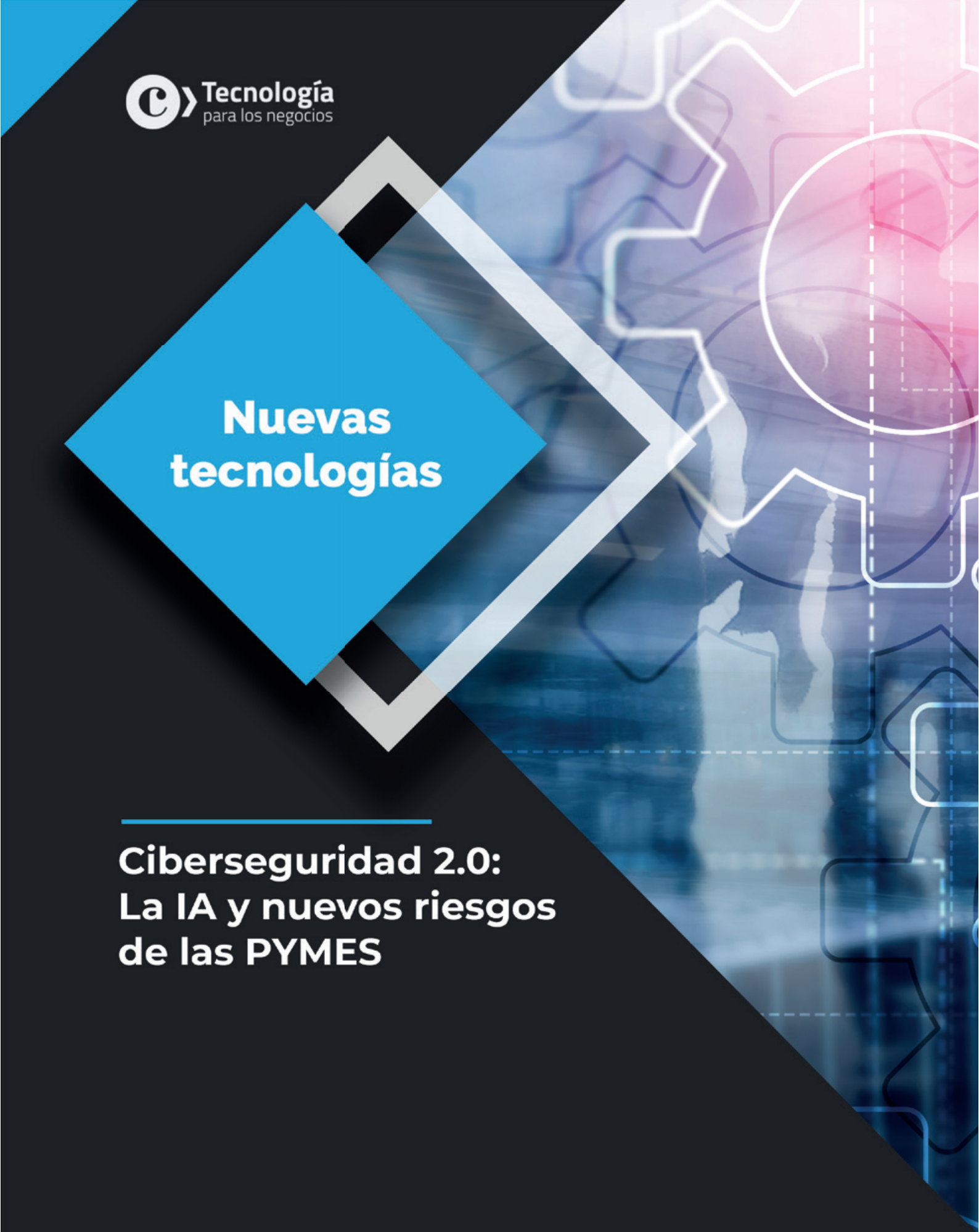
Tecnología
para los negocios



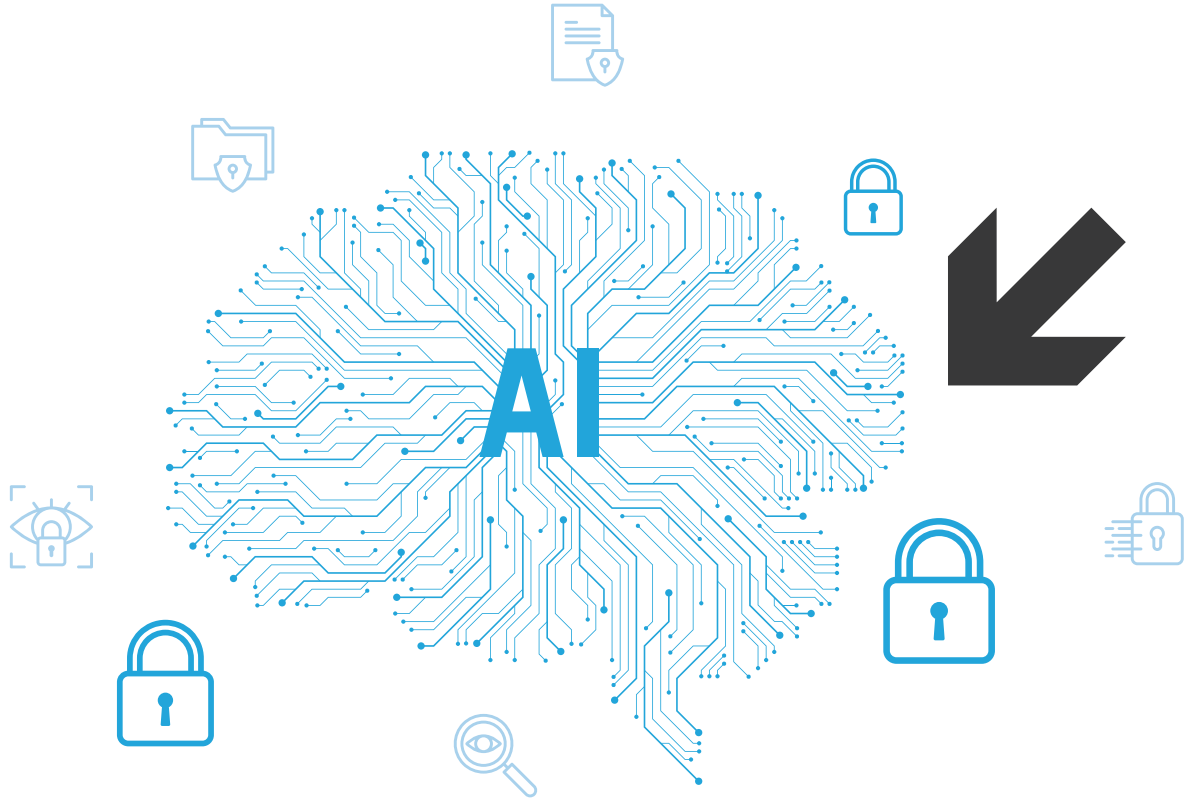
Nuevas tecnologías

Ciberseguridad 2.0: La IA y nuevos riesgos de las PYMES

Ciberseguridad 2.0

ticnegocios.es

Índice



1. Introducción

La inteligencia artificial (IA) es una herramienta extraordinariamente útil para acelerar determinados procesos productivos, efectuar tareas repetitivas y monótonas, e incrementar la productividad. También es uno de los ejes imprescindibles que definen la ciberseguridad 2.0.

Frente a la ciberseguridad tradicional, basada en la protección de la información de manera reactiva, surge este concepto que nos obliga a ser proactivos. Ha sido una evolución, cuyos primeros pasos se dieron con la tríada formada por la confidencialidad, la integridad y la disponibilidad. Posteriormente, se incorporó la seguridad OT o de la tecnología de las operaciones, que priorizó el control.

2. La IA y la seguridad

La simbiosis entre ambas es clara e inequívoca. La razón es la capacidad de la IA para manejar grandes volúmenes de datos y su eficiencia al llevar a cabo tareas complejas, pues sus algoritmos procesan con rapidez. Además, identifican patrones que podrían detectar amenazas. Los actuales sistemas de información y las redes generan cantidades ingentes de datos muy complicadas de manejar con los métodos tradicionales.

Por otra parte, tiene la capacidad de aprender de forma continua gracias al aprendizaje automático. En consecuencia, su adaptación a los nuevos contextos y ciberdelitos es mucho mayor. De hecho, puede ser entrenada para detectar actividades sospechosas en tiempo real. Al analizar patrones de tráfico en la red, transacciones de los usuarios y comportamientos del sistema, identifica rápidamente cualquier anomalía.

Otra de sus aplicaciones se relaciona con su respuesta ante posibles incidentes de seguridad. En este sentido, presta un enorme servicio a las pymes y organizaciones, que pueden actuar y recuperarse con mayor celeridad y eficacia. Por lo demás, puede dar una información muy valiosa sobre la amenaza, su origen y naturaleza, y las soluciones.

↘ 2.1

Los sistemas autónomos de IA

Son sistemas que operan sin necesidad de intervención humana. Son independientes y están capacitados para tomar decisiones sobre seguridad y responder por sí mismos a las amenazas que detecten. Utilizan técnicas de aprendizaje profundo e incorporan sus propias experiencias.

↘ 2.2

Algunas herramientas de IA para pymes

Tenéis a vuestra disposición varias herramientas de IA que podéis aplicar a distintas áreas de las pymes. Os mencionamos algunas de las más populares:

↘ 1

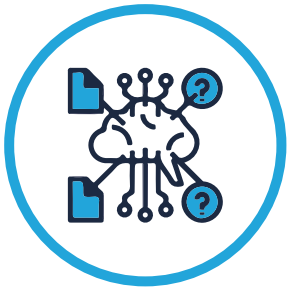
ChatGPT

Es la que lidera, de momento, el desarrollo de esta tecnología. Es muy útil para analizar los datos de vuestro negocio, crear anuncios o pulir vuestra estrategia de **marketing.**

↘ 2

Salesforce Einstein

Os ofrece recomendaciones avanzadas y predicciones con los datos.



↘ 3

Analytics Intelligence

Con ella, podréis descubrir tendencias y nuevas oportunidades.

↘ 4

Kuki

Está especializada en tiendas virtuales y os ayuda a guiar a los clientes durante el proceso de compra.

3. Los riesgos de la IA para las pymes

Sin duda, las ventajas son notables y nada exageradas. Sin embargo, debéis prestar atención a sus posibles riesgos. El primer indicador lo descubrimos en el mes de mayo cuando el científico **británico Geoffrey Hinton**, uno de sus creadores, renunció a su puesto en Google. Entre sus explicaciones, alega que tendrían que haber esperado antes de lanzarla.

Lo mismo dejaron por escrito 1300 expertos en una carta, quienes sugirieron la necesidad de frenar el lanzamiento de la IA, al menos, durante seis meses. El motivo es que la evolución de esta tecnología es infinitamente más rápida que el ritmo que siguen los legisladores para regularla. Os mostramos algunos de los peligros que entraña esta asincronía.

↘ 3.1 Responsabilidad objetiva indeterminada

Imaginad que una máquina autónoma guiada mediante IA provoca un accidente. Partamos de la base de que, aunque es una tecnología increíble, también falla. De hecho, puede ser objeto de demandas de responsabilidad civil por los daños causados. Con el vacío legal actual, sería imposible determinar si ha de ser la empresa que usaba la IA la que debe pagar o el proveedor de esta tecnología.

La Unión Europea ha sido el primer territorio en darse cuenta de este problema. En octubre de 2022, la Comisión presentó una propuesta de revisión y otra de una directiva específica para esta tecnología, ambas vinculadas con la responsabilidad. No obstante, aún están en el proceso de alegaciones y no se han aprobado.

↘ 3.2
Información falsa

La IA es capaz de imitar la voz de cualquiera, de crear imágenes falsas e, incluso, de proporcionar información completamente errónea. No es difícil imaginar lo que eso puede suponer al sistema político de un país en las manos inadecuadas o al honor de una persona o a vuestra imagen como marca. Con las herramientas correctas, cualquiera puede iniciar una campaña de descrédito sin que nada ni nadie os pueda proteger.

↘ 3.3
La doble cara de la IA respecto a la ciberseguridad

Efectivamente, la inteligencia artificial es un arma de doble filo con respecto a la ciberseguridad. Ya vimos cómo puede ayudaros. Aun así, también es crucial que tengáis presentes sus efectos menos controlables. Las aplicaciones que emplean IA manejan muchos datos, pero no se tiene muy claro dón de se almacenan, ni a qué tipo de tratamientos están sometidos. Esto, lógicamente, es un gran atractivo para los ciberdelincuentes, y las pymes miran con preocupación este hecho.
Por otra parte, la inteligencia artificial está igualmente disponible para los ciberdelincuentes. Aunque, de momento, todavía no han generado ningún **malware,** hay tres áreas clave en las que los modelos lingüísticos son atractivos:

1-Suplantación de identidad mucho más eficaz.
2-Los ciberdelincuentes que utilizan el **ransomware** pueden automatizar los rescates y ahorrar tiempo para dedicarlo a delinquir más.
3-Mejorar las estafas telefónicas.

↘ 3.4

Plantillas desmotivadas y sin formación en las pymes

Se ha hablado tanto sobre los empleos que pueden ser sustituidos por los sistemas de IA que, inevitablemente, ha calado cierto temor en las plantillas. Según Fundación Aquae, un 16 % de los puestos de trabajo serán llevados a cabo por la IA en la siguiente década. En efecto, el Parlamento Europeo ha cuantificado en un 14 % los automatizables en los países de la OCDE y el 32 % se verá afectado de un modo u otro.

Por tanto, es cierto que muchos trabajos podrán ser realizados por esta tecnología, pero también lo es que se crearán otros nuevos. El motivo es que estas soluciones avanzadas necesitan a humanos para gestionarse y mantenerse.

Un sistema educativo enfocado en la nueva realidad y la formación de los trabajadores jugarán un rol esencial con un doble objetivo. Por un lado, evitarán el desempleo a largo plazo y, por otro, garantizarán que hay mano de obra cualificada para este nuevo contexto.

↘ 3.5
Riesgo de sesgos y merma de los derechos fundamentales

Los sesgos, intencionales o involuntarios, son una realidad porque dependen de los datos que maneje el sistema o de su diseño. Por consiguiente, sus resultados podrían reflejar o replicar discriminaciones o desigualdades raciales y étnicas, sexistas, por edad o de cualquier otra naturaleza. Para agravar este problema, el uso de datos numéricos para describir una realidad social compleja le proporciona una pátina de objetividad que es completamente falsa. Es el fenómeno conocido como mathwashing. Ya imaginaréis lo que supondría una toma de decisiones basada en un sistema así constituido, por ejemplo, a la hora de pedir un préstamo. Igualmente, ocasionaría discriminaciones en vuestro ámbito al decidir a quién contratar o despedir si tiene sesgos de edad, raciales, religiosos o sexistas.

↘ 3.6
Amenaza a las democracias

Muchos expertos temen que pueda estimular la inestabilidad política y, con ella, la económica y social. La razón es que es una herramienta con la que se puede manipular cualquier proceso democrático. De esta manera, puede llevarnos a una situación de desconfianza generalizada.Para empezar, entraña cierto peligro en el tratamiento de la información dentro del proceso democrático. Si ya habéis apreciado la esfera mediática en la que se han convertido las redes sociales, imaginad lo que supondría alimentarlas con información no verificada y que mezcla opiniones y conocimientos. Sería un gran difusor de noticias falsas. Algunas personas podrían utilizarlo con fines de desinformación con la finalidad de distorsionar la opinión pública. Asimismo, podría tener un gran impacto en el sentido del voto en una u otra dirección. La ciudadanía se quedaría sin capacidad para tomar decisiones informadas y autónomas. En definitiva, todos estaríamos en manos de los propietarios de empresas privadas con fines comerciales que nos proveen de inteligencia artificial.

4. ¿Qué peligros nos acechan en el futuro inmediato?

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha elaborado una lista con las principales amenazas que prevé que habrá en el futuro inmediato, concretamente, en 2030. Según sus cálculos, los peligros estarán diversificados y serán muy parecidos a los actuales, pero con matices más complejos por las tecnologías empleadas. Destacan:

1. Campañas de desinformación avanzada. Ya las hemos podido ver en numerosas campañas electorales a nivel mundial.
2. Aumento de comportamientos autoritarios en los poderes públicos y de la vigilancia digital, y como consecuencia, una pérdida de privacidad.
3. Errores humanos, la mayoría de ellos, en el entorno de los sistemas ciberfísicos actuales.
4. Ataques por medio de dispositivos inteligentes.
5. Incremento de amenazas híbridas.
6. Falta de habilidades.
7. Sobreutilización de la Inteligencia Artificial.

En resumen, la ciberseguridad 2.0 es extremadamente importante y conviene que os familiaricéis con ella. Pese a que hay partes no exentas de polémica, constituirá un paso de gigante en la forma de abordar la seguridad en las pymes con la ayuda inestimable de la IA. Por tanto, es vital una formación de calidad y os invitamos a participar en nuestros cursos y seminarios. “¡Consultad nuestra agenda y apuntad las fechas de vuestro interés!” esta alineada de forma diferente.

ticnegocios.es