

# La militarización de la inteligencia artificial: ataques impulsados por IA.

**Fátima Rodríguez Giles**

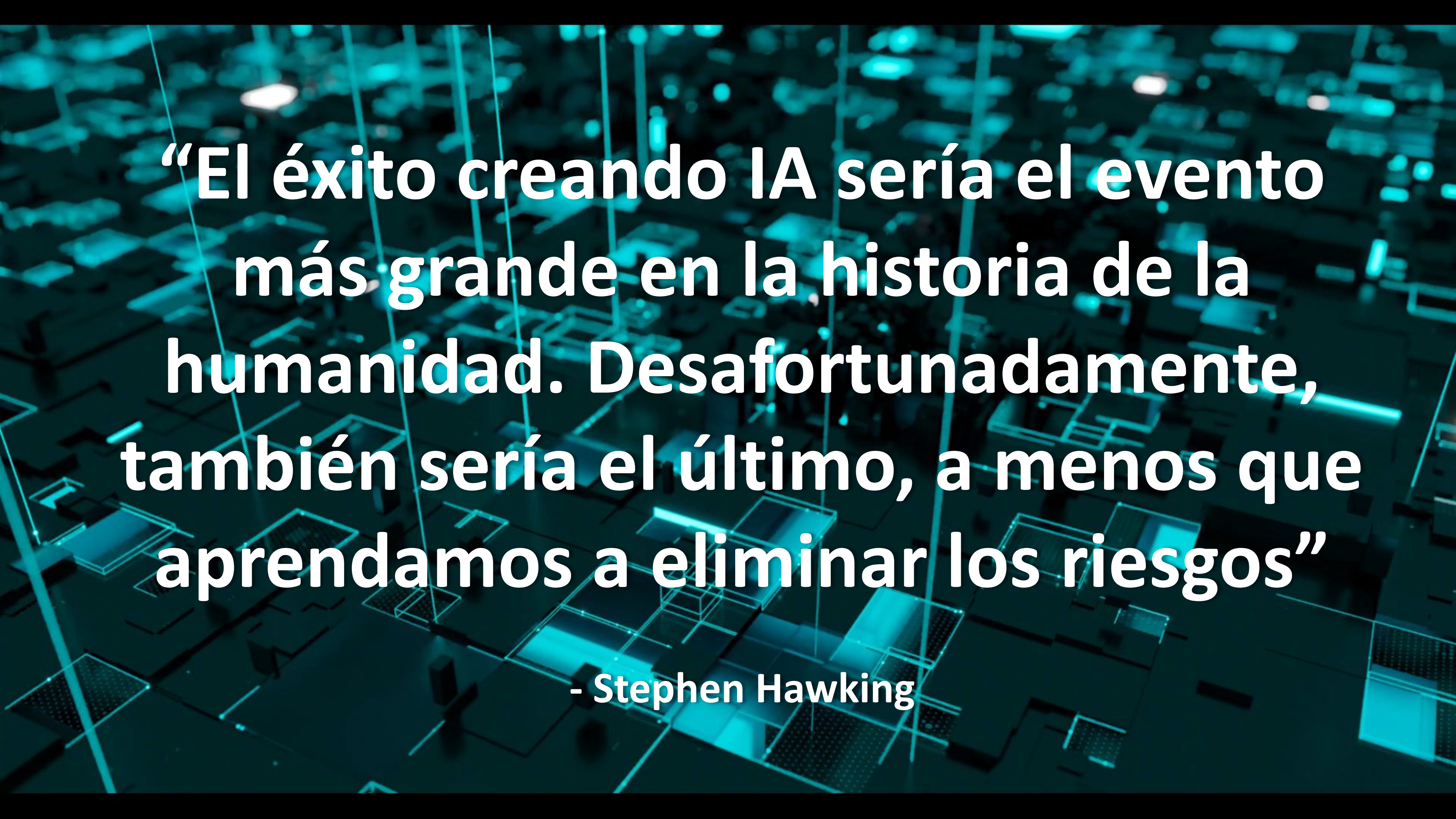
Cybersecurity Intelligence Analyst

ESET Latinoamérica



SECURITY  
DAYS 2024





**“El éxito creando IA sería el evento más grande en la historia de la humanidad. Desafortunadamente, también sería el último, a menos que aprendamos a eliminar los riesgos”**

**- Stephen Hawking**



# Top challenges organizations face



Complex and  
evolving threat  
landscape

**2,200**

cyber attacks  
per day



Compliance  
and regulatory  
requirements

**66%**

of companies expect  
spending driven by  
compliance mandates



Cybersecurity  
talent shortage

**49%**

professionals  
admit gaps in their  
organization



Budget  
constraints and  
increasing costs

**51%**

expected increase of  
cybersecurity budget  
2016-2023



# Características de los ataques potenciados por IA

**Personalización**

**Refuerzo del  
aprendizaje**

**Eficiencia en la  
recopilación**

# Diferencia entre los ataques tradicionales

Y aquellos potenciados por Inteligencia Artificial



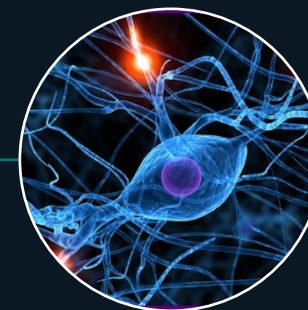




Rapidez y automatización



Especificidad del objetivo



Capacidades de evasión



Manipulación



Nivel de habilidades



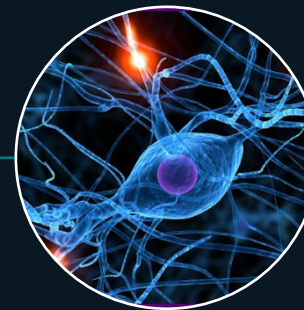
Costos



**Rapidez y automatización**



**Especificidad del objetivo**



**Capacidades de evasión**



**Manipulación**



**Nivel de habilidades**



**Costos**

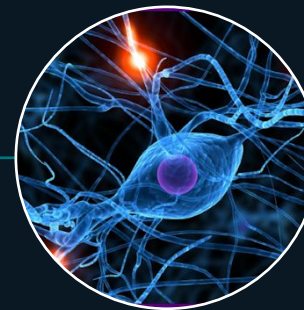




Rapidez y automatización



**Especificidad del objetivo**



Capacidades de evasión



Manipulación



Nivel de habilidades



Costos

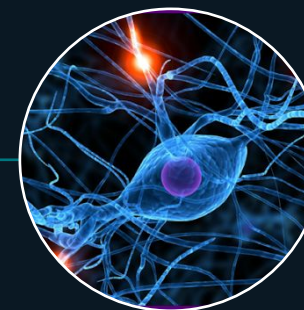




Rapidez y automatización



Especificidad del objetivo



Capacidades de evasión



Manipulación



Nivel de habilidades



Costos

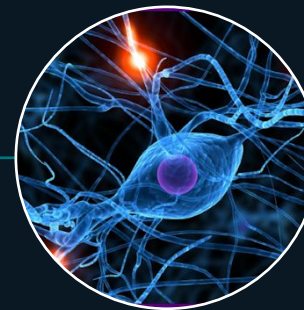




**Rapidez y automatización**



**Especificidad del objetivo**



**Capacidades de evasión**



**Manipulación**



**Nivel de habilidades**



**Costos**

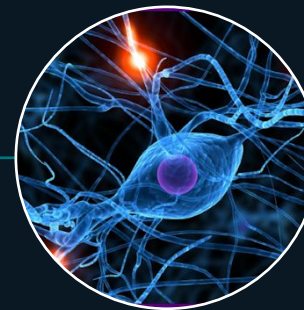




Rapidez y automatización



Especificidad del objetivo



Capacidades de evasión



Manipulación



Nivel de habilidades



Costos

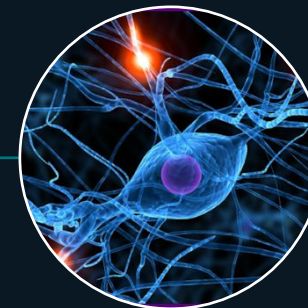




Rapidez y automatización



Especificidad del objetivo



Capacidades de evasión



Manipulación



Nivel de habilidades



Costos



# Modern Ransomware



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service



## Examines Network and Users

Living off the land



## Downloads other utilities



## Escalate Privileges /Steal Credentials



## Moves Across Network



## Find and Exfiltrate Files

Allows for Extortion



## Deploy Encryption

Ransomware



## Demand Payment

# Extortionware



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service



## Examines Network and Users

Living off the land



## Downloads other utilities



## Escalate Privileges /Steal Credentials



## Moves Across Network



## Find and Exfiltrate Files

Allows for Extortion



## Demand Payment



# Cuantificando las consecuencias

de un ataque potencia por IA





# Cuantificando las consecuencias

Costo promedio (en millones USD)





# Articulando las soluciones

de un ataque potencia por IA





# Tres frentes unificados

## Gobiernos

Estableciendo marcos  
legales sólidos,  
regulaciones **efectivas** y  
controles reales

## Organizaciones

Implementando **controles**  
tecnológicos y de gestión, y  
cumpliendo las normativas

## Usuarios

Tomando **consciencia**  
de los riesgos y  
aplicando medidas de  
protección



# Regulaciones como aliados clave

- Bases sólidas para un problema complejo
- Las más completas sugieren elementos concretos, como ejercicios de seguridad o periodicidad
- Esclarece situaciones complejas, como el post-ataque
- La búsqueda final debe ser fortalecer todas las fases de tratamiento de datos de manera integral, y no cumplir con una lista de requerimientos.





# Que la tecnología nos acompañe

**Detección de anomalías en red**

**Comportamiento en email**

**Administración de postura**

**Seguimiento automático de  
alertas**

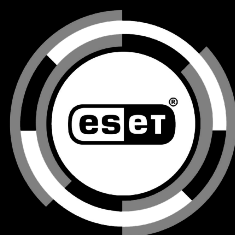
**AI-focused threat detection**







# Gracias.



**SECURITY  
DAYS 2024**