades / organismos responsables de la protección de los derechos fundamentales, y lo notifiquen a la Comisión y a los demás Estados miembros.
- **2025 Feb.** Se empieza a aplicar las prohibiciones sobre determinados sistemas de IA
- **2025 Mar.** El Gobierno de España aprueba el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial, con el objetivo de adaptar la legislación nacional al nuevo marco europeo
- **2025 Ago.** Se aplican las normas sobre organismos notificados, gobernanza, confidencialidad, sanciones y los propósitos generales
- **2026 Feb.** Plazo para que la Comisión facilite directrices que especifiquen la aplicación práctica del artículo 6, que versa sobre las normas de clasificación de los sistemas de IA de alto riesgo
- **2026 Ago.** Se aplica el resto de la ley, salvo el artículo 6
- **2027 Ago.** Se aplica la Ley de IA al completo y las obligaciones correspondientes del Reglamento empiezan a aplicarse
- **2028 Ago.** La CE evaluará el funcionamiento de la Oficina de IA y el impacto de los códigos de conducta

Fuente: EU Artificial intelligence Act. eE

Casi la mitad de los puestos de trabajo tecnológicos surgieron tras la pandemia

El confinamiento destapó el atraso digital que sufrían muchas compañías. Desde entonces, el perfil profesional que buscan incluye habilidades técnicas, además de sociales y personales

Pilar Ceballos

La tecnología es una aliada para las empresas, pero también para los que las conforman: los trabajadores. Según el *Mapa de Empleo Tecnológico en España 2025 (2013-2023),* una herramienta interactiva de métricas, elaborada por la Fundación Cotec, "desde 2023, se han creado 494.000 puestos de trabajo en las ramas más tecnológicas de la economía en España". El estudio expone que 240.000 de ese total, "aparecieron después de 2020, el año de la pandemia", por lo que el 48,58% de las ocupaciones tecnológicas surgieron tras la Covid-19.

"La pandemia no creó la necesidad, la visibilizó", asegura Marta Sánchez, CEO & Head Hunter de Candee. Durante años, "la transformación digital fue una promesa pendiente. De pronto, se volvió urgente: o digitalizas o te detienes", añade la CEO y explica que lo que antes era "innovación", pasó a ser "infraestructura básica". Y esto, "arrastró a todos los sectores, no solo al tecnológico, a repensar cómo operaban, cómo vendían, cómo se relacionaban con sus clientes y, sobre todo, con sus equipos", agrega.

Raquel Pérez, directora de RRHH de Sopra Steria, apoya esta afirmación y asegura que "en el sector de la consultoría tecnológica se dice, a menudo, que la pandemia aceleró la digitalización de las empresas y las administraciones públicas en hasta cinco años". Por este motivo, "se impulsó la demanda de perfiles tecnológicos para implantar soluciones seguras, plataformas digitales y sistemas de gestión remota". Como consecuencia, se promovió "una mayor inversión en infraestructura en la nube y en ciberseguridad y, por ello, una mayor demanda de desarrolladores, ingenieros de datos, expertos en *cloud* y expertos en ciberseguridad", añade la directora.

No obstante, "la tecnología ha dejado de ser un ámbito exclusivo del sector tecnológico para convertirse en el eje transversal que impulsa la transformación de prácticamente todas las industrias", explica Verónica Arteaga, *People and Culture Director* en Softtek EMEA. La experta destaca sectores como "la medicina personalizada, la movilidad inteligente, la banca y las finanzas, la logística y el *retail*, donde se usan algoritmos de optimización, inteligencia de clientes y gestión inteligente de cadenas de suministro para mejorar la eficiencia y la experiencia del usuario". Y asevera que "dentro de las propias compañías, esta transformación ha permeado todos los departamentos, incluso aquellos que antes no estaban vinculados con la tecnología".

Los últimos datos del estudio antes citado, que recoge la evolución de 2013 a 2024, reflejan que de los 13 empleos tecnológicos de la economía, el segmento de Programación, Consultoría y Otras Actividades encabeza la lista de afiliados con un crecimiento del 6,9%. Le sigue el de Fabricación de Vehículos de motor, remolques y semirremolques, con un 6,8%, y Fabricación de Maquinaria y Equipo n.c.o (No clasificado Ocasionalmente), con un incremento del 6,8%. En el cuarto puesto, se encuentra Investigación y Desarrollo, que ha crecido 6,7% en la última década.

Por el contrario, los segmentos donde el empleo tecnológico ha evolucionado menos durante este periodo de tiempo son: Actividades de Programación y Emisión y Distribución de vídeos (5,8%), Fabricación de productos informáticos electrónicos y ópticos (5,9%), Servicios de información (5,9%) y Fabricación de material y equipo eléctrico (6%).

El segmento de Programación, Consultoría y Otras Actividades encabeza la lista de afiliados. ISTOCK

Nuevos perfiles

Estas nuevas tendencias reflejan la necesidad de formar nuevos roles profesionales. Pero, ¿qué nuevas *skills* necesitan las compañías? "Las organizaciones buscan hoy profesionales con una combinación equilibrada de *hard skills* y *soft skills"*, asevera Juan Luis Moreno, *Partner & Mananging Director* de The Valley. Las primeras hacen referencia a habilidades más técnicas como el análisis de datos o la comprensión de la inteligencia artificial, mientras que con las segundas se refieren a habilidades personales y sociales como la comunicación o el liderazgo. El experto declara que "las *soft skills* han ganado protagonismo y ahora se buscan personas que combinen conocimiento tecnológico con sensibilidad humana". Por su parte, Sánchez manifiesta que "el talento que realmente aporta valor no es el que lo sabe todo, sino el que sabe evolucionar porque vivimos en un mercado donde las herramientas caducan más rápido que los títulos".

No obstante, para que las personas desempeñen sus capacidades se necesitan oportunidades y, en ocasiones, estas se ven truncadas por prejuicios o barreras culturales. Según el estudio de Cotec, en España, "el 68% del empleo tecnológico es masculino". Sin embargo, desde 2017, "el femenino ha crecido todos los años a tasas superiores que el masculino, incluso en 2020".

Aun así, el cambio no viene solo. La plantilla de recursos humanos tiene un gran papel para fomentarlo. "Muchas veces el problema no está en la falta de talento femenino, sino en cómo se diseñan los procesos: desde el lenguaje de la oferta hasta la validación técnica o la expectativa de *trayectoria ideal*", respalda Sánchez.

Pero ¿dónde está el capital humano? En cuanto a la localización de este, el estudio señala que "el empleo tecnológico está fuertemente polarizado". Prueba de ello, es que "solo cinco comunidades autónomas presentan un peso del empleo tecnológico por encima de la media de España". Estas son: la Comunidad de Madrid (10,5%), Navarra (10%), País Vasco (9,2%), Cataluña (9%) y Aragón (8,5%). Por el contrario, las comunidades, cuyo peso está muy por debajo de la media, son Baleares (2,7%), Extremadura (2,4%) y Canarias (2,2%), donde "la diferencia con los otros territorios es de casi 8 puntos porcentuales", expone el documento.

Aunque la diferencia entre áreas depende de múltiples factores estructurales y de contexto, "las regiones con más talento tecnológico suelen contar con una mayor inversión en I+D, la presencia de universidades y centros de innovación, un tejido empresarial diversificado y un ecosistema digital consolidado", sostiene Moreno.