



# Ciberseguridad, soberanía digital e IA.

INFOSEC, octubre 2025

---

Óscar García



# Contexto Actual

Situación  
Geopolítica

Profesionalización  
del Cibercrimen

Mundo  
Hiperconectado

Cadena de  
suministro

Brecha de Talento

Nuevo paradigma  
regulatorio

# Situación Geopolítica



Polarización

Propaganda / Desestabilización

Objetivos políticos

Hacktivismo

# Profesionalización del Cibercrimen

Cibercrimen  
como Servicio  
+ Recursos

Lucro  
económico

Incentivos por  
resultados

Colaboración

IA

Eficiencia

Organización  
empresarial



€€€



# ¿Qué es la Soberanía digital y tecnológica?

Es el derecho y capacidad de un Estado, empresa o institución para controlar y decidir cómo se recopilan, almacenan, procesan y utilizan sus datos y tecnologías digitales.



# ¿Qué factores que afectan en la Soberanía del Dato?

Localización

Donde se almacenan los  
Datos

Jurisdicción

Cumplir con la legislación  
(GDPR en UE, ENS en ES)

Gobernanza y  
Control

Garantizar el control y  
acceso de los Datos



# ¿Cómo afecta la Ciberseguridad a la Soberanía?

*Sin seguridad no hay soberanía real.*

Si no podemos proteger nuestros datos e infraestructuras, no tenemos control.



# ¿Qué riesgos existen?

La Geopolítica global inclina la balanza de la supremacía tecnológica, esto puede provocar que Estados, empresas, medios y grupos ideológicos puedan utilizar la tecnología para la propaganda, la manipulación o la legitimación y:

Exposición de  
datos sensibles

En jurisdicciones no  
reguladas ni garantistas.

Fuga de  
propiedad  
intelectual

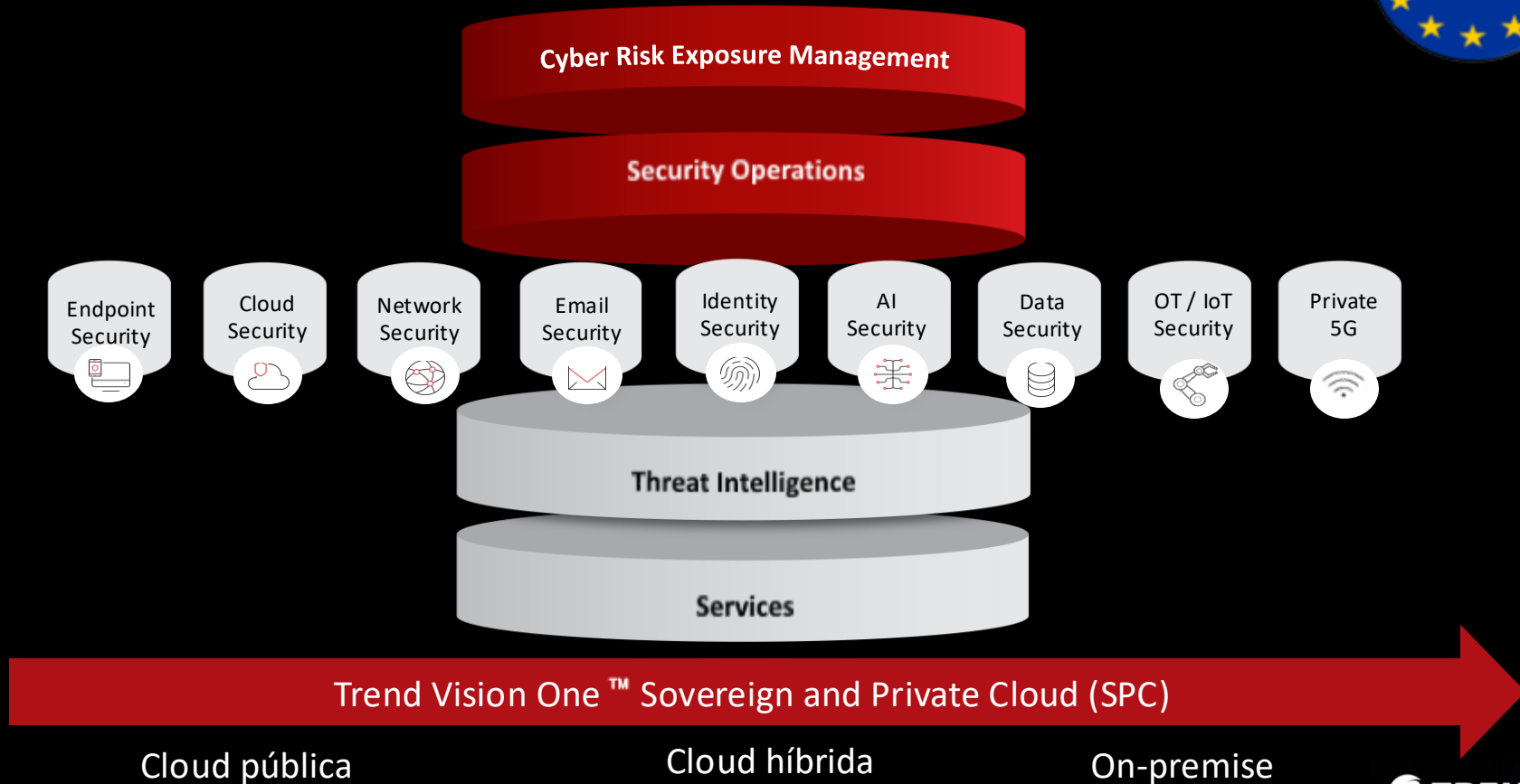
Espionaje, fraude y  
suplantación de identidad

Pérdida de  
confianza

De los ciudadanos y/o  
usuarios.



# Nubes Soberanas e Infraestructura híbrida



# Nubes Soberanas e Infraestructura hibrida



Trend Vision One SPC Deployment Service | Trend Vision One SPC Platform Support

Endpoint  
Security  
Essentials

Endpoint  
Security  
Pro

EDR /  
XDR add-  
on

CREM  
Core

XDR add-  
on for  
DDI

Other

Trend Vision One SPC: Platform Operating System  
(Base Software)



Deployment Environments



GKE



EKS



AKS

...

Private Cloud



Red Hat  
OpenShift  
DC 1



Red Hat  
OpenShift  
DC ...N

Data Center

Portable

Flexible

Cloud Agnostic



# Soberanía y Seguridad de la IA



Seguridad desde el diseño en las  
para proteger la integridad y reducir  
riesgos.



Inversión en centros de Innovación  
de IA (IA Factory) a través de  
alianzas con líderes de IA.

*Barcelona Supercomputing Center*



# Soberanía y Seguridad de la IA



## Seguridad de la IA

Protección de entornos de IA  
híbrida y soberana

Ecosistema de IA

Inteligencia de amenazas y ataques

IA Responsable (\*) (\*\*)

(\*) Paris Paece Forum Partner

(\*\*) Gold sponsor of the OWASP Top 10 for LLM and Gen AI Project

# Riesgos para las aplicaciones de IA



## Riesgos de Datos

- Exposición de datos sensibles
- Insecure Outputs
- Extorsión (deepfakes)



## Riesgos de Modelo

- Prompt Injection
- Jailbreaks
- Model Denial of Service
- Alucinaciones
- Desalineación
- Envenenamiento (Poisoning)



## Riesgos Operacionales

- Violaciones de Políticas
- Shadow AI
- Uso no autorizado de IA

La IA puede crear malware que se adapta y evoluciona para evadir la detección por parte de las herramientas de seguridad tradicionales, lo que dificulta su detección y neutralización.

*Source: Forbes Technology Council – Dec 2024*



# Seguridad para la IA

|                |                                                                                   | Security Challenges                                                                                                                                             | Security Controls                                                                                                                                        | Trend Vision One                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Data           |  | Sensitive information blind spots                                            | Secure Data                                                           | CREM for Cloud (DSPM)                                         |
| Microservices  |  | Vulnerabilities in AI Supply Chains & Microservices Architecture             | Security validation on CI/CD pipeline & Implement Container Controls  | Shift Left Security & Container Security                      |
| Models         |  | Model Poisoning & Improper Model Usage                                       | Implement guardrails for inbound requests for AI APIs                 | ZTSA AI Service Access                                        |
| Infrastructure |  | Security Risks in AI Model Deployment & Resource Exhaustion Attacks          | Infrastructure Posture Management                                     | CREM for Cloud (AI-SPM and API Risk) & AI-DR (XDR for Cloud)  |
| Network        |  | Exploiting Vulnerabilities in AI Infrastructure & Hybrid Cloud Environments  | Network secure against exploits                                       | TippingPoint Network IDS/IPS                                  |
| Users          |  | Insecure Design & Mismanagement Leading to Sensitive Data Exposure by AI     | AI Application Access Control & Protect local AI Application Configs  | ZTSA AI Service Access & V1ES – (Deepfake and AI App Guard)   |

# Seguridad para la IA

|                |                                                                                   | Security Challenges                                                                                                                                             | Security Controls                                                                                                                                        | Trend Vision One                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Data           |  | Sensitive information blind spots                                            | Secure Data                                                           | <br><br><b>Trend Vision One™<br/>Cybersecurity<br/>Platform</b> |
| Microservices  |  | Vulnerabilities in AI Supply Chains & Microservices Architecture             | Security validation on CI/CD pipeline & Implement Container Controls  |                                                                                                                                                    |
| Models         |  | Model Poisoning & Improper Model Usage                                       | Implement guardrails for inbound requests for AI APIs                 |                                                                                                                                                    |
| Infrastructure |  | Security Risks in AI Model Deployment & Resource Exhaustion Attacks          | Infrastructure Posture Management                                     |                                                                                                                                                    |
| Network        |  | Exploiting Vulnerabilities in AI Infrastructure & Hybrid Cloud Environments  | Network secure against exploits                                       |                                                                                                                                                    |
| Users          |  | Insecure Design & Mismanagement Leading to Sensitive Data Exposure by AI     | AI Application Access Control & Protect local AI Application Configs  |                                                                                                                                                    |



# Gracias!

Madrid, octubre 2025

