La IA trae nuevas amenazas en los ciberataques a empresas

La Inteligencia Artificial presenta tantas posibilidades como riesgos entraña. Entre ellos, el de convertirse en un gran aliado para los ciberdelincuentes en un tiempo en el que los delitos cibernéticos contra empresas y particulares están a la orden del día.

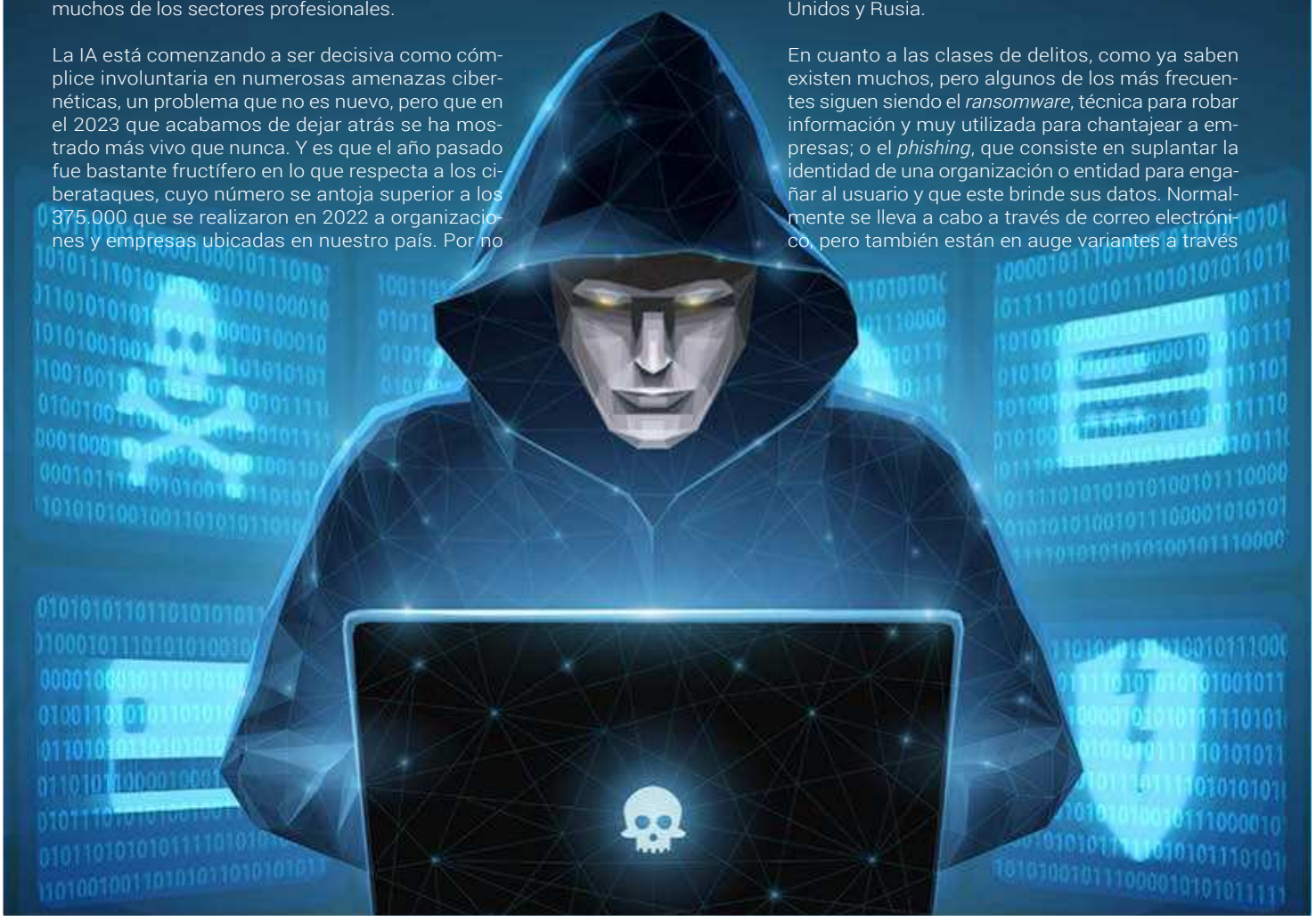
Diego Fernández Torrealba. Fotos: iStock

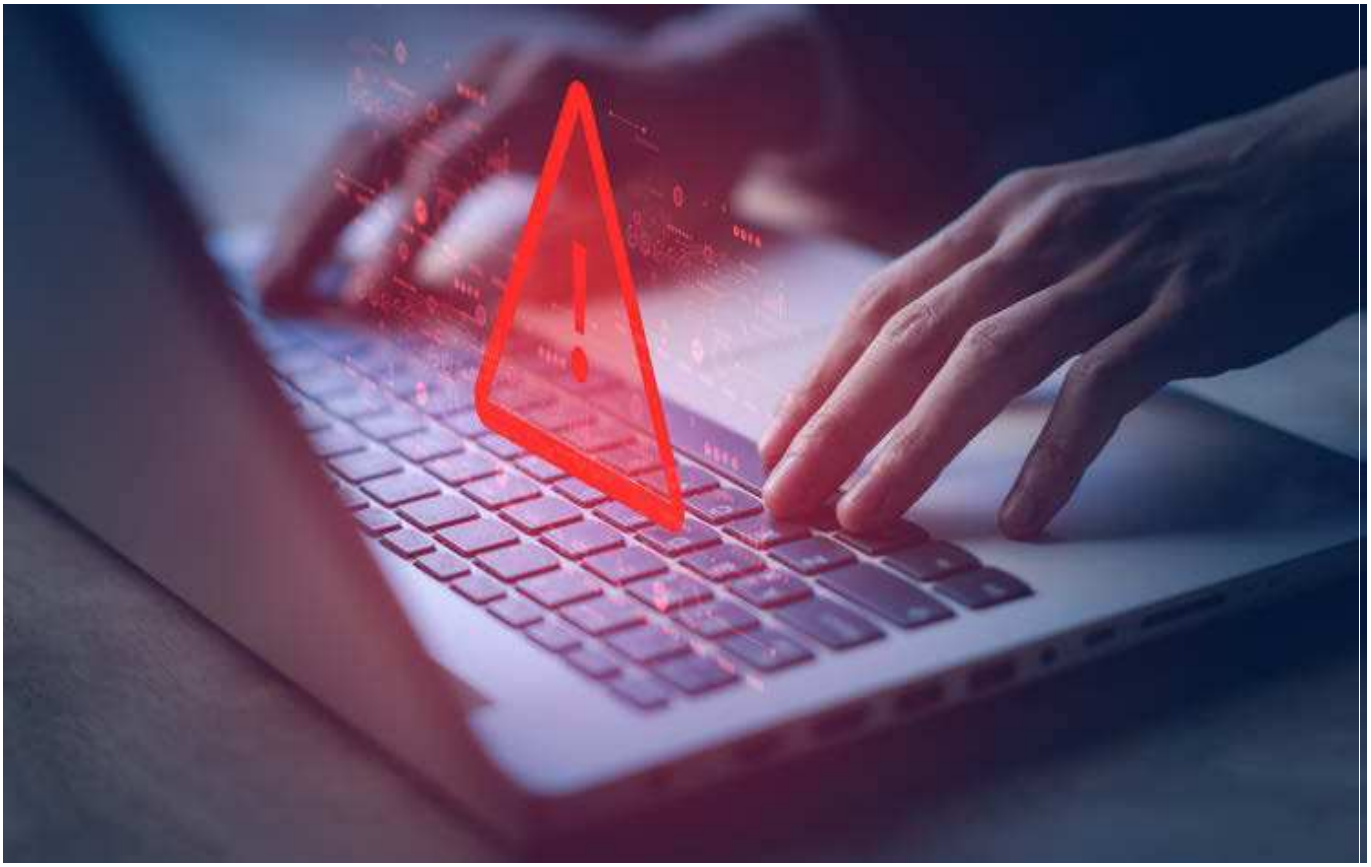
La tecnología avanza a pasos agigantados, y con ello las posibilidades para hacer el bien –y el mal– se multiplican exponencialmente. La Inteligencia Artificial se empieza a emplear como un método que multiplica las posibilidades, incrementa la velocidad y simplifica un sinfín de tareas, pero tiene unos enormes riesgos asociados desde su puesta en práctica más allá de la pérdida masiva de puestos de trabajo que puede generar en muchos de los sectores profesionales.

La IA está comenzando a ser decisiva como cómplice involuntaria en numerosas amenazas cibernéticas, un problema que no es nuevo, pero que en el 2023 que acabamos de dejar atrás se ha mostrado más vivo que nunca. Y es que el año pasado fue bastante fructífero en lo que respecta a los ciberataques, cuyo número se antoja superior a los 375.000 que se realizaron en 2022 a organizaciones y empresas ubicadas en nuestro país. Por no hablar de los particulares, también afectados no sólo a través de sus ordenadores, sino de sus teléfonos móviles.

El problema es especialmente grave en España, donde según estudios recientes se producen 1.250 ciberataques de media cada semana, convirtiéndonos en el tercer país del mundo que más delitos cibernéticos registra, tan sólo por detrás de Estados Unidos y Rusia.

En cuanto a las clases de delitos, como ya saben existen muchos, pero algunos de los más frecuentes siguen siendo el *ransomware*, técnica para robar información y muy utilizada para chantajear a empresas; o el *phishing*, que consiste en suplantar la identidad de una organización o entidad para engañar al usuario y que este brinde sus datos. Normalmente se lleva a cabo a través de correo electrónico, pero también están en auge variantes a través





de mensajes SMS (*smishing*), así como extorsiones por vía telefónica (*vishing*).

Una nueva amenaza

La implantación de la Inteligencia Artificial supone, como decíamos antes, grandes posibilidades, pero también importantes riesgos y amenazas, mejorando las armas e incrementando el potencial de los ciberdelincuentes, que encuentran nuevas vías para realizar sus delitos. Por ejemplo las clonaciones de voz e incluso los *deepfakes*, vídeos que muestran imágenes falsas que parecen ser reales, multiplicando las opciones de engaño.

En cuanto al *phishing*, la IA ha mejorado la eficiencia de esta técnica. ¿Por qué? Porque anteriormente, en muchos de estos intentos de timo la manera de escribir o las faltas de ortografía recurrentes llevaban a los usuarios a sospechar de la fiabilidad y autenticidad de la fuente que los enviaba, poniéndose en guardia y evitando así ser engañados.

Pero ahora, los delincuentes pueden utilizar la Inteligencia Artificial para escribir textos prácticamente perfectos y sin errores, reduciendo las posibilidades de ser descubiertos.

Prevención ante el fraude

Ante estas nuevas posibilidades de fraude, extorsión y engaño, el escudo pasa por una buena política de prevención. Más allá del sexto sentido de las personas y las empresas a la hora de detectar estos engaños, la mejor respuesta es tener los medios suficientes para la detección de estas prácticas fraudulentas.

Así lo consideran profesionales como Javier Huergo, responsable de la correduría especializada en seguros de ciberriesgo Watch&Act, quien afirma que "la formación del personal y la inversión en medidas de ciberprotección son esenciales para reducir el riesgo y minimizar el impacto negativo de los ciberataques"; en la misma línea se muestra Felipe Gar-cía, abogado y socio del despacho **Círculo Legal** Madrid: "Las empresas deben revisar sus políticas de riesgo y, si ven que el fraude puede crecer más, rea-lizar las inversiones correspondientes para preve-nir este tipo de comportamientos irregulares". Este último añade que "hay que contar con equipos lide-rados por personas –*compliance officers*– que im-pulsen planes de formación específicos en evitar fraudes en todas las modalidades. De nada sirven los sistemas, modelos o programas si detrás, no hay personas que involucren a la organización en acciones de formación específicas para ello".

Otro de los aspectos esenciales es el desarrollo de una legislación práctica, útil y justa con respecto al uso de la IA. La UE pretende poner en marcha la Ley de Inteligencia Artificial, estableciendo obligaciones para proveedores y usuarios en función del nivel de riesgo. En España, por su parte, se ha desarrollado la Aesia, la agencia estatal para la supervisión de la inteligencia artificial. Habrá que esperar para ver el impacto de ambas medidas en la regulación de una tecnología tan poderosa como peligrosa.