PROSEGUR RESEARCH

Hybrid Security Series

La ola distópica de la inteligencia artificial: un marco de competencias

2024

PROSEGUR
SECURITY

Este documento es **interactivo**

HOME

01 **Un tsunami llamado IA** pág. 3

02 **Ante la inquietud, reflexión** pág. 10

03 **El empoderamiento como hábito** pág. 15

04 **La IA en un ecosistema empresarial ampliado** pág. 21

01

Un tsunami llamado **IA**

HOME

01
Un tsunami llamado IA

02
Ante la inquietud, reflexión

03
El empoderamiento como hábito

04
La IA en un ecosistema empresarial ampliado

01 UN TSUNAMI LLAMADO IA

La tecnología lleva acompañando al ser humano desde hace miles de años, debido a la tendencia humana de reinventar y tratar de buscar soluciones a problemas complejos. Las primeras técnicas agrícolas, la rueda o los sistemas de engranajes son solo algunos ejemplos. **Desde el siglo XX el desarrollo tecnológico ha vivido con internet un crecimiento exponencial** que, como una gran ola de cambio, ha ganado gran protagonismo dada las oportunidades y potenciales derivadas de su convergencia.

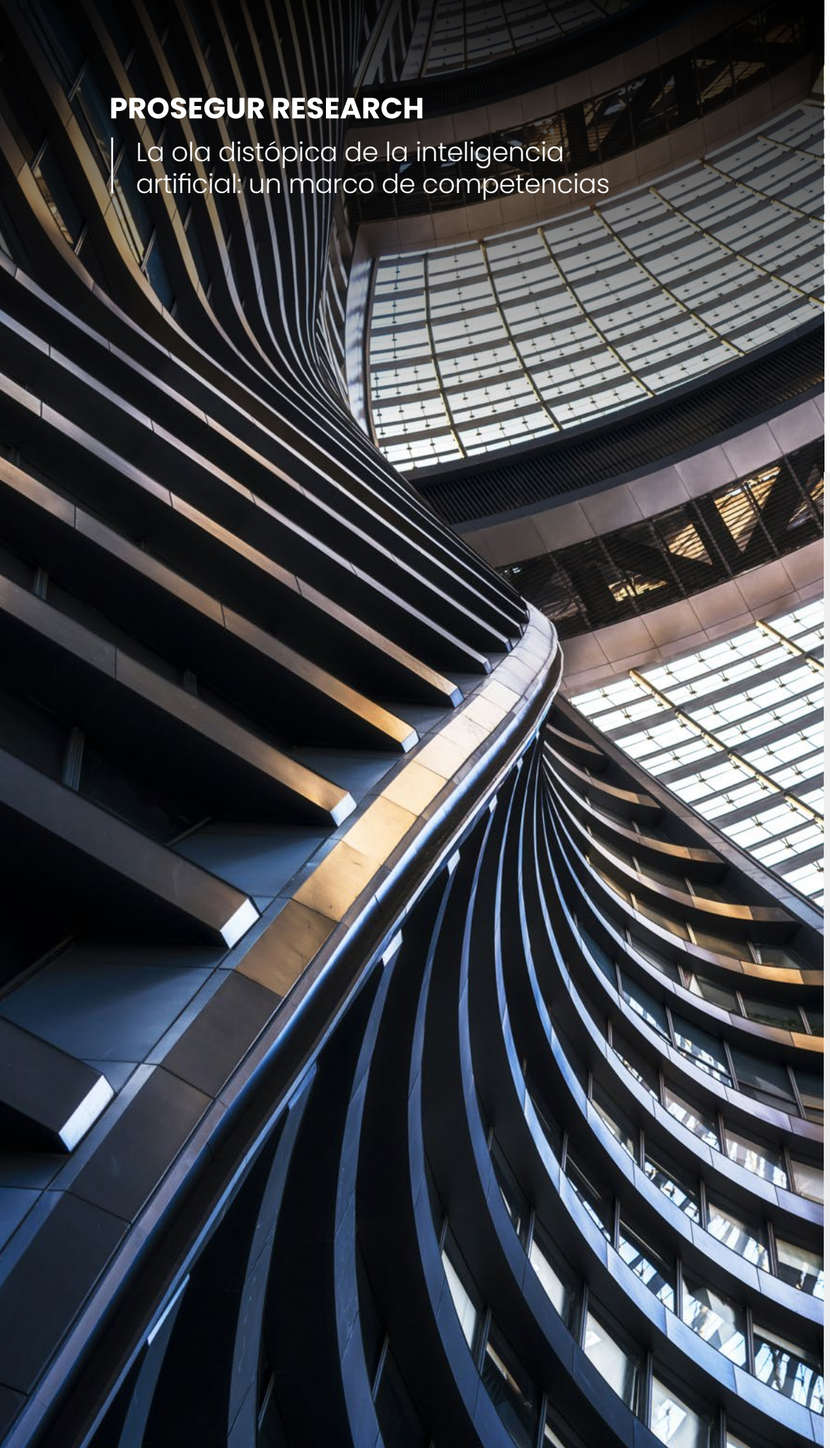
En este contexto, la **inteligencia artificial,** un concepto tan antiguo como la propia computación y que fue acuñado en la década de los 50, ha vivido un gran **auge dada la explosión de los datos digitales y los avances en la capacidad de procesamiento informático.** Estas olas de cambio contienen importantes transformaciones para las sociedades y son nuestras decisiones del presente sobre el desarrollo tecnológico las que originarán los impactos a múltiples niveles del mañana.

La **inteligencia artificial** (IA) es una "tecnología que aplica análisis avanzados y técnicas basadas en la lógica, principalmente el machine learning, para interpretar eventos y respaldar y automatizar decisiones".

Dentro de la IA se encuentra la IA generativa, una herramienta que, junto a otras prácticas que definen esta tecnología -optimización, heurística, machine learning, simulación-, ofrece la capacidad de crear contenido creativo y original, simulando el comportamiento y el razonamiento que sigue el ser humano en tareas no informáticas.

MIT

HOME

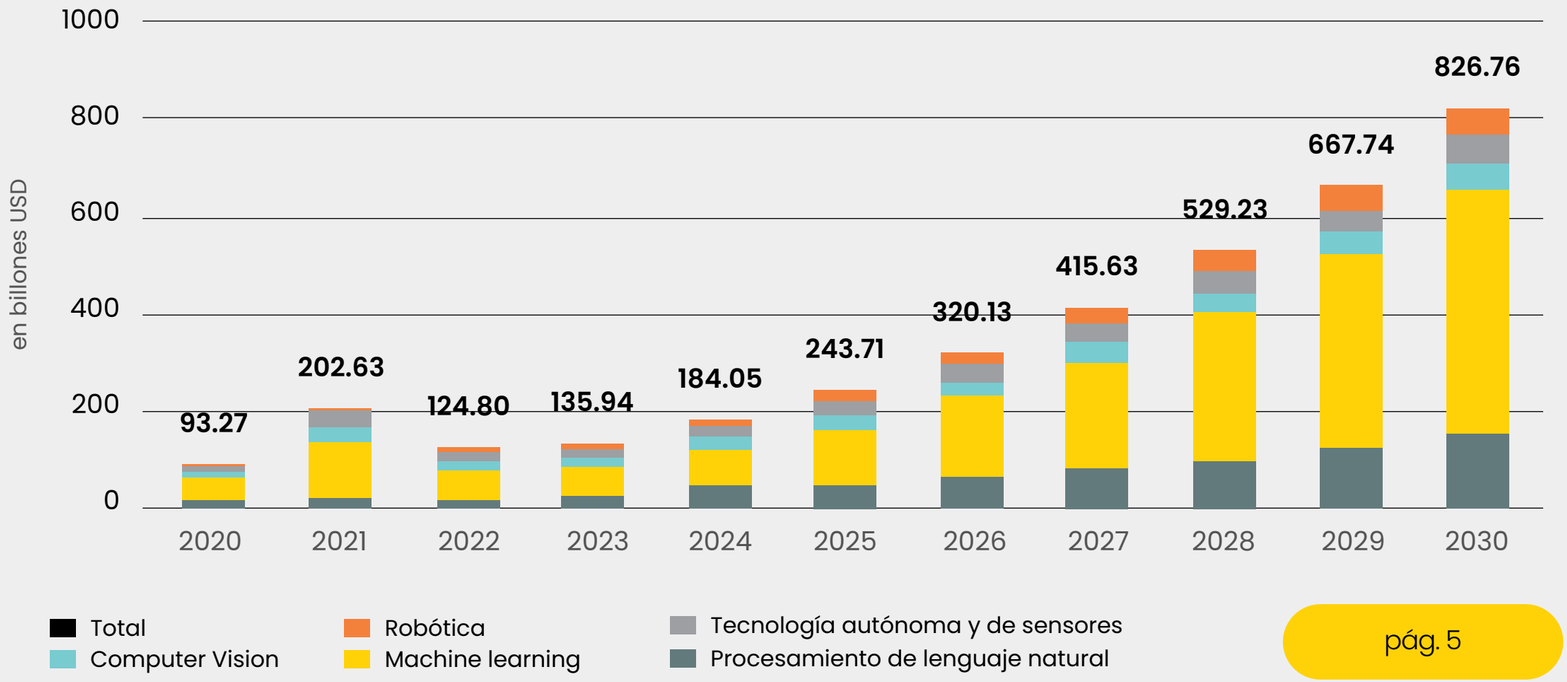


HOME

Tras décadas de desarrollo, el papel de la IA en el mercado mundial se prevé que registre un **crecimiento anual medio del 28,46%,** pasando de 184.000 millones de euros en 2024 a 826.000 millones en 2030. En este contexto, dentro de las distintas modalidades que integran la IA se estima que las relacionadas con el machine learning y el Procesamiento de Lenguaje Natural (PLN) representen el mayor volumen de mercado.

Gráfico 1
Volumen de mercado de la IA

Fuente: Prosegur Research, 2024
basado en Statista Market Insight

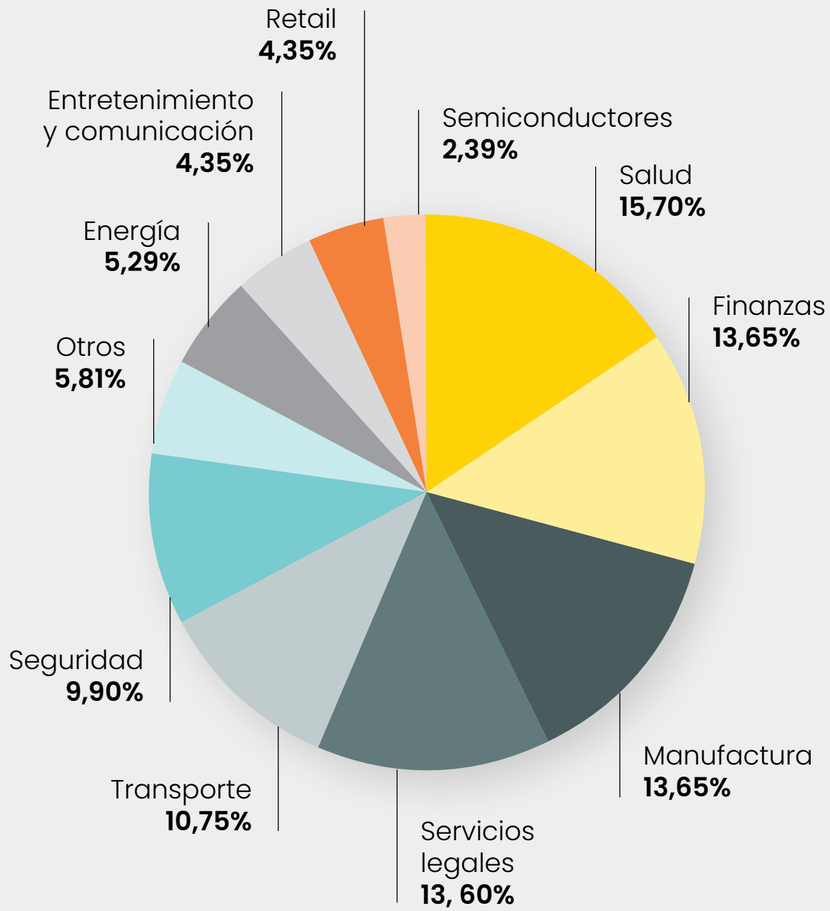


pág. 5

La democratización que presenta el acceso a este tipo de tecnología ha propiciado su inclusión en una gran diversidad de campos, ofreciendo modelos que permiten labores de clasificación o reconocimiento autónomo e incluso la generación de contenido original. Se prevé que estas nuevas capacidades registren un elevado impacto en el mercado laboral. Según el FMI y **Standford,** afectando al **40% de los puestos de trabajo en todo el mundo,** generando una transformación del mercado laboral al modificar las necesidades técnicas para la mano de obra y potenciando habilidades informáticas, como el manejo de lenguajes de programación y análisis de datos.

La implementación de la IA entre las herramientas de las organizaciones demuestra tratarse de un factor disruptivo, redefiniendo la manera en que son concebidos sectores industriales tradicionales. Según el **Artificial Intelligence Index Report,** atendiendo al volumen de inversión privada en el 2023, **se prevé que las áreas relacionadas con la gobernanza/reseach, servicio al cliente, procesamiento y gestión de datos, medicina o Fintech posean un mayor impacto y transformación por el empleo de la IA.**

Gráfico 2
Volumen de mercado por Industria



Fuente: Prosegur Research, 2024 basado en Statista Market Insight

HOME

HOME

De acuerdo con Gartner, toda tecnología pasa por un ciclo de vida con cierto nivel de homogeneidad, desde su concepción hasta su adopción masiva y estabilización en los mercados. En el gráfico, se analiza la proyección esperada de la IA, en sus distintos tipos y vertientes *(ver Glosario).*

En conjunto, la IA vendría sufriendo un **vertiginoso ascenso en un tiempo reducido.** En primer lugar, el pico de expectativas, una fase de gran expectación y entusiasmo en la concepción de futuras implicaciones, quedaría encabezado por la IA Generativa, seguida de la IA Responsable y la IA General como tecnologías destacadas.

Al no ser capaz de cumplir con inmediatez expectativas y futuribles, por lo general, poco realistas, la IA ingresaría en el valle de la desilusión, disminuyendo el grado de atención mediático en su derredor, así como el énfasis en su desarrollo.

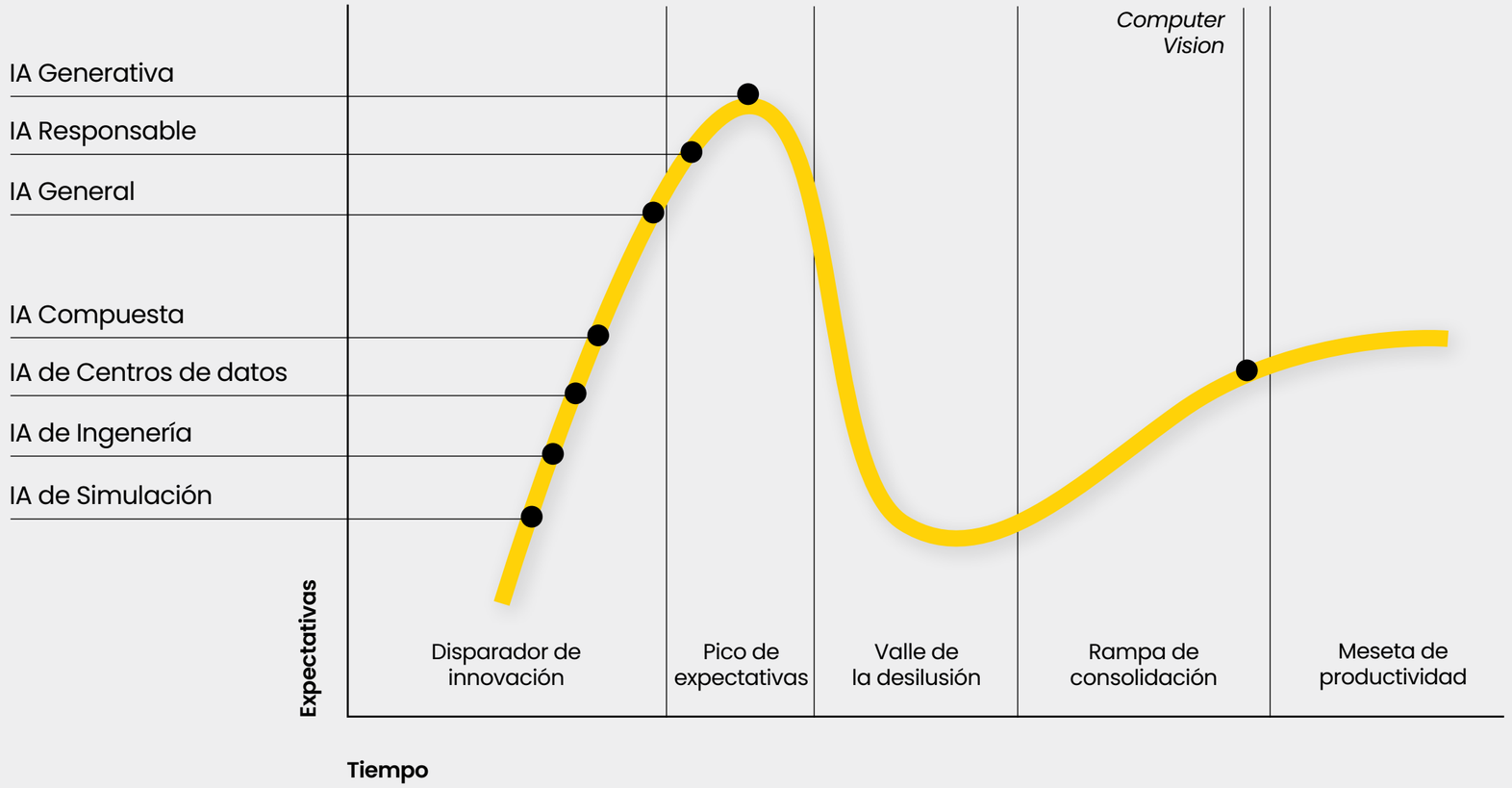
Luego de superar problemas y limitaciones en el diseño, la IA sufrirá un ascenso sostenido y moderado en el tiempo, con **orientación a la producción efectiva de beneficios prácticos.**

En la meseta de productividad, la tecnología se estabilizaría, formando **parte activa y productiva del mercado,** generalizando su adopción al demostrar resultados eficaces y eficientes.

Gráfico 3

Ciclo de expectación de tecnologías emergentes de Gartner
(Hype Cycle for Emerging Technologies)

Fuente: Prosegur Research, 2024 basado en Gartner



Olas disruptivas

Analizar la inteligencia artificial es pasado, presente, pero sobre todo, como tecnología prometedora, **es pensar en futuro.** Como si de un tsunami se tratara, la creciente implementación de la IA en ámbitos y sectores de manera amplificada puede llevar a **olas disruptivas que generen escenarios distópicos** relacionados con las preocupaciones citadas. A continuación, se comparten algunos puntos de interés:

A

Mundo phygital

- La IA acerca los mundos físico y digital, provocando una **excesiva dependencia** en la tecnología y acentuando el impacto de la **desigualdad tecnológica.**
- Fenómenos criminológicos combinan más conductas físicas y digitales, así como la **seguridad física** y la **ciberseguridad** cada vez están más **interrelacionadas.**

B

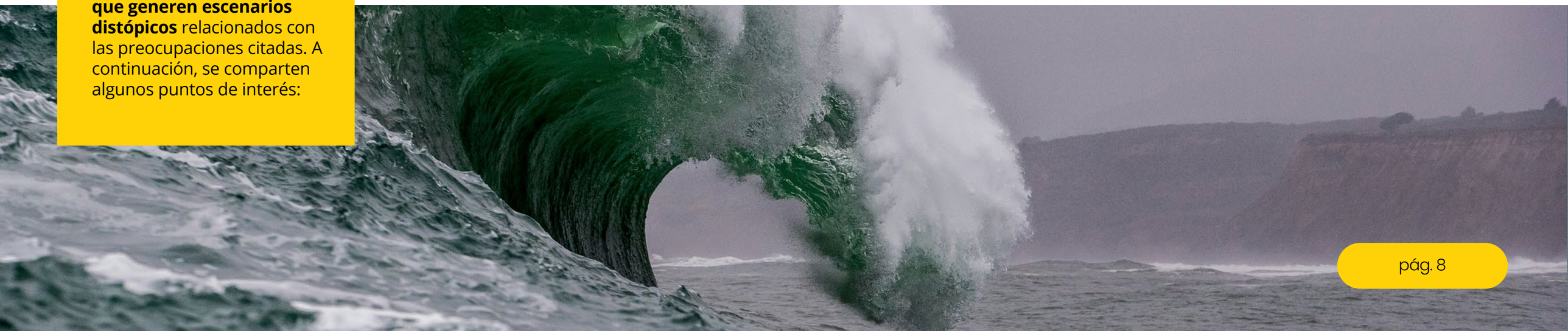
Cambio de reglas del juego

- La convergencia tecnológica va más rápido que la regulación y la adaptación del sistema y modifica numerosos aspectos de la sociedad, a la par que crea **nuevas distribuciones de poder y de capacidad,** afectando desde organizaciones y países hasta empleados y ciudadanos.

C

Alucinaciones artificiales y sesgos naturales

- En función de su programación, la IA puede **potenciar los sesgos y la discriminación** en la toma de decisiones, especialmente en los casos donde las personas depositen una elevada credibilidad en la máquina.
- Las llamadas **alucinaciones,** o respuestas seguras de la IA que no parecen estar justificadas por su entrenamiento, se configuran como otro elemento estructural que puede crear deficiencias en la toma de decisiones.



D

Homo legalis

- La sobrerregulación reactiva, sin medidas preventivas ni estrategias proactivas, podría conducir a un escenario donde el **exceso de restricciones,** en lugar de fomentar el desarrollo responsable, genere parálisis en la innovación y **estancamiento tecnológico.**

E

Datos (con)sentidos

- La cesión de datos y su utilización algorítmica requerida para el funcionamiento de la IA puede generar enormes **problemas de privacidad y ética** si los usuarios carecen del debido control, consentimiento y transparencia.
- Es necesario proteger los datos del cliente; así lo **exige cada vez más el usuario.** A su vez, en aquellos que se consienta su uso y este sea ético, permiten anticipar innumerables problemas de seguridad, salud, etc.

F

Pensamiento acrítico

- La capacidad de confeccionar deepfakes con vídeo, imagen o voz se adhiere al progresivo incremento de la desinformación en las noticias. Esta combinación puede generar una **erosión de la confianza** en las fuentes de información tradicionalmente confiables, transformando el pensamiento crítico en cinismo y teniendo como consecuencia el **desinterés en el conocimiento.**

Generar un **ecosistema de confianza** basado en la legalidad, la transparencia y el respeto a los derechos humanos permitiría el avance y la **innovación de la IA** de una forma **responsable y centrada en el buen uso,** desde una perspectiva ética en su diseño.

HOME

Confiabilidad, posiblemente el mayor reto de futuro

La opacidad, la ubicuidad y la falta de medios para cuestionar la IA cuando produce resultados inesperados, perjudiciales, injustos o discriminatorios, siembran la sospecha y la desconfianza entre sus usuarios.

Esto puede derivar en la intensificación de **corrientes que promueven la reducción en el uso de las tecnologías,** incrementando sentimientos naturalistas, antiglobalistas o minimalistas digitales con reclamaciones sobre la limitación en el consentimiento del uso de datos por miedo al abuso. Asimismo, incluso aumentando las acciones dirigidas a la **paralización de actividades y el boicot,** como los movimientos de neoluditas o primitivistas.

02

Ante la inquietud, **reflexión**

HOME

01
Un tsunami llamado IA

02
Ante la inquietud, reflexión

03
El empoderamiento como hábito

04
La IA en un ecosistema empresarial ampliado

02

ANTE LA INQUIETUD, REFLEXIÓN

> No es que nada esté en llamas. Es que todos en nuestra organización están sosteniendo un lanzallamas.
>
> ***Generative AI-nxiety,***
> **Reid Blackman**

Desde el punto de vista empresarial, y teniendo en cuenta el carácter multidisciplinar de la IA, esta tecnología muestra una **doble proyección:**

- Por un lado, una mayor exposición a las amenazas emanadas de la esfera digital **incrementa la vulnerabilidad de las compañías,** convirtiendo a la IA en un activo de riesgo susceptible de generar fricciones con aspectos del derecho e incluso la integridad de los sistemas o protocolos de seguridad.

- Por otro lado, se convierte en el **núcleo de la estrategia de seguridad integral** a la vez que, como herramienta, potencia las capacidades de los empleados en diversas materias de trabajo, aumentando la productividad y optimizando costes.

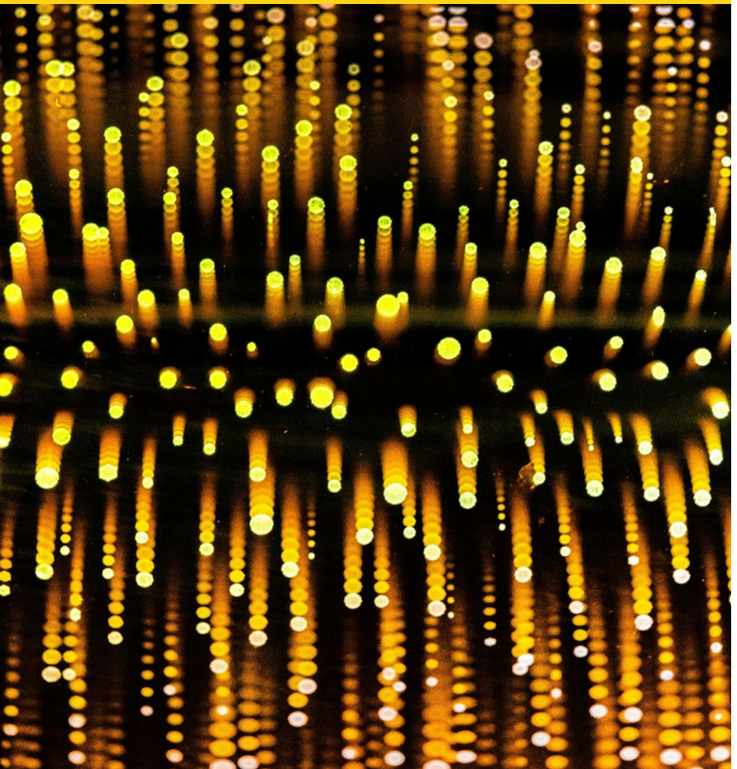
HOME

PROSEGUR RESEARCH

La ola distópica de la inteligencia artificial: un marco de competencias

Malos usos

La inteligencia artificial potencia las **actividades ilícitas** de muy diversas formas, desde su diseño e implementación hasta su uso.
Algunas de ellas pueden ser:



Potenciación del crime as a service

La IA plantea el riesgo de profesionalizar el cibecrimen y facilitar la democratización de la prestación de servicios criminales a usuarios no expertos. Esta dinámica es denominada por **Europol** como la economía criminal compartida, donde el **crime as a service** adquiere una creciente relevancia: la automatización de ataques, la generación de contenidos maliciosos y la optimización de redes de botnets para facilitar ataques de denegación de servicio (DDoS) son solo algunos ejemplos de fórmulas difíciles de mitigar, eficientadas gracias a la IA.

IA para todo tipo de fraudes

La ya señalada capacidad de la IA para diseñar ataques basados en ingeniería social supone un importante apoyo para la comisión de **fraudes o estafas tradicionales** gracias a tareas preparatorias como la suplantación de terceros que induzcan a error a las potenciales víctimas o la gestión de distribuciones masivas a través del mail. Esto también puede servir como apoyo a otros tipos de delitos informáticos, afectando en muchos casos al plano físico, especialmente desde dentro de la empresa, como el **fraude interno.**
Además, la IA es capaz de modificar de forma sustancial y sin autorización imágenes y contenidos, dotándolos de nuevos significados y aprovechamientos ilícitos. También potencia robos de información, particularmente **propiedad intelectual,** a través de softwares maliciosos o ataques de fuerza bruta, lo que, junto a la mayor capacidad a la hora de analizar y procesar grandes cantidades de información, está registrando una gran proliferación en el **fraude financiero.**

Gran aliada del crimen organizado

La IA incrementa la sofisticación y escala de las actividades relacionadas con la criminalidad organizada. La optimización de **operaciones logísticas** en todo tipo de tráficos, el análisis de grandes cantidades de datos para **fraude financiero y blanqueo de capitales** para ganar sofisticación o el apoyo en **vigilancia y contrainteligencia,** incluyendo el empleo de drones y la gestión de la información para generar ataques dirigidos, son formas en las que la IA potencia la efectividad y la eficacia criminales, sin necesidad de dotarse de un alto nivel de cualificación.

Nuevas fórmulas para espionaje industrial

Las potenciales capacidades que ofrece la IA en cuanto al análisis de big data, monitoreo de redes e ingeniería social la configuran como un activo de alto valor en el entorno criminal relativo al espionaje industrial, pudiendo aplicarse a tareas cuyo objetivo sea **detectar información estratégica, automatizar la vigilancia o diseñar ataques** avanzados contra objetivos de la competencia, incluyendo desde la sustracción de información clave hasta la identificación de fórmulas para manipular a empleados o clientes con el fin de que revelen información confidencial. En el ámbito de la propiedad industrial, además del robo de datos, destaca el **uso de la ingeniería inversa** que puede ayudar a desglosar productos o procesos patentados para comprender su funcionamiento interno y replicarlos sin autorización.

En foco: **wAIponization**

La rápida evolución tecnológica ha facilitado la integración de la IA en una amplia gama de aplicaciones y se erige como un arma de doble filo en materia de seguridad. Así, su aplicación como herramienta en sistemas que pueden suponer una amenaza ha derivado en el surgimiento de un nuevo concepto: **"wAIponization"[1],** que describe el **empleo de la IA como arma en contextos de seguridad,** incluyendo tanto conflictos armados como actividades delictivas.

La IA ya se utiliza ampliamente para una variedad de propósitos, especialmente aquellos relacionados con los sistemas pasivos de seguridad, como la **planificación de operaciones militares, la vigilancia ubicua, el reconocimiento por patrones y la detección de ciberamenazas.**

[1] WAIponization es el resultado de la combinación entre los términos "weaponization", referente al proceso de convertir cualquier elemento en arma, junto con AI, siglas de inteligencia artificial en inglés ("Artificial Intelligence").

Esta imagen se ha creado con inteligencia artificial generativa

No obstante, **su utilización en la toma de decisiones ofensivas,** en la fijación de objetivos o el propio uso de sistemas autónomos de armas impulsados por la IA, se erige como uno de los principales focos de **inversión armamentística** en el medio plazo y plantea importantes desafíos ético-legales en términos de responsabilidad y control humano. Así, la **reducción del factor humano en la conducción de hostilidades** genera fricciones en torno al grado de cumplimiento de los **principios básicos del jus in bello** del Derecho Internacional Humanitario.

En un contexto de incremento de actores no estatales violentos, **la IA empodera a organizaciones criminales** y su uso como arma acentúa la profesionalización al facilitar el acceso a medios operativos más sofisticados.

En los **conflictos armados o disturbios violentos,** el extendido uso de armas inteligentes de bajo coste potencia la **asimetría,** dificultando la capacidad para controlar, anticipar y analizar al adversario; al mismo tiempo que, paradójicamente, empodera a actores que hasta ahora no contaban con capacidades equiparables.

HOME

pág. 13

Buenos usos

Aumentar las capacidades humanas con inteligencia artificial **permite tanto mejorar la seguridad como generar nuevos productos y servicios** para las empresas y personas.

En Prosegur hemos integrado, en nuestro modelo de seguridad híbrida, el desarrollo tecnológico y los buenos usos de IA para ser más eficaces y eficientes al ejercer servicios de seguridad integrales e integrados, con el objetivo de hacer del mundo un lugar más seguro y próspero. A continuación, destacamos algunos de los infinitos buenos usos de la IA en el ámbito de la seguridad:

Reconocimiento de patrones

Permite analizar datos de cámaras de seguridad para **identificar patrones y comportamientos inusuales, así como detectar intrusiones en tiempo real** y alertar de cualquier incidencia. Por ejemplo, en una tienda mediante computer vision, el **vigilante conectado al iSOC** cuenta con información sobre conductas atípicas en base a un algoritmo de elaboración propia que identifica potenciales hurtos en tiendas.

Análisis de flujo de personas y gestión de multitudes

Permite **analizar patrones de movimiento para optimizar la disposición de recursos de seguridad** y ayuda a gestionar grandes multitudes mediante la identificación de situaciones potencialmente peligrosas. En labores de seguridad para **grandes eventos** tanto musicales como deportivos, dicho análisis se realiza mediante el uso de robótica que aporta información sobre los aforos de las zonas y necesidades de mayor apoyo operativo.

Sensores conectados y sistemas de alarma avanzados

Interpreta datos de sensores para identificar amenazas potenciales, como incendios, inundaciones o intrusiones. Los **sensores con IA integrada** son capaces de percibir fuego cuando el humo no es aún detectable para la vista y el olfato humanos.

HOME

Integración con sistemas de gestión

Permite operar a los iSOCs aprovechando la convergencia de la tecnología, los datos en tiempo real y las personas expertas que toman las decisiones de seguridad. Ahora, con un altísimo nivel de capacidad de análisis, se logra una asignación de recursos más eficientes en todo el conjunto de servicios de seguridad vinculados: cámaras, vigilantes, sensores, robots y drones, etc. Esto mejora sensiblemente la detección y la respuesta ante hurtos en supermercados, por ejemplo.

Modelos para el futuro

Los **algoritmos y modelos matemáticos** permiten detectar y anticipar áreas de mayor riesgo en función de datos masivos históricos y actuales, como la información sobre incidentes y delitos. El gran **cambio de paradigma** viene de la mano del uso paralelo de los datos en tiempo real, y el aprovechamiento de estos para identificar cursos de acción a medio y largo plazo.

HOME

03

El empoderamiento como hábito

01
Un tsunami llamado IA

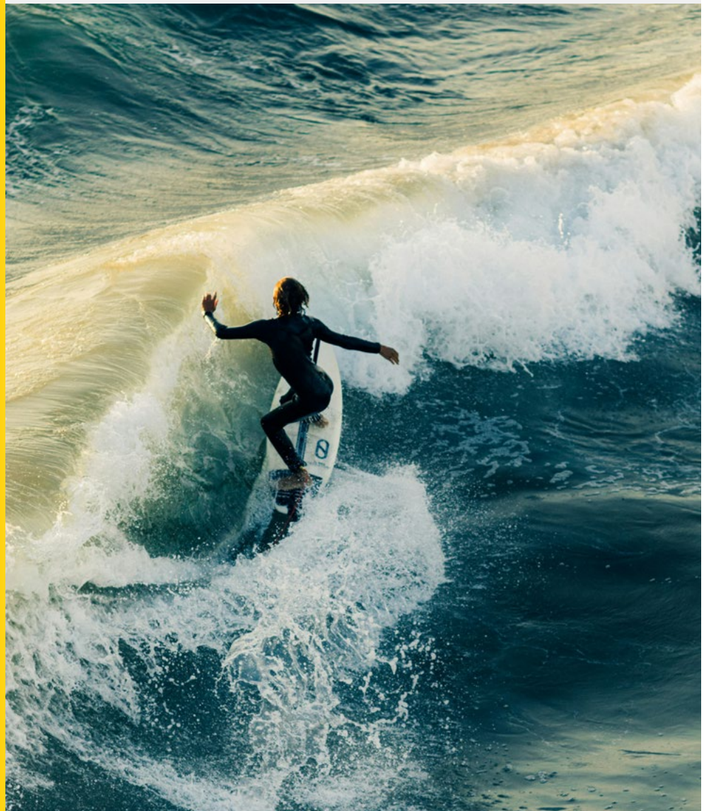
02
Ante la inquietud, reflexión

03
El empoderamiento como hábito

04
La IA en un ecosistema empresarial ampliado

03

EL EMPODERAMIENTO COMO HÁBITO



A pesar de que la IA cuenta con siete décadas de historia, ha sido durante los últimos años cuando se ha incrementado su papel como **driver con potencial de transformación en el panorama laboral,** empoderando las capacidades de los trabajadores en organizaciones de todos los sectores para mejorar la eficiencia, la productividad y la innovación. Sin embargo, **el verdadero valor de la IA no radica en reemplazar a los trabajadores, sino en potenciar sus habilidades.**

En la actualidad el reto de la capacitación en tecnología, habitualmente denominado **Alfabetización Mediática e Informacional** (AMI), es uno de los principales ejes de futuro para el desarrollo corporativo y social, con el objetivo de conseguir **aprovechar al máximo sus beneficios y minimizar, en la medida de lo posible, sus riesgos.** En este sentido, el World Economic Forum (WEF) ha señalado en 2024 los **resultados adversos de la IA como el sexto mayor riesgo global** para la próxima década.

Según algunos datos, aunque el 60% de todos los empleos tienen al menos algunas tareas que podrían automatizarse, **sólo el 5% de los trabajos podrían automatizarse en su totalidad.** Esto, **lejos de ser una amenaza, supone una oportunidad** de gran impacto para las organizaciones: facilitar la burocracia y la automatización de tareas repetitivas y monótonas permitiría la dedicación del tiempo laboral a las labores que requieran las capacidades más puramente humanas, como aquellas relacionadas con la comunicación o la resolución de problemas complejos, entre otras. Además, la IA, junto con la convergencia y el desarrollo tecnológico general, puede **generar campos y nichos de mercado en el futuro que ahora parezcan impensables.** Basta con pensar en las profesiones relacionadas con los influencers o los gamers, que hace apenas unas décadas podrían parecer ciertamente distópicas.

Es en este contexto donde surge el **empoderamiento inteligente,** un marco conceptual basado en la capacitación y la mejora de habilidades humanas gracias a la aplicación tecnológica. Más que la sustitución o mera complementación, **el empoderamiento inteligente busca una simbiosis entre humanos y tecnología disruptiva** para ampliar el abanico de oportunidades a todos los niveles.

A nivel corporativo, una empresa de seguridad debe adaptarse a multitud de situaciones, actores y contextos debido a sus flujos operativos, puesto que cada cliente es único y cuenta con una serie de requisitos y particularidades. Bajo el marco de la **seguridad híbrida, las personas son la esencia misma del modelo,** ya que sin expertos no se pueden llevar a cabo los millares de operaciones, controles y reportes diarios en diferentes puntos geográficos simultáneamente. De esta manera, siguiendo la **taxonomía de habilidades y competencias para la seguridad híbrida** elaborada por Prosegur Research, a continuación se destacan las principales **características del empoderamiento inteligente gracias a la IA:**

1 Competencias **en seguridad**

Debido a la incertidumbre generalizada en la actualidad, recordando términos como VUCA, BANI o TUNA, las empresas requieren **profesionales con conocimiento y experiencia en gestión de riesgos y seguridad** para adaptarse a los contextos y el marco empresarial en el que operan, con una visión sistémica y entendiendo el valor y la transversalidad de todos los procesos organizacionales.

En la **era del dato,** la inteligencia artificial se ha convertido en un catalizador para el empoderamiento del conocimiento en diversas esferas y ámbitos de la actualidad, desde lo geopolítico y geoeconómico hasta lo social o lo regulatorio, con múltiples impactos en las corporaciones. Así, la IA tiene el potencial de **modificar la manera en la que los profesionales de la seguridad** acceden, procesan y aplican la información de la que disponen.

De esta manera, la IA está reconfigurando la recopilación y el análisis de información sobre las dinámicas y tendencias globales. El acceso a fuentes de información y la capacidad de análisis de grandes volúmenes de datos, medios de comunicación y redes sociales es una de las grandes áreas de empoderamiento gracias a este desarrollo tecnológico, con el objetivo de generar hipótesis, definir alertas tempranas, identificar tendencias o realizar evaluaciones de contextos con alta inseguridad, permitiendo tomar decisiones más informadas y efectivas.

2 Competencias **digitales**

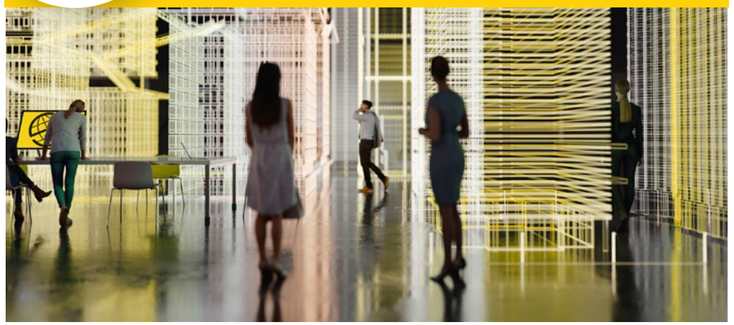
El desarrollo tecnológico, interrelacionado con la evolución de las operaciones corporativas, requiere profesionales en seguridad que conozcan las aplicaciones de las novedades más disruptivas. En la actualidad existen numerosas áreas emergentes, desde el blockchain hasta la computación cuántica, por lo que las empresas deben contar con **equipos diversos, con bagajes multidisciplinares y una visión holística** tanto de la tecnología como de la propia organización.

En el componente digital, las empresas de seguridad han sido testigo durante los últimos años del **traslado paulatino de la conducta humana desde el plano físico al ámbito digital.** Al respecto, los aumentos en ilícitos como las **estafas informáticas** y otras amenazas a la continuidad de negocio y la reputación, como el espionaje industrial o los ciberataques, son resultado de un uso malintencionado de las tecnologías. De este modo, la IA puede desempeñar un papel relevante en la detección de actividades maliciosas, como las interacciones en redes sociales con actividad delictiva o publicación masiva de contenido ilícito, mediante técnicas de valoración de mensajes y perfiles a mayor velocidad que los expertos humanos.

En el componente más puramente tecnológico, conocer el diseño y la implementación de las innovaciones en la materia, requiriendo *hard skills* como programación, permite **establecer servicios operativos con mayor conocimiento sobre las necesidades específicas de seguridad,** como las tareas en la nube o los gemelos digitales, entre otros.

Por tanto, más allá de los riesgos existentes y potenciales, la IA puede suponer un significativo avance en las capacidades de los trabajadores de las empresas de seguridad. Por ejemplo, el análisis automatizado de patrones de comportamiento en circuitos de videovigilancia puede potenciar las capacidades de los centros de operaciones de seguridad (SOC) y las centrales de alarmas, **superando así las limitaciones y sesgos de la atención humana.**

3 Competencias **humanas**

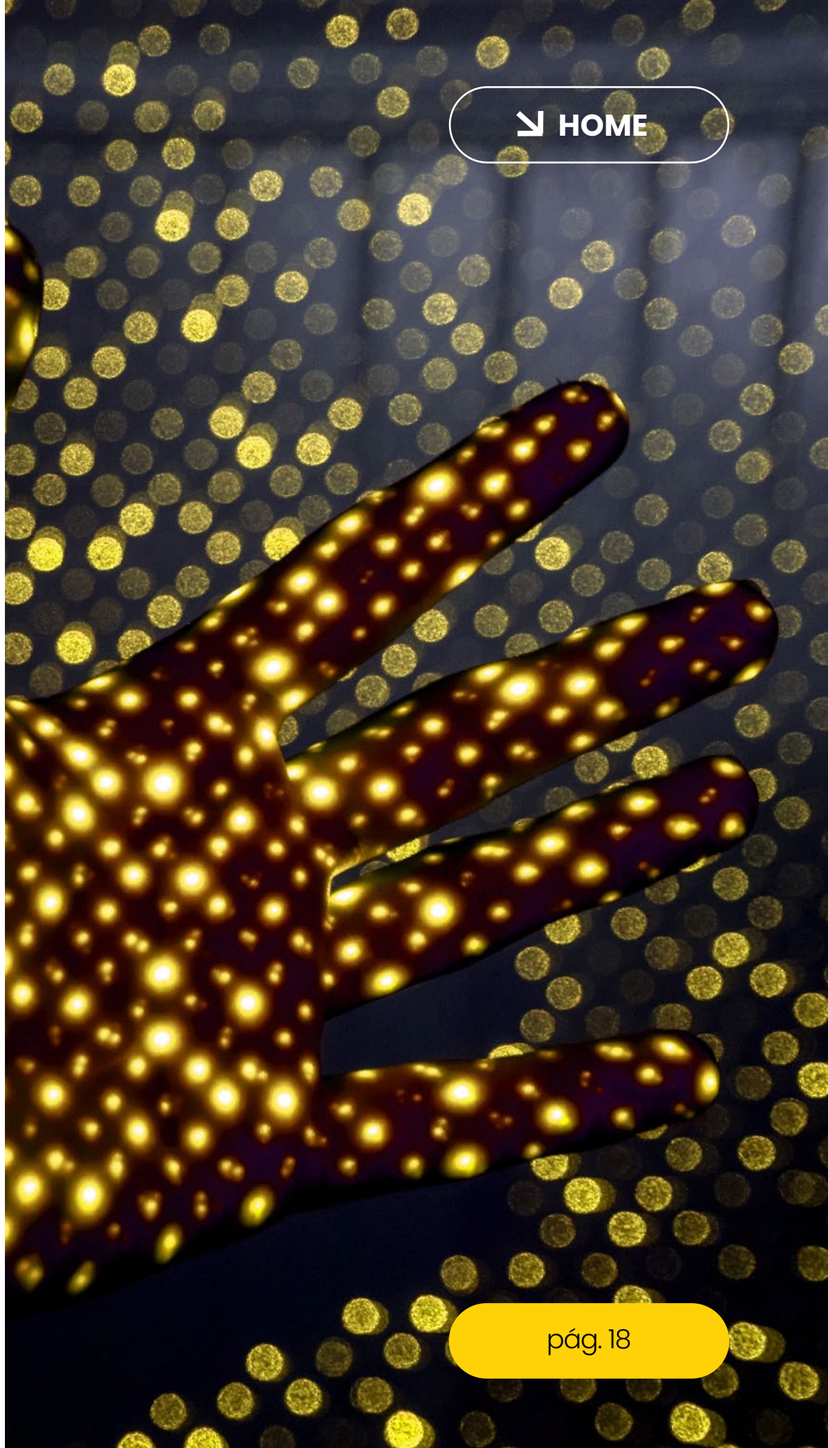


Como se señalaba anteriormente, las competencias puramente humanas, conocidas como *soft skills,* entre las que destacan la creatividad, el pensamiento crítico, la resolución de problemas complejos o la empatía son **más necesarias que nunca.**

En ocasiones la **tecnología contiene sesgos,** puesto que detrás de cada desarrollo tecnológico se encuentra un grupo de personas: desde la definición de objetivos hasta la selección de modelos y la interpretación de los resultados las personas juegan un papel fundamental. Ahora bien, la inteligencia artificial puede mejorar las capacidades organizativas mediante lo que se ha denominado **fuerza laboral aumentada** (o *augmented workforce* en inglés).

La **creatividad** y el **análisis de escenarios adversos** requieren de un proceso mental complejo, superando limitaciones como el dilema del innovador con el objetivo de aumentar la ventaja competitiva de la organización. Por este motivo, la IA mediante la automatización de tareas y la agilización de la burocracia puede eliminar lastres con los que los trabajadores deben lidiar a diario, reorientando su jornada laboral hacia las labores que verdaderamente marcan una diferencia. Además, la posibilidad de creación de escenarios y simulaciones puede permitir a los departamentos y especialistas en innovación identificar nuevas soluciones orientadas a necesidades específicas de seguridad.

Por otra parte, el análisis de datos mediante algoritmos y nuevos desarrollos tecnológicos posibilita la identificación de patrones de acción o consumo de los clientes, permitiendo a los trabajadores detectar y mejorar los servicios operativos y la comunicación con los mismos. Esta **generación de ideas y el pensamiento integrador** hace que las empresas evolucionen en ecosistemas corporativos tan ágiles.



HOME

4 Competencias **en autogestión**

En el dinámico y ágil contexto actual, con entornos progresivamente más sistémicos y exigentes, la autogestión se configura como un **eje esencial para garantizar un correcto servicio de seguridad** para las empresas del sector.

Los profesionales deben adoptar constantemente **nuevas estrategias de aprendizaje** según el contexto en el que se encuentren, aplicando diferentes herramientas pertinentes para cada situación. Por ello, la **IA generativa** (GenAI) supone un avance en el acceso y gestión de la información, especialmente en las capacidades de inteligencia en fuentes abiertas (OSINT), destacando algunos desarrollos como ChatGPT o Perplexity. A modo de ejemplo, el análisis de grandes volúmenes de datos sobre cuestiones financieras, documentación técnico-legal, licitaciones o generación de reportes son solo algunas de las áreas en las que la IA generativa ya ha supuesto un cambio operativo. Sin embargo, las capacidades humanas como el pensamiento crítico señalado anteriormente no deben obviarse en estos contextos: las posibles erratas en los resultados de la IA, los sesgos que pueda contener en su formulación o los propios intereses y valores organizaciones no contemplados necesitan que una persona analice y valide los resultados.

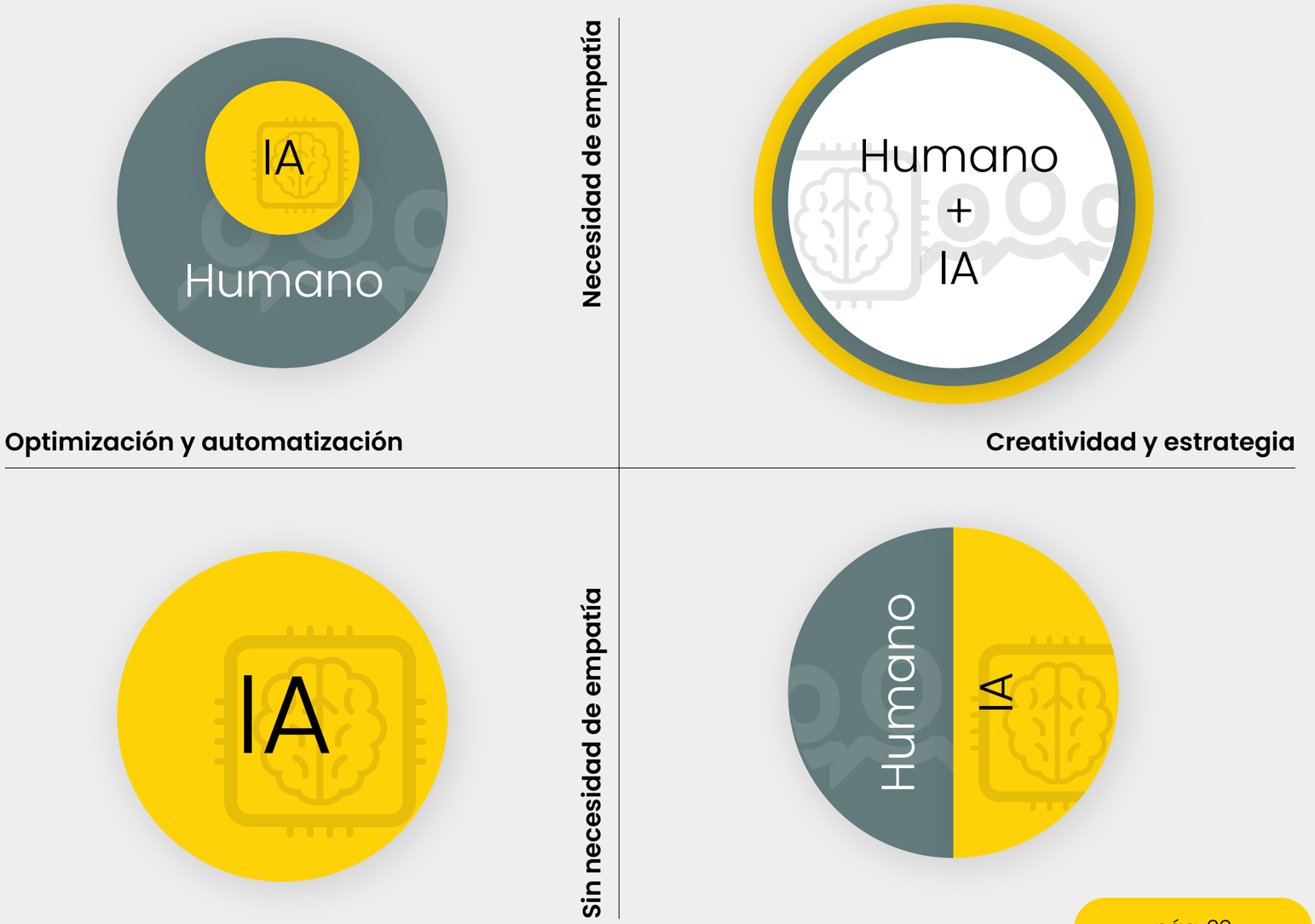
Adicionalmente, la IA puede favorecer la **creación de planes de desarrollo laboral y/o académico personalizados,** con un alto valor y retorno en el ámbito empresarial. A este respecto, algunos estudios han señalado que la inteligencia artificial generativa puede tener **hasta siete diferentes tipos de roles** para potenciar las capacidades humanas: desde el tutor o el estudiante hasta el motivador o el simulador, entre otros. En otras palabras, la GenAI puede **proporcionar puntos de vista alternativos, enseñar técnicas de aprendizaje, aplicar conocimientos y escenarios o retroalimentar los resultados de un proceso de aprendizaje,** potenciando en última instancia las competencias humanas y de autogestión señaladas.

HOME

La pregunta, por tanto, es si las empresas están preparadas para la IA. La robótica y los drones pueden incorporar sensores inteligentes que detecten una alteración en las condiciones climatológicas antes que los humanos, pero las máquinas, al menos por el momento, no pueden sustituir la generación de hipótesis o la comunicación empática y directa con el usuario. Basta con imaginar, como indica el escritor y empresario **Kai-Fu Lee,** en el médico que diagnostica y comunica una dolencia al paciente. De este modo, el **empoderamiento tecnológico inteligente** no debe considerarse un proceso estanco y puntual en las compañías, sino que debe **incorporarse como hábito:** si las tecnologías siguen un ciclo llamado **hype tecnológico,** solo las organizaciones que se mantengan actualizadas constantemente sobre las innovaciones más disruptivas serán capaces de surfear la ola –o el tsunami– del hype, manteniéndose a la vanguardia y marcando un valor diferencial.

Gráfico 5
Simbiosis entre la IA y el trabajador según la necesidad y el grado de optimización y atención humana

HOME



Fuente: Prosegur Research, 2024 basado en BBVA

04

La IA en un ecosistema empresarial ampliado

HOME

01
Un tsunami llamado IA

02
Ante la inquietud, reflexión

03
El empoderamiento como hábito

04
La IA en un ecosistema empresarial ampliado

HOME

01 LA IA EN UN ECOSISTEMA EMPRESARIAL AMPLIADO

La inteligencia artificial lleva décadas cambiando la forma de trabajar en el mundo. Su actual popularización y convergencia con otras tecnologías está suponiendo un rápido crecimiento para muchas organizaciones, configurando fórmulas y enfoques especialmente útiles en el ámbito de la seguridad. Desde Prosegur Research entendemos que **las principales oportunidades de las tecnologías radican en su potencial para empoderar expertos;** esto es, la capacidad de aumentar las habilidades de los profesionales de la seguridad, incrementando enormemente la eficacia y eficiencia como nunca antes se ha visto.

Ahora bien, se debe entender que los algoritmos no actúan de forma aislada, sino que se ensamblan en un ecosistema tecnológico junto con drones y robots, sistemas RFID, tecnología NFC y LiDAR. En consecuencia, **las oportunidades y los riesgos adquieren un carácter sistémico,** por lo que la seguridad y ciberseguridad, así como el cumplimiento normativo, son pilares básicos que otorgan robustez al diseño, implementación y uso de todas las tecnologías, no solo la IA.

En este contexto, el modelo de seguridad híbrida integra la inteligencia artificial como una herramienta que empodera a los expertos en seguridad, permitiendo un uso estratégico de los datos y destacando la importancia de la integración y la convergencia tecnológica. Por supuesto, el abordaje de este modelo debe ser también integral y holístico. Es vital considerar el **ecosistema tecnológico y empresarial** en el que trabajamos. La involucración de empleados y stakeholders, así como de clientes y organizaciones académicas y de investigación de primer nivel para el diseño, permiten una auténtica revisión y mejora de la aplicación de la IA con la intención de ajustar las fórmulas de innovación. En definitiva, abrazar las tecnologías como parte de nuestras herramientas habituales de trabajo desde una **visión sistémica, humanista y, por tanto, empoderadora** nos permite acompañar e incluso impulsar las olas de cambio del mundo.

> La década venidera versará sobre la colaboración humana y la IA. Nuestra misión consistirá en automatizar la rutina y humanizar lo excepcional.
>
> ***Peter H. Diamandis***

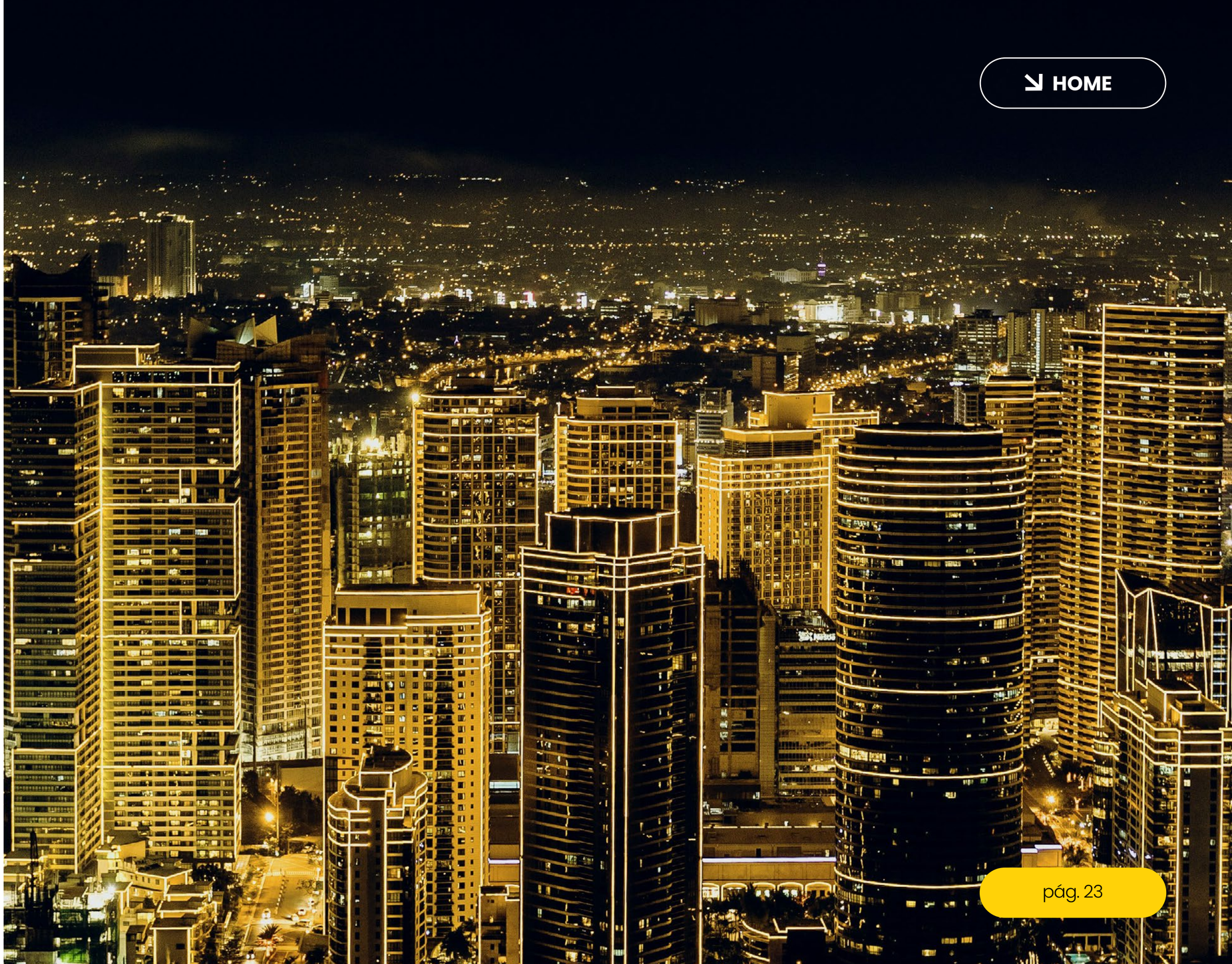
En la actualidad se viene **reflexionando** con especial hincapié acerca de los **sesgos de la IA.** Sin embargo, la distorsión de la realidad es algo propio de todas las personas en muchos ámbitos. En Prosegur Research estamos convencidos de que los sesgos y la distorsión de la realidad superan la tecnología: es algo tan humano que ha de entenderse como un desafío global para el conjunto de las organizaciones, por lo que iniciativas transversales de capacitación, diversidad y sostenibilidad que aborden este reto de forma integral en toda la compañía, y no solo para una tecnología o el ámbito de la innovación, son necesarias si queremos verdaderamente abrazar los cambios del mundo.

HOME

Por tanto, se puede concluir que orientar la aplicación de la inteligencia artificial como fórmula de empoderamiento humano, potenciando sus capacidades, será la opción transformadora de éxito; pero requerirá **valentía** para superar el beneficio cortoplacista de la automatización, **creatividad** para identificar las ideas nunca planteadas y las oportunidades hasta ahora inexistentes y **serenidad** para adoptar decisiones desde la reflexión humana y honesta.

Si reorientamos los esfuerzos sobre la inteligencia artificial hacia el potenciamiento de las competencias humanas, no será solo una tecnología centrada en los humanos, sino una **tecnología para conocernos mejor y prepararnos para los cambios.** El futuro no se puede predecir, pero una cosa está clara: no será igual que el pasado. Las empresas que inviertan en el empoderamiento de las personas generarán sociedades más prósperas y tendrán una tecnología competitiva para influir en la construcción de su propio y nuevo futuro.

Desde nuestro enfoque de seguridad híbrida, queremos formar parte de la transformación social y tecnológica, que unidas conforman la mejor manera de **hacer del mundo un lugar más seguro.**



Glosario

Siguiendo la terminología de Gartner, a continuación se señalan los principales tipos de IA:

- **IA Generativa**
  Se refiere a las técnicas de IA a través de las que se asimila una representación de artefactos a partir de datos y con el objetivo de generar nuevos y únicos artefactos similares a los originales, pero sin repetirlos.

- **IA Responsable**
  Es un término general que engloba los aspectos de la toma de decisiones empresariales y éticas adecuadas a la hora de adoptar la IA. Abarca las responsabilidades y prácticas organizativas que garantizan un desarrollo y un funcionamiento de la IA positivos, responsables y éticos.

- **IA General**
  (AGI) es la inteligencia (actualmente hipotética) de una máquina que puede realizar cualquier tarea intelectual que pueda realizar un ser humano.

- **IA Compuesta**
  Se refiere a la aplicación combinada (o fusión) de diferentes técnicas de IA para mejorar la eficiencia del aprendizaje y ampliar el nivel de representaciones del conocimiento. Resuelve una gama más amplia de problemas comerciales de una manera más efectiva.

- **IA de Centros de datos**
  Se orienta hacia el enriquecimiento de datos para tomar decisiones basadas en los mismos, mejorando la calidad, la privacidad y la escalabilidad.

- **IA de Ingenería**
  Es fundamental para la entrega empresarial de soluciones de IA a escala. La disciplina crea sistemas coherentes basados en IA, entrega y desarrollo empresarial.

- **IA de Simulación**
  Es la aplicación combinada de la IA y las tecnologías de simulación para desarrollar conjuntamente agentes de IA y los entornos simulados en los que pueden entrenarse, probarse y, a veces, desplegarse.

Libros que nos han inspirado

AI and machine learning for Coders: a programmer´s guide to Artificial Intelligence
Laurence Moroney

AI tools and techniques for corporate facilitators and leaders
R.W. Rockwell

AI 2041: ten visions for our future
Chen Qiufan y Kai-Fu Lee

Artificial. La nueva inteligencia y el contorno de lo humano
Mariano Sigman y Santiago Bilinkis

Civilización artificial
José María Lassalle

Competing in the age of AI: strategy and leadership when algorithms and networks run the world
Marco Iansiti y Karim R. Lakhani

El sueño de la inteligencia artificial
Gisela Baños

El mito del algoritmo: cuentos y cuentas de la inteligencia artificial
Richard Benjamins y Idoia Salazar García

¿Qué hacemos con los humanos?
César Antonio Molina

The age of AI
Henry Kissinger, Eric Schmidt y Daniel Huttenlocher

The bussiness case for AI: a leader´s guide to AI strategies, best practices and real-world applications
Kavita Ganesan

PROSEGUR
SECURITY

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

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com