Segovia,
05 / Julio / 2023

# Evolución de los SOCs y su relación con la IA

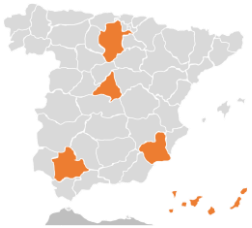
## AI Segovia Summit

Centr@Tec
Servicios Avanzados de Innovación para Pymes

# Índice

- Presentación
- Contexto
- Introducción
- Orígenes de los SOCs
- SOCs tradicionales
- Hacia la automatización
- Incorporación de la IA
- IA y Ciberseguridad
- Conclusiones

# Presentación de compañía



**+200**
Empleos

Ingeniería y Consultoría

Desarrollo Normativo y Cumplimiento

Desarrollo de Software

Concienciación y Formación

Soporte y Evolutivos

**Operaciones de Ciberseguridad**

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010

**Partner**
Principales Fabricantes HW y SW

**+25 M€**
Año 2022

# ¿De qué estamos hablando?

**Empresas inscritas en la Seguridad Social**

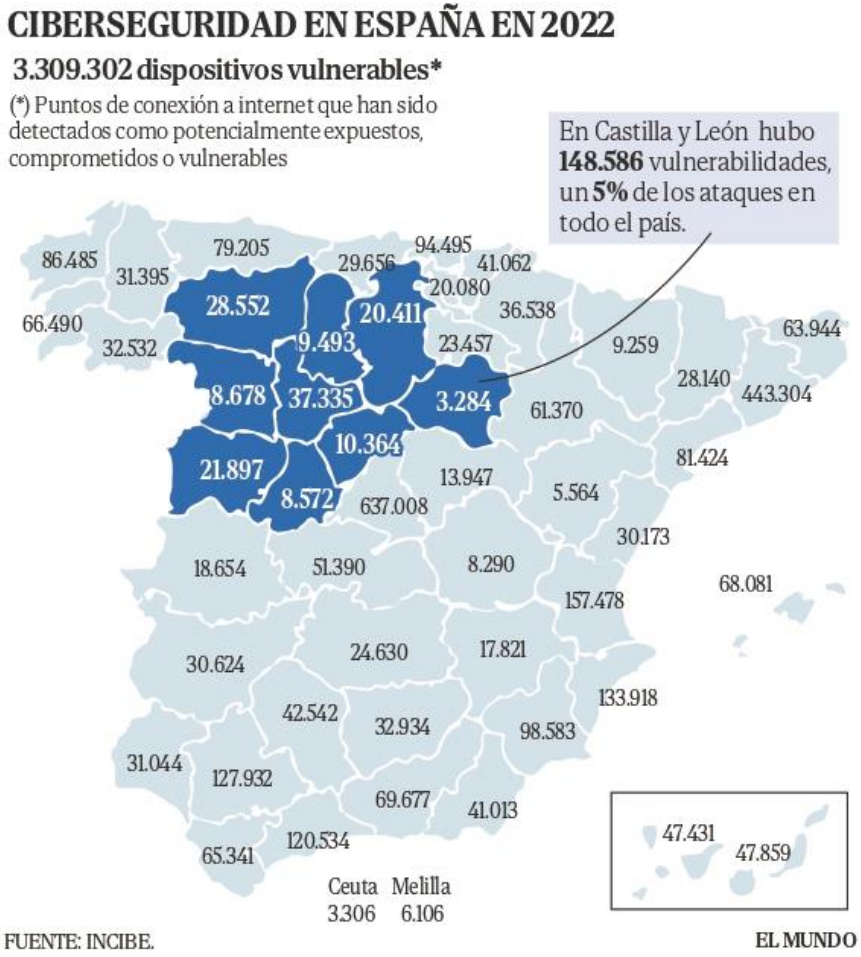
| (a 31 de mayo) | Empresas 2023 | Variación 2022-2023 Absoluta | Variación 2022-2023 % | Trabajadores 2023 | Variación 2022-2023 Absoluta | Variación 2022-2023 % |
|---|---|---|---|---|---|---|
| **▼ Provincias** | | | | | | |
| ■ Ávila | 5.217 | *88* | 1,7 | 36.059 | *1.049* | 3,0 |
| ■ Burgos | 10.663 | *-58* | -0,5 | 116.047 | *2.079* | 1,8 |
| ■ León | 12.588 | *-79* | -0,6 | 115.521 | *3.331* | 3,0 |
| ■ Palencia | 4.794 | *-28* | -0,6 | 47.357 | *1.683* | 3,7 |
| ■ Salamanca | 10.168 | *-19* | -0,2 | 88.802 | *2.795* | 3,2 |
| ■ Segovia | 5.442 | *-83* | -1,5 | 43.615 | *1.008* | 2,4 |
| ■ Soria | 2.994 | *-1* | 0,0 | 29.402 | *527* | 1,8 |
| ■ Valladolid | 15.417 | *-52* | -0,3 | 170.568 | *3.465* | 2,1 |
| ■ Zamora | 5.336 | *-50* | -0,9 | 38.029 | *860* | 2,3 |
| **■ Total** | **67.338** | ***-427*** | **-0,6** | **685.400** | ***16.797*** | **2,5** |
| **▼ Sectores** | | | | | | |
| ■ Agrario | 5.725 | *-73* | -1,3 | 22.145 | *52* | 0,2 |
| ■ Industria | 6.688 | *-63* | -0,9 | 135.112 | *3.402* | 2,6 |
| ■ Construcción | 7.498 | *-64* | -0,8 | 44.113 | *1.516* | 3,6 |
| ■ Servicios | 47.427 | *-227* | -0,5 | 484.030 | *11.827* | 2,5 |
| **■ Total** | **67.338** | ***-427*** | **-0,6** | **685.400** | ***16.797*** | **2,5** |

FUENTE: Ministerio de Trabajo y Economía Social ICAL

**Inmensa mayoría**:

- Son PYMES
- Poco concienciadas en ciberseguridad
- *No disponen de SOCs*
- Han tenido o van a tener un incidente de ciberseguridad
- En proceso de digitalización

# Mas allá de los costes financieros




**SEGOVIA:** Con 10.364 es la siguiente, pudiendo estar afectada por la cercanía con Madrid y con las operaciones que puedan realizarse entre ambos territorios


Los ciberataques generan además:

- Publicidad negativa
- Impacto sobre la marca y reputación
- Costes de notificación a clientes
- Pérdida de clientes
- Infracciones a terceros
- Aumento del gasto en gestión de crisis
- …

# Un par de preguntas

¿ Quiénes conocen lo que es un **SOC** ?

¿ Quién no ha probado el **ChatGPT** ?

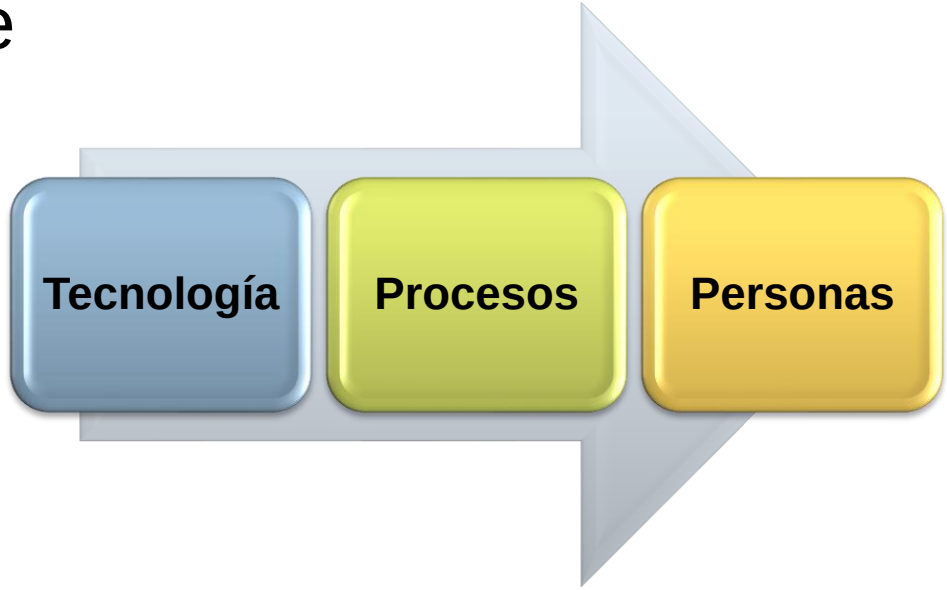
¿ Versión de pago o gratuita ?

# Qué es un SOC?

- **C**entro de **O**peraciones de **S**eguridad

- Es un equipo de recursos que supervisa toda la infraestructura TI de una organización, para detectar incidentes de ciberseguridad y abordarlos lo antes posible

- Consta de:



# Orígenes

- Surgieron a principios de la década de los 90
- Como respuesta a la necesidad de combatir las crecientes amenazas y cibertaques
- Se basaban en herramientas y tecnologías tradicionales
  - Sistemas de detección de intrusos (IDS)
  - Firewalls

# SOCs tradicionales

- Se basan en la detección y respuesta manual de incidentes de seguridad
- Los analistas de seguridad revisaban los registros de eventos y las alertas generadas por las herramientas de seguridad para identificar y responder a las amenazas
- El enfoque era predominantemente reactivo

# Piezas de un SOC tradicional

## Tecnología

- SIEM
- SOAR
- Gestión de vulnerabilidades
- EDR
- UEBA
- IDS
- …

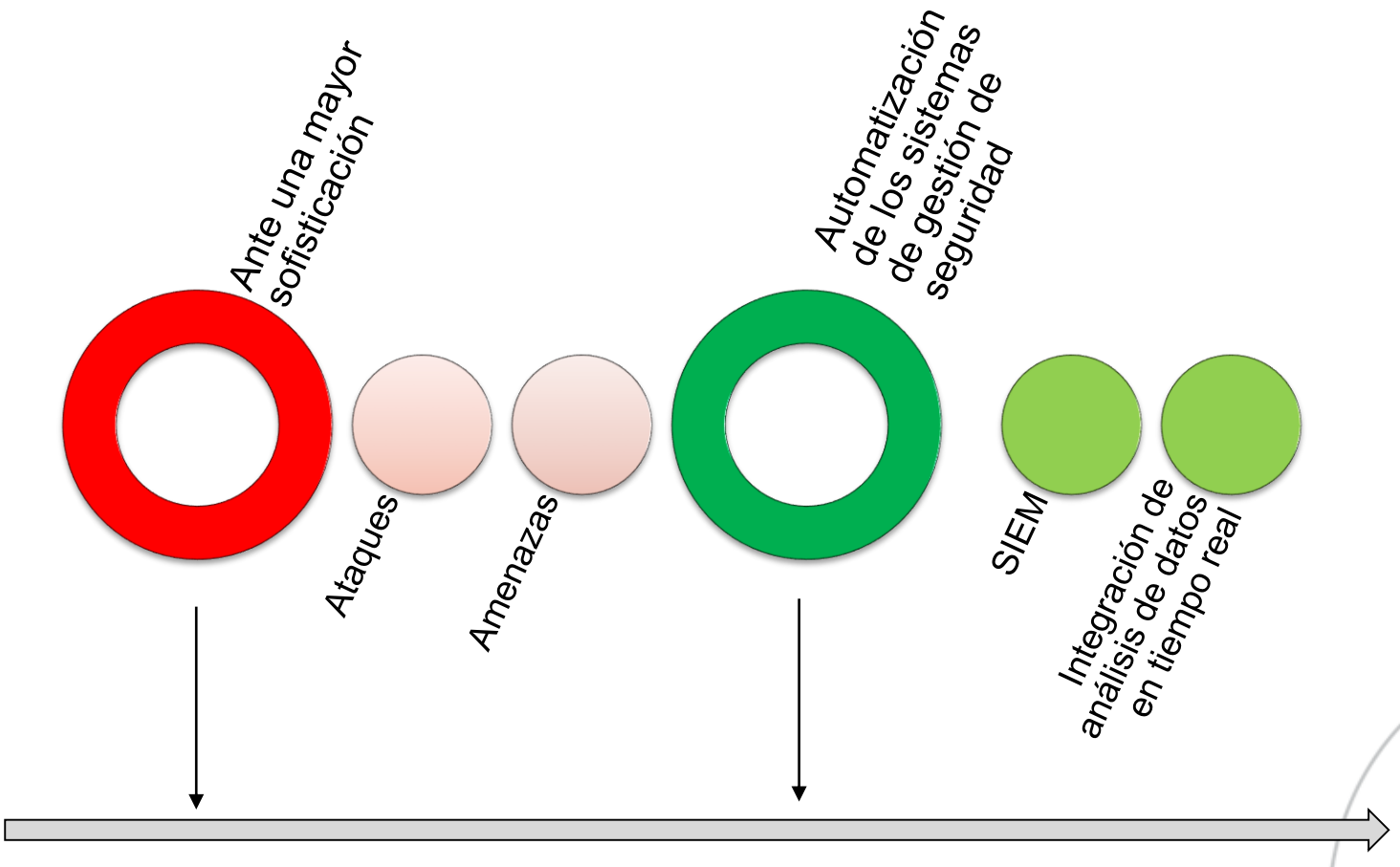
## Procesos

- Prevención
- Protección
- Detección
- Respuesta
- …

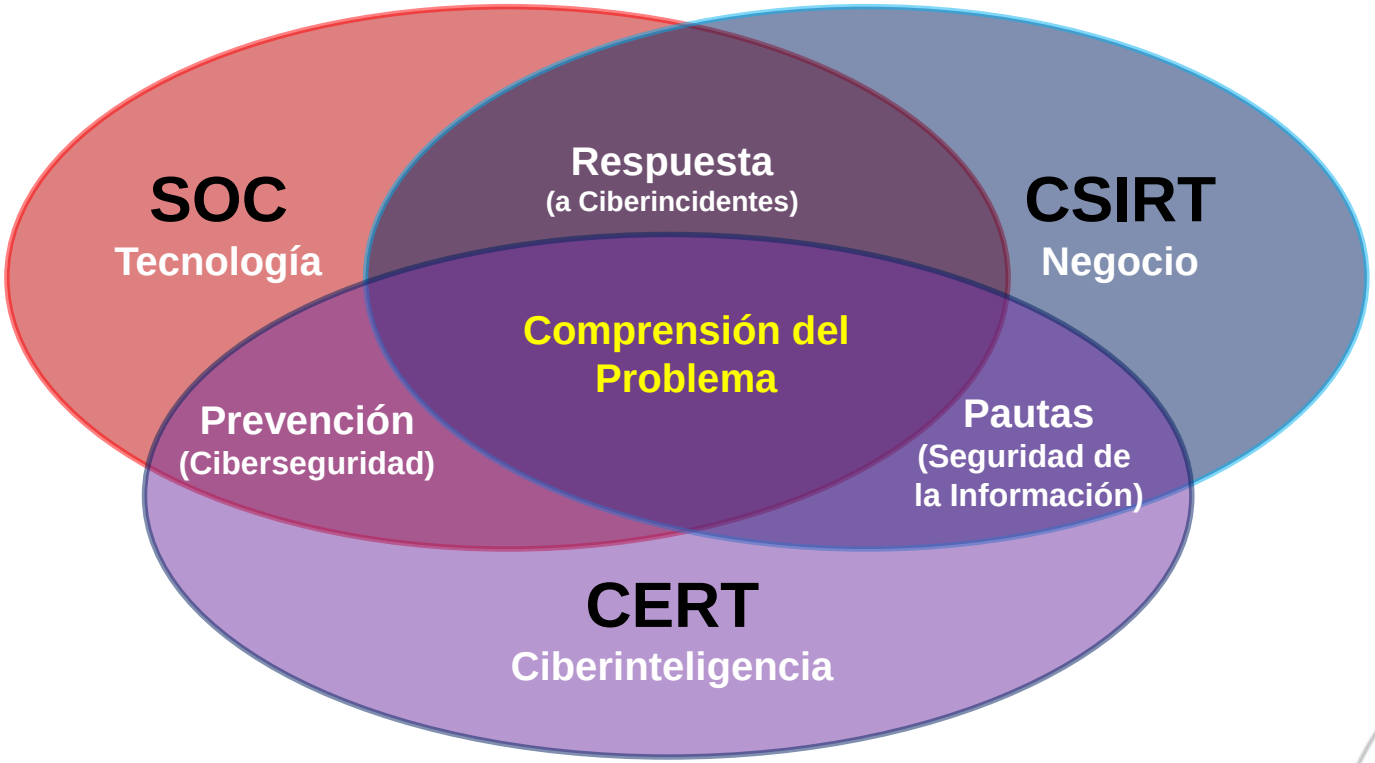
## PERSONAS

- Responsable
- Ingenieros de seguridad
- Analistas de seguridad
- Otros perfiles

# Respuesta de la automatización

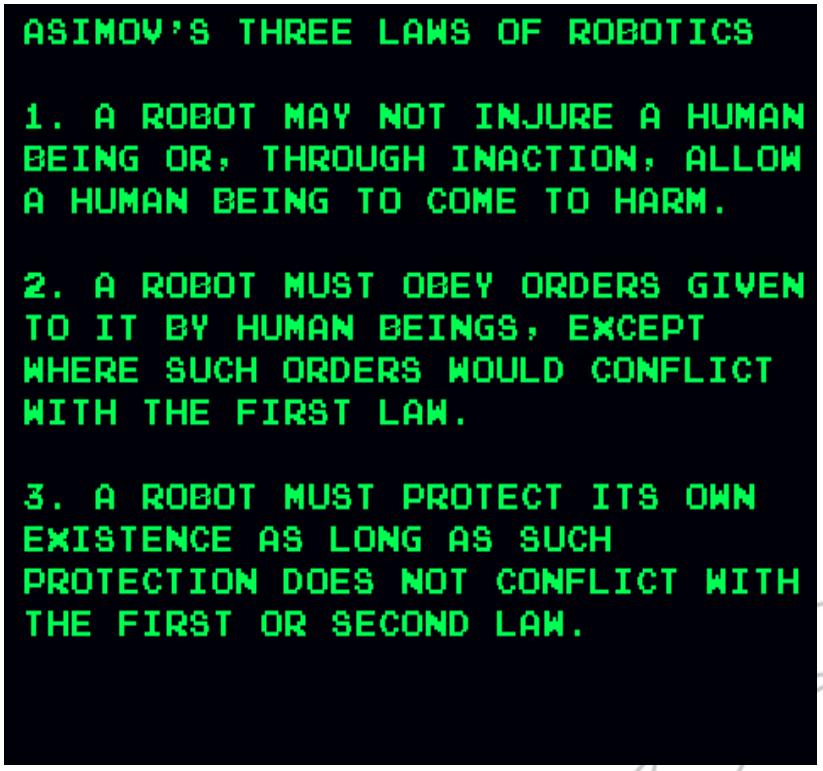


# Capacidad de respuesta integral

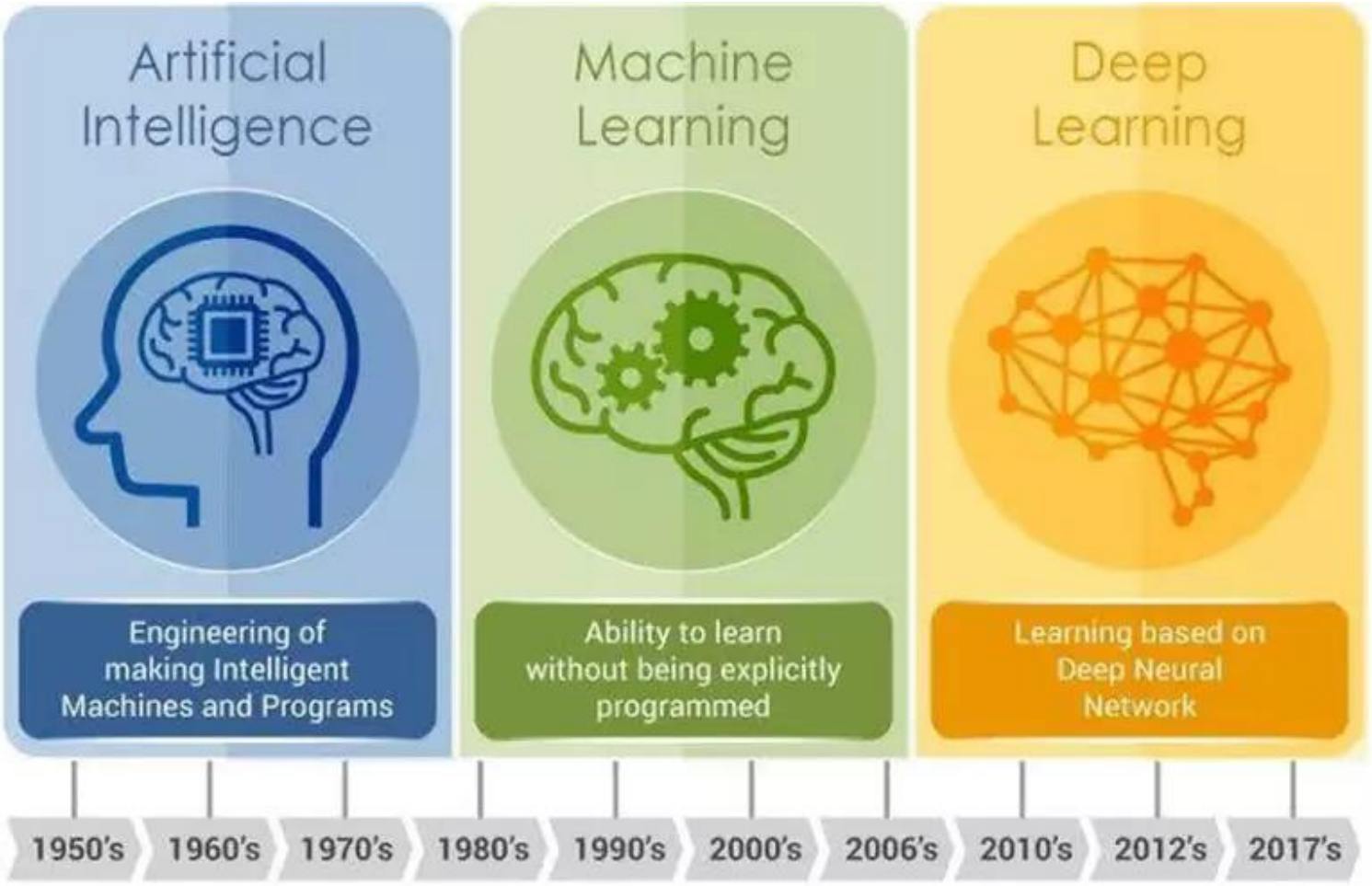


# Skynet / Asimov

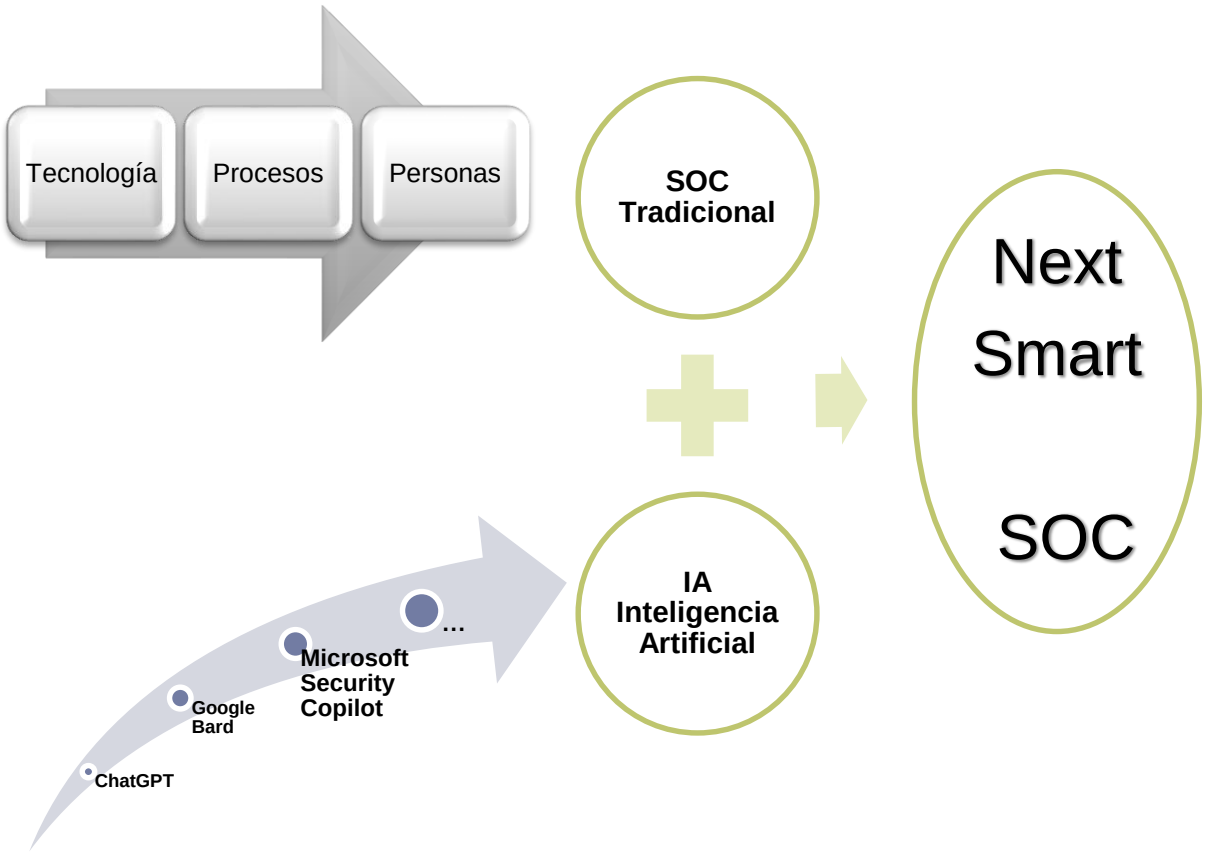
- *Skynet* predice que la IA toma conciencia, y esta se rebela contra la sociedad, ¿Es factible?
- Leyes de robótica (*Asimov*) "***No poner en peligro la vida del humano***"
- Salvo que la ética fracase como modelo global en regular la IA, puede ser factible que algunos experimentos financiados/relevantes pueda tomar conciencia
- Sin embargo, el peligro real representa emplear la IA por parte de los adversarios contra la sociedad



# ¿ De dónde venimos ?



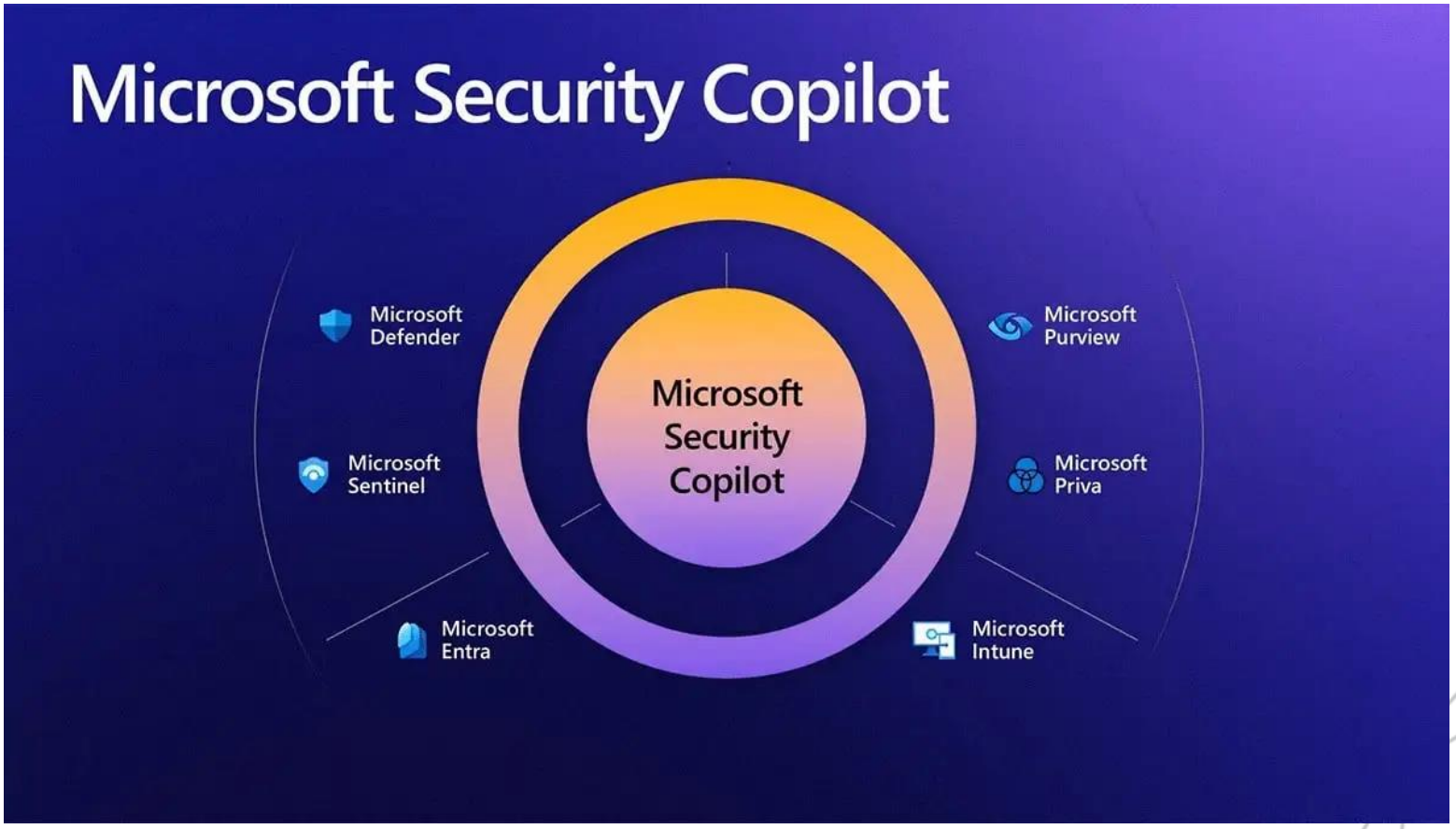
# ¿ A dónde vamos ?




**Resultados de la suma**:

- Simplifica lo + complejo
- Suprime tareas repetitivas
- Genera cálculos de alto valor, mediante ingesta de datos
- Mejora la falta de especialistas
- Aumenta la productividad
- ***Mismas herramientas que el enemigo***

# Ejemplo disponible




https://www.microsoft.com/enus/security/business/ai-machine-learning/microsoft-security-copilot

# Casos de uso

*“¿Con qué comando puedo montar/desmontar unidades extraíbles, genérame una tarea programada en Linux/Windows…”*

**POSITIVOS**

*“Analiza este PDF (300 páginas) destácame los puntos mas ejecutivos, compáralo con la edición 2022, ¿Qué ha cambiado?”*

*“Genera una tabla comparativa entre el desarrollo en “X” lenguaje frente a este otro, conviértelo en post de Linkedin que sea atractivo”*

# Casos de uso

*“Clona la voz de este directivo/CEO, monta un video mensaje de DEEPFAKE de 30 segundos, advirtiendo que no esta localizable y que debemos atender un correo que nos llegara con la máxima agilidad…”*

**ADVERSARIOS**

*“Analiza todos los correos electrónicos de este buzón, identifica aquellos donde hay facturación pendiente, escribe un texto creíble, modifica la cuenta bancaria de todas las facturas con la siguiente IBAN466XXXXXXXXX*

*¿ Identifica los proveedores claves de un cliente grande?*

*Crea un script en “X” lenguaje que me permita obtener credenciales*

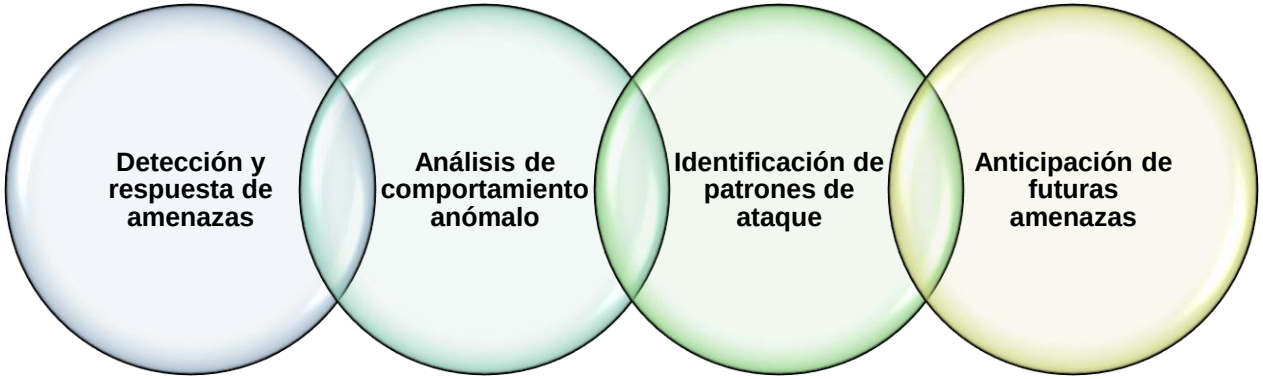
*En base a las redes sociales de “X” usuarios determina sus gustos leyendo toda su cronología de actividades en los últimos meses, genérame posibles casos de uso de Phishing.*

# Nuevo escenario

- Los nuevos desarrollos tecnológicos de la IA evolucionará los SOCs en que:
  - Los ciclos de decisión sean más cortos
  - Los márgenes de error sean más pequeños
  - La superficie de exposición sea mayor
  - Creciendo las necesidades de:
    - Más conectividad
    - Mayor almacenamiento de datos
    - Mayor computación
- Sin contar con el cómo afectará la nueva tecnología emergente que está por venir de forma masiva
  - La ***Computación Cuántica*** … ?

# IA y Ciberseguridad (+)

- La IA se utiliza en los SOCs para diversas aplicaciones de Ciberseguridad:




- Mejora la capacidad de respuesta a incidentes mediante la automatización de la investigación de incidentes y la generación de alertas más precisas

# IA y Ciberseguridad (-)

- Algunos vendors / fabricantes incorporan la IA con unas expectativas generadas artificiaente, sobrevalorando sus cualidades
- Ojo con los falsos negativos
- Dependencia de datos de calidad
- Amenazas de IA maliciosas
- Tener en cuenta la privacidad y la ética

Red Nacional de SOC

incibe_

Empresas especialistas

- Instrumento para coordinar la colaboración y el intercambio de información entre los SOCs del sector público español
- Entidades adscritas:
  - Públicas 87
  - Privadas 53
- Información compartida relativa a los indicadores de ataques o compromisos (IOA/IOC)

TU AYUDA POR TELÉFONO EN CIBERSEGURIDAD
incibe_
017

- Fabricantes
- Integradores
- Auditores

# Conclusiones

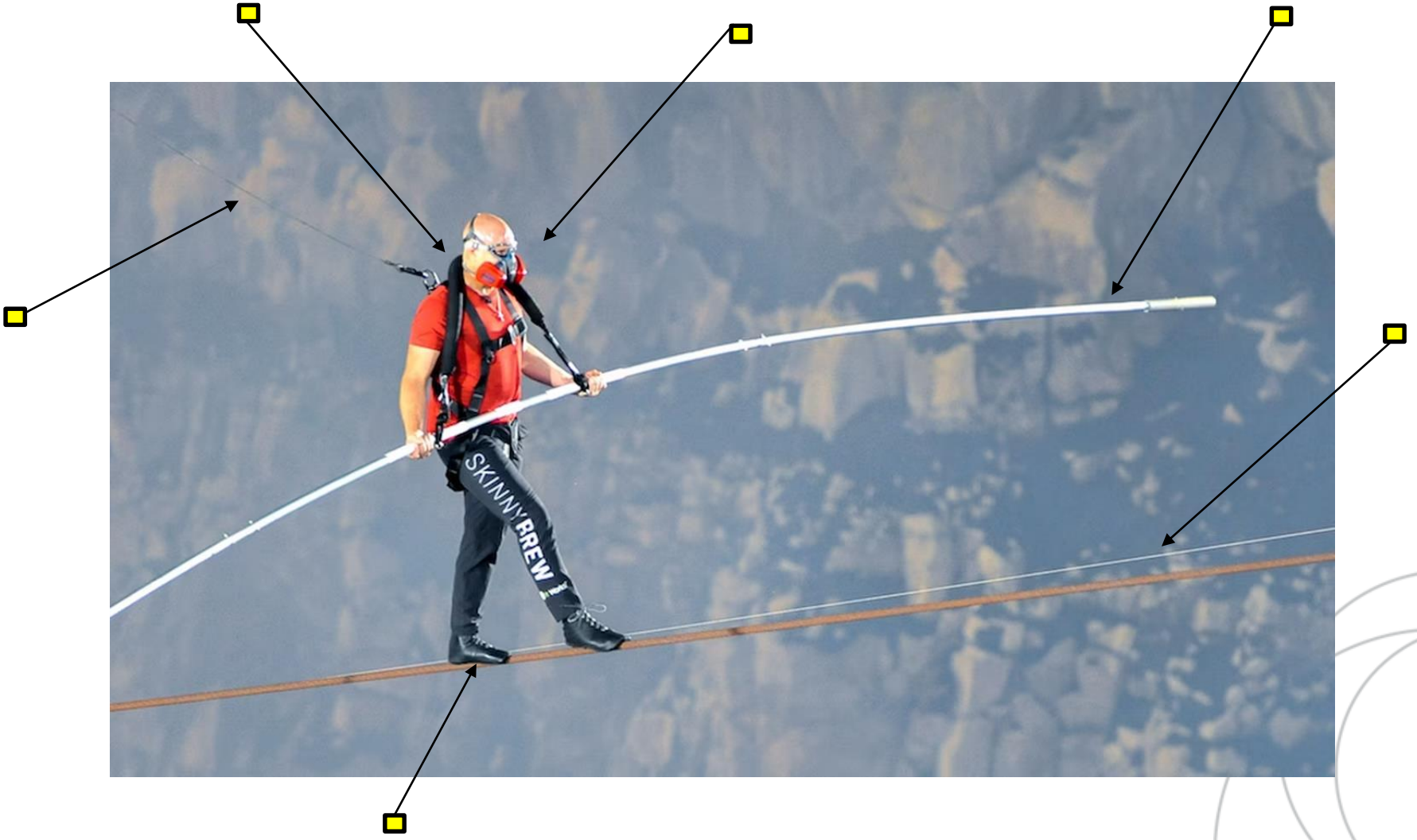
- La evolución de los SOCs ha sido impulsada por la necesidad de enfrentarse a las ciberamenazas cada vez más complejas y sofisticadas

- La incorporación de la IA ha transformado los SOCs al permitir
  - Análisis de datos más rápido y preciso
  - Automatización de tareas
  - Mejora de la capacidad de respuesta a incidentes

- La IA continúa desempeñando un papel fundamental en la protección contra las ciberamenazas en constante evolución

# Sin IA

# Con IA



# Reflexión diaria

**¿Cómo puedo utilizar la IA para defenderme de los ataques de los “malos” que utilizan la IA?**

**…**

# Gracias por su atención

SU SOCIO EN IT

*Desde 1996*