PROSEGUR RESEARCH

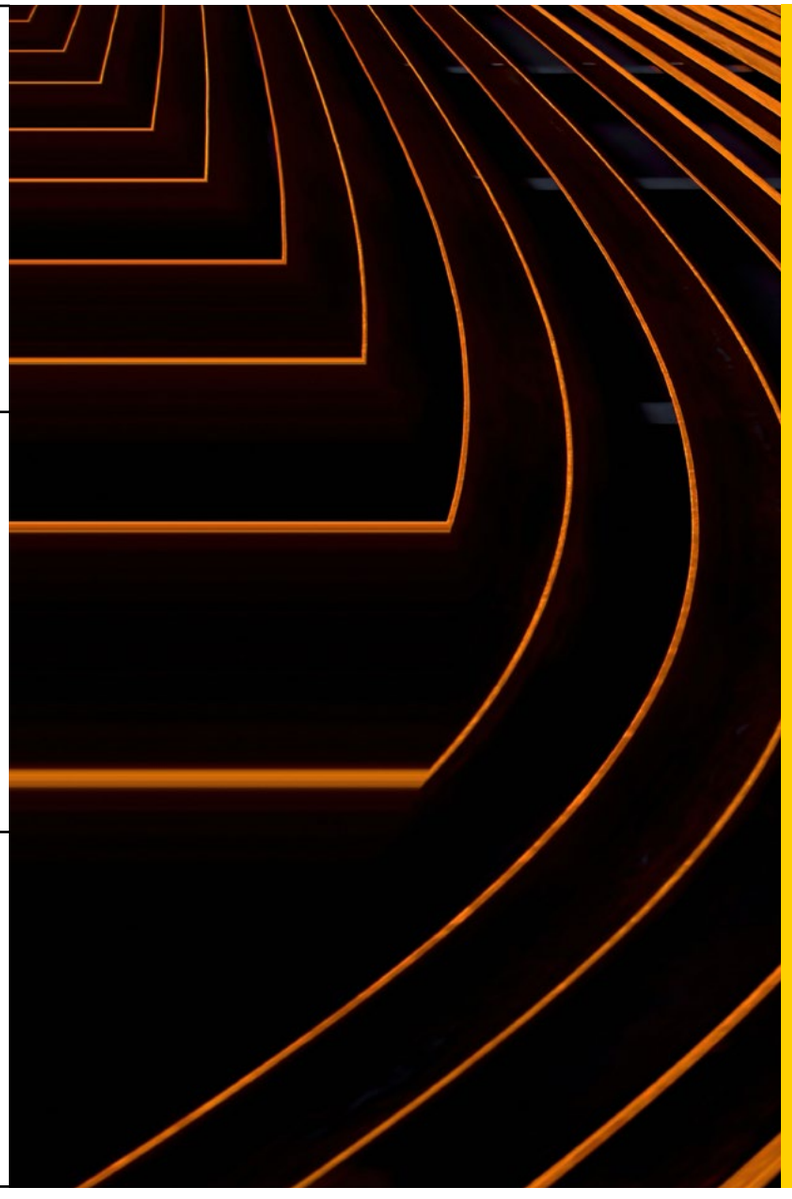
Highlights

ChatGPT: riesgos y oportunidades para la seguridad

PROSEGUR

PROSEGUR RESEARCH
Highlights

Contenidos



01

Introducción: la tecnología como herramienta para el futuro

PROSEGUR RESEARCH

Highlights

Vivimos momentos apasionantes; no cabe duda. Y posiblemente **asistimos al inicio de una nueva revolución** que va a afectar a todas las facetas de nuestras vidas: educación, comunicación, trabajo, relaciones personales y el binomio hombre-máquina.

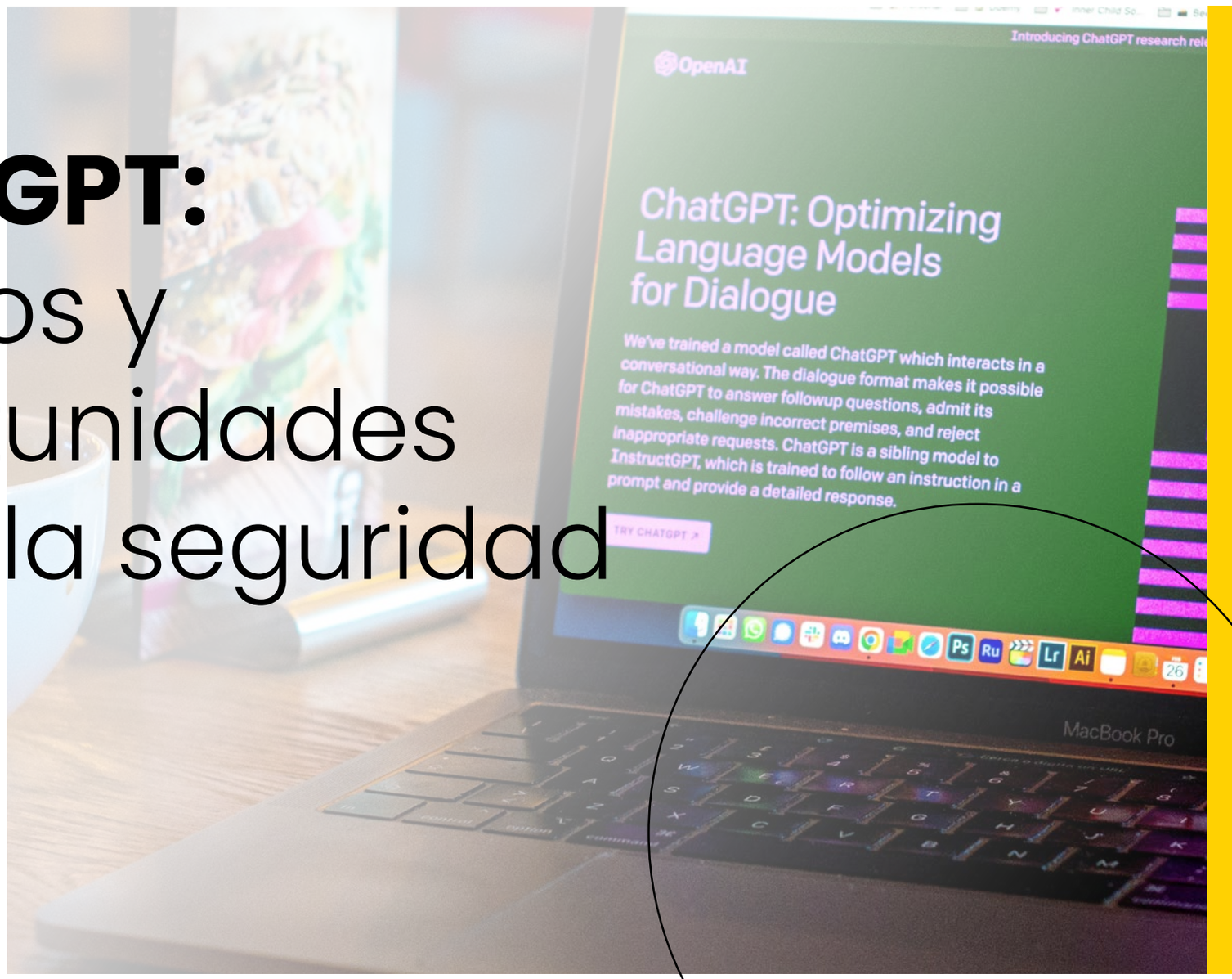
Adaptarnos a los nuevos desarrollos tecnológicos requiere una mentalidad de crecimiento que asuma **la única constante que experimenta el mundo: el cambio.** Sin embargo, el mundo en el que vivimos requiere una toma de decisiones cada vez más compleja y variada, intrincada por diversos factores de carácter internacional como las crisis económicas, las emergencias sanitarias o las disrupciones tecnológicas entre las que destaca la computación cuántica.

En este proceso de cambio **la tecnología juega un importante papel como palanca de desarrollo.** Es por este motivo que se considera uno de los grandes game changers del futuro, afectando a todas las áreas de nuestras vidas y a la práctica totalidad de empresas repartidas por todo el globo.

Este crecimiento exponencial acelerado, junto con la convergencia tecnológica, aumenta la complejidad de todo lo que nos rodea, al mismo tiempo que nos permite hacer lo aparentemente imposible.

02

ChatGPT: riesgos y oportunidades para la seguridad



PROSEGUR RESEARCH

Highlights

ChatGPT, popularizado en los últimos meses, es uno de los desarrollos de inteligencia generativa que se han puesto a disposición del público en general. Entendemos por ello una **forma de aprendizaje automático, basado en modelos de lenguaje, capaz de generar contenido nuevo en cualquier formato** (texto, imagen, vídeo, voz, código). Previamente aplicaciones como Dall-e, Midjourney o Stable Diffusion asombraron por su capacidad para realizar imágenes de alta calidad a partir de texto. Hace unas semanas Microsoft presentó su propuesta de Bing con IA, cuya potencialidad es mucho mayor que la de ChatGPT. Además, en breve se espera el lanzamiento de Bard, la solución de Google. Y mientras tanto proliferan multitud de propuestas que no se limitan a ofrecer resultados textuales basados en modelos de lenguaje, sino a la generación y combinación de cualquier tipo de contenido.

Como decíamos, no cabe duda de que la **tecnología apoya el progreso.** Los enormes avances tecnológicos han mejorado aspectos tan fundamentales para el ser humano como la comunicación, la educación o la sanidad. Pero también conocemos, especialmente desde el ámbito de la seguridad, que **toda oportunidad genera nuevas amenazas,** al igual que de muchas amenazas se pueden detectar oportunidades.

Es por ello que desde Prosegur Research señalamos los **principales diez riesgos para la seguridad de este desarrollo tecnológico:**

PROSEGUR RESEARCH

Highlights

Riesgos para la seguridad de ChatGPT

1

Lucha de poder geopolítico y geoeconómico

En un contexto de poderes difusos y fragmentados, el liderazgo ya no sólo se mide por la capacidad económica, la diplomática o la militar. En el año 2017 Vladimir Putin señaló que quien dominara la inteligencia artificial (IA) dominaría el mundo. La geopolítica y la geoeconomía presentan nuevos riesgos, pero también oportunidades para Estados y empresas que sepan leer el futuro. Los datos, además de las tecnologías, están en el centro de configuración del poder, generando una asimetría entre quienes disponen de ellos y quienes no.

2

Polarización social

Las IA generativas, dada su capacidad de producir contenidos multimedia, pueden ser utilizadas para expandir mensajes de odio o discriminación, así como difundir mensajes de carácter radical o extremista.

3

Desinformación

A través de la generación de noticias falsas se pretende influir en la opinión pública, dañar la cohesión social o afectar a procesos electorales. La desinformación es una clara cuestión que afecta a la seguridad nacional, dañando la cohesión social y los principios democráticos.

4

Doxing

La desinformación también es susceptible de afectar a empresas y organizaciones, con la difusión de bulos, informaciones sesgadas, la creación de falsos perfiles laborales o la manipulación de documentos para dañar la credibilidad de las organizaciones. Su finalidad puede ir desde la parodia hasta el ataque a la reputación o la influencia en los mercados.

PROSEGUR RESEARCH

Highlights

5

Generación de chatbots maliciosos con objetivos delictivos

Destaca la interacción con individuos para la obtención de información sensible o fines ilícitos económicos.

6

Suplantaciones de identidad

Mediante la utilización de los denominadas “deep fakes” y la capacidad de la IA para generar textos, imágenes, vídeos e incluso simular la voz. Apoya la creación de avatares que integren todos estos elementos, aumentando la verosimilitud de la identidad.

7

Generación de código malicioso

Como virus, troyanos, malware, ransomware o spyware, entre otros, con el objetivo de cometer ciberdelitos de diferente naturaleza.

8

Phising

Generación automatizada de correos de apariencia real con objeto de engañar a usuarios a efectos de acceder a información confidencial o a los sistemas informáticos. Las IA generativas redactan contenido con gran calidad, lo que invalida las sospechas que un phishing con baja calidad puede despertar.

PROSEGUR RESEARCH
Highlights

9

Fuga de información y robo de datos

Empresas como Amazon o Google han alertado a sus empleados sobre los riesgos de compartir información sobre la empresa en ChatGPT y aplicaciones similares, que posteriormente pudiera ser desvelada en las respuestas que ofrece a usuarios.

10

Fraudes y estafas

Son tipologías delictivas que crecen fuertemente en los últimos años. Los fraudes tradicionales, existentes en todos los sectores económicos, son potenciados por el uso de internet, redes sociales y nuevas tecnologías. Las IA generativas pueden contribuir a diseñar fraudes con mucha más calidad, así como a perfilar objetivos.

PROSEGUR RESEARCH

Highlights

Ahora bien, **la tecnología, como gran factor de cambio de nuestras sociedades,** no nace generalmente orientada a un uso malicioso, sino que éste viene determinado y potenciado por la acción humana: basta con recordar que, según IBM, ***hasta el 95% de los ciberataques se deben a fallos humanos.***

Por este motivo, no sería ni justo ni proporcionado destacar potenciales riesgos sin señalar, de la misma manera, las oportunidades que ChatGPT puede generar en el campo de la seguridad. Desde Prosegur Research indicamos **diez principales oportunidades de ChatGPT en materia securitaria:**

1

Automatización de tareas rutinarias en funciones de seguridad

Ello, a su vez, potenciaría las competencias más humanas y facilitaría el bienestar de los empleados al eliminar tareas repetitivas y tediosas.

2

Generación de chatbots atractivos

Con un perfil más atractivo para el consumidor, se mejoraría la interacción con clientes y con otros humanos, fomentando la customización que en la actualidad se requiere por parte de las compañías.

PROSEGUR RESEARCH

Highlights

3

Acceso a ingentes cantidades de información de interés para la seguridad, de una manera estructurada por el uso del lenguaje natural

Las capacidades inteligencia de fuentes abiertas (OSINT) pueden verse ampliamente beneficiadas, siendo siempre conscientes de la criticidad de evaluar la fiabilidad de las fuentes y la credibilidad de la información.

4

Análisis de riesgos

Apoyo en la detección y catalogación de riesgos para las organizaciones en multitud de sectores.

5

Reconocimiento de patrones

El valor no estaría únicamente en el patrón, sino en la anomalía: aquello que se sale de lo habitual y puede contribuir a generar una señal débil o una alerta temprana en un entorno de gran volumen de datos y volatilidad.

6

Apoyo en el análisis de inteligencia

Puede contribuir a la generación de hipótesis, la identificación de tendencias y la construcción de escenarios en seguridad. Aunque la IA no puede sustituir la creatividad humana sí puede resultar un complemento interesante para pensar fuera de la caja.

PROSEGUR RESEARCH

Highlights

7

Estructuración de recomendaciones en cuestiones de seguridad

Desde cómo defenderse de un ciberataque hasta qué medidas de seguridad adoptar previamente o durante un viaje. No obstante, esta labor no puede sustituir de ninguna manera la labor de un analista de seguridad internacional, que cuenta con competencias puramente humanos que enriquecen el análisis.

8

Analítica predictiva

Puede facilitar ciertas predicciones, con sus probabilidades asociadas, en base a la ingente cantidad de datos en que se basa.

9

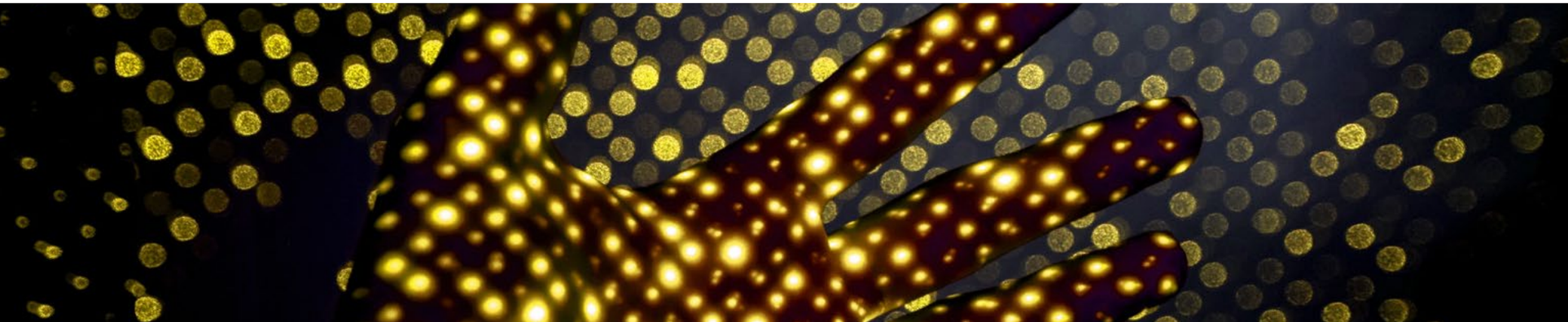
Prevención y detención de ciberdelitos

En ciberseguridad puede apoyar la detección de phishing, probar y testar código, identificar vulnerabilidades, generar contraseñas seguras, simular conversaciones con actores adversarios e incluso con potenciales objetivos, para poder anticipar sus acciones, entre otros efectos.

10

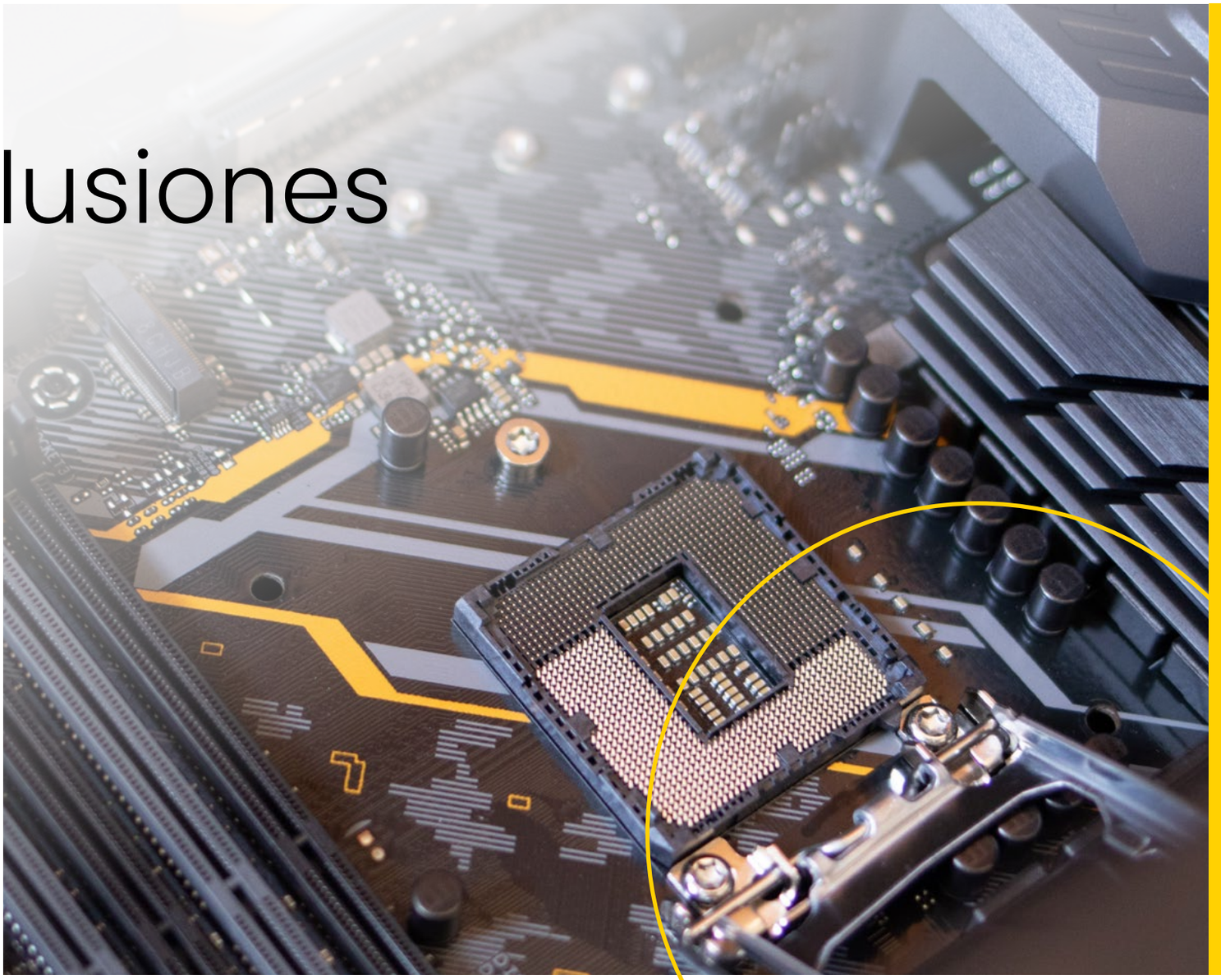
Aprendizaje

Las IA generativas pueden ser un primer punto para el aprendizaje sobre cuestiones vinculada a seguridad, especialmente tecnologías o riesgos.



03

Conclusiones



PROSEGUR RESEARCH

Highlights

Como acertadamente señala Xavier Marcet, “las tecnologías nos empoderan si no dejamos de pensar, pero si dejamos de pensar, solamente nos hipnotizan”.

Todo profesional de la seguridad debe reconfigurar sus habilidades de una forma continua, para afrontar el presente y el futuro con nuevas herramientas. Ello va a implicar que modifiquemos nuestros modelos mentales, y pensar de manera diferente para abordar el cambio de manera propicia, sabiendo aprovechar todas las oportunidades que se nos presentan.

Solo los ciudadanos empoderados y las empresas con propósito son capaces de lograr los resultados deseados, guiados por una línea de objetivos definida y ambiciosa: contribuir al bienestar global. Liderar esta tarea supone un reto, pero contar con expertos que cuentan con capacidades potenciadas por tecnologías disruptivas lo hace posible.

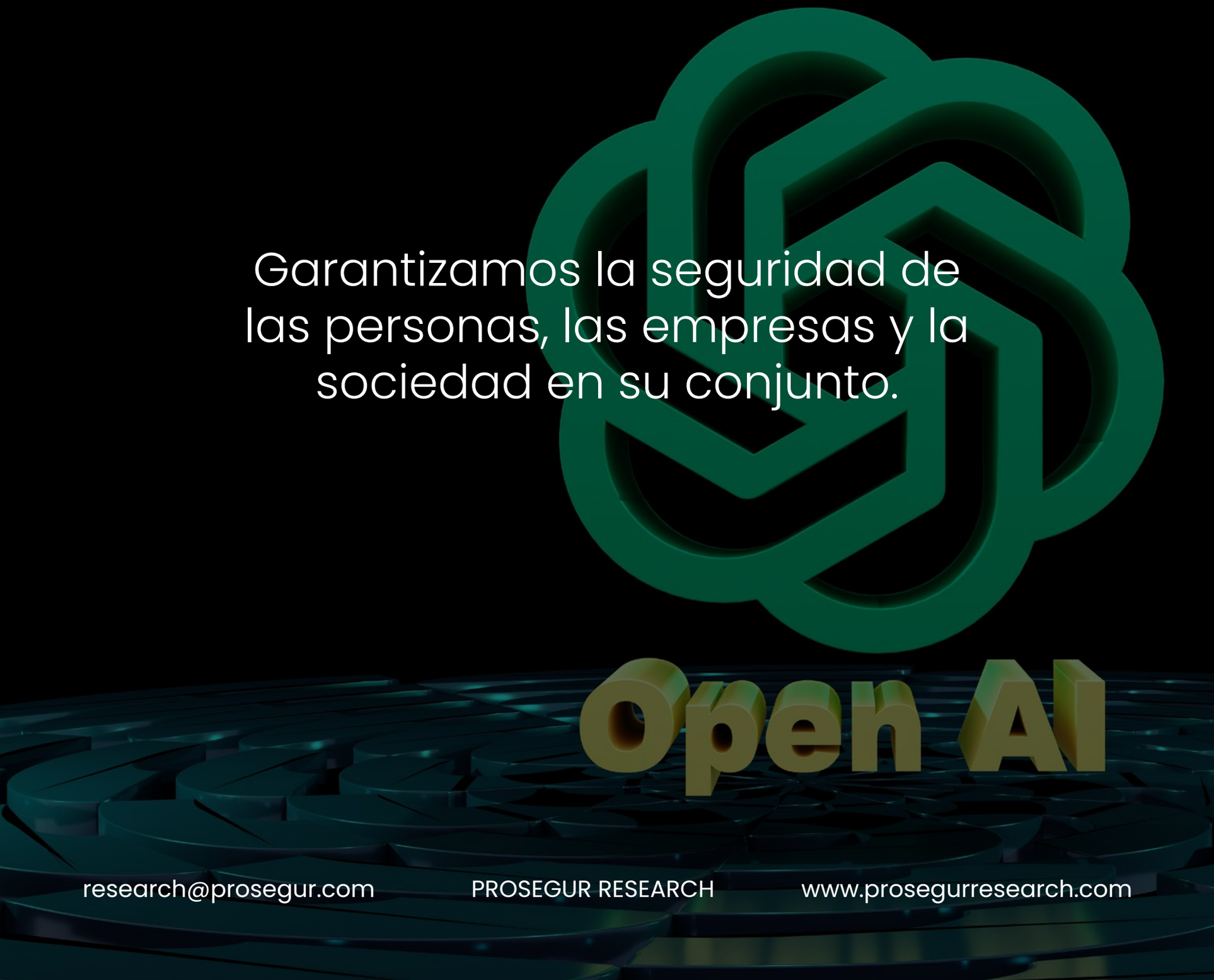
Y, como no podía ser de otra manera, ChatGPT nos recuerda que el futuro es incierto, al mismo tiempo que en el mundo están sucediendo hechos positivos, como las mejoras en la calidad de vida de muchas personas o los esfuerzos en materia social y ambiental.

Todos nosotros somos protagonistas del avance humano, tecnológico y social, y debemos ser responsables del legado que dejemos a los que nos sucederán. Porque sin progreso no hay futuro.

El futuro es incierto y puede ser influenciado por una variedad de factores. Es importante trabajar juntos para crear un futuro mejor y más justo para todos, y esto puede requerir la colaboración internacional y la adopción de soluciones creativas. También es importante considerar el impacto de nuestras acciones en el medio ambiente y en la sociedad, y buscar maneras de reducir el impacto negativo y promover un mundo más sostenible.

Fuente: ChatGPT, 2023

PROSEGUR



Garantizamos la seguridad de las personas, las empresas y la sociedad en su conjunto.

research@prosegur.com PROSEGUR RESEARCH www.prosegurresearch.com