

## El riesgo cibernético

El Periódico



Una persona interactúa con un asistente virtual, una herramienta que simula las respuestas que daría un humano mediante IA.

# El Gobierno fomenta la mezcla entre inteligencia artificial y ciberseguridad

► El Ejecutivo ha puesto en marcha un plan que implica invertir 1.500 millones en expandir el uso de esta tecnología en la economía y el sistema público

AGUSTÍ SALA  
Barcelona

El Gobierno pretende fomentar el uso de la inteligencia artificial (IA) en la ciberseguridad. Es uno de los puntos que establece la Estrategia de Inteligencia Artificial 2024. Este plan da continuidad a las iniciativas desplegadas por el Ejecutivo en esta materia y refuerza el compromiso «con la vanguardia tecnológica, reafirmando su posición como líder en el desarrollo y aplicación de soluciones de IA», según afirmaron desde La Moncloa cuando se aprobó. Uno de los organismos públicos que con mayor celeridad ha abrazado el potencial de la inteligencia artificial es la Agencia Tributaria, pero siempre «con intervención humana», siguiendo las directrices generales, del Ejecutivo.

Tras la aprobación de esta estrategia, el Gobierno destacó que «se trata de un plan ambicioso, diseñado para consolidar y expandir el uso de la IA en el conjunto de la

economía y en la administración pública». Su despliegue se realiza en 2024 y 2025, y cuenta con recursos por un total de 1.500 millones de euros, adicionales a los 600 millones ya movilizados, procedentes fundamentalmente del plan de recuperación, transformación y resiliencia y de la adenda a dicho plan.

### La estrategia pública

Uno de los aspectos destacados es la intención de promover el desarrollo de la IA en el sector privado, especialmente en el ámbito de las pymes y autónomos. Para ello se desarrolla el programa *Kit Consulting*, dotado con 300 millones de euros, para que los proyectos empresariales de menor tamaño puedan contratar servicios de asesoramiento para la adopción de la IA. Además, se ha ampliado el programa *Kit Digital* con la incorporación de nuevos productos IA y una inversión de 350 millones. También se dedicarán 400 millones a través del Fondo NextTech con el objetivo de facilitar financiación a

las empresas que desarrollen soluciones de IA.

Este eje se completa con la futura ley de ciberseguridad –que establecerá un marco claro e integral para desarrollar esta actividad en España y mejorará la protección de los sistemas de información, redes y datos– y con el impulso del ecosistema empresarial de ciberseguridad con IA «que fomentará la innovación, la colaboración y la adopción de tecnologías de IA en el ámbito de la ciberseguridad».

El Ejecutivo también propone acciones para fomentar la innovación, la colaboración y la adopción de tecnologías de inteligencia artificial en el ámbito de la ciberseguridad a través del Instituto Nacional de Ciberseguridad (Incibe). Además, la Agencia Española de Supervisión de la IA (AESIA), pionera en Europa, es clave para definir las buenas prácticas en el uso de la inteligencia artificial y garantizar la evaluación de los modelos que se vayan desarrollando. También garantizará el cumplimiento de las normas armonizadas en

materia de IA recogidas en la ley europea.

Estas iniciativas se dan cuando el impacto de la IA en la ciberseguridad crece y abarca áreas tanto en prevención como en respuesta a incidentes, según se detalla en la Estrategia de Inteligencia Artificial 2024. Por una parte, los avances en IA suponen un desafío, pero por otra proporcionan herramientas que mejoran la prevención y detección avanzada de amenazas a través de modelos predictivos.

### Foco global

La ciberseguridad se ha convertido en un auténtico desafío y en uno de las grandes preocupaciones de las cúpulas de las empresas, como se ha visto en los últimos encuentros del Foro Económico Mundial, que se celebra en la ciudad suiza de Davos. Todos los países están poniendo el foco de manera creciente en la ciberseguridad, especialmente ante la irrupción de tecnologías como la IA.

La ciberseguridad es una pieza central de soberanía estratégica y es un elemento esencial en la generación de la confianza y la seguridad. Los sectores económicos claves son muy dependientes de las redes y de los sistemas de información con altos niveles de interconexión: por ello, es especialmente relevante disponer de los mayores niveles de seguridad en las infraestructuras críticas y los servicios esenciales, tanto en el sector público como en el sector privado, destaca el ejecutivo en su estrategia.

Reforzar la ciberseguridad es necesario para fomentar la confianza, la innovación, la conectividad y la digitalización protegiendo a la vez los derechos de los ciudadanos y su privacidad, argumenta el ejecutivo. «La ciberseguridad es un componente intrínseco de la propia digitalización y del desarrollo de nuevas tecnologías (muy especialmente de la IA), y su fortalecimiento es determinante para la soberanía estratégica de las naciones y para garantizar la transición digital», destacan.

El impacto de la IA en la ciberseguridad es significativo, y abarca varias áreas tanto desde el punto de vista de la prevención como de la respuesta a los incidentes. Por una parte, los avances en la IA suponen un desafío a la ciberseguridad, pero a la vez la IA proporciona herramientas que suponen una mejora de la prevención y detección avanzada de amenazas a través de modelos predictivos. «España parte de una buena situación en ciberseguridad: es el tercer país europeo tras Reino Unido y Estonia en el índice global de ciberseguridad (ICG) evaluado por las Naciones Unidas», afirman. ■

