Ciberseguridad y soberanía digital y tecnológica.

Madrid, Septiembre 2025

Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad

¿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.

Protección Infraestructuras Críticas

Control de Datos Estratégicos

Cumplimiento Normativo

Confianza Digital

¿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	Fuga de propiedad intelectual	Pérdida de confianza
En jurisdicciones no reguladas ni garantistas.	Espionaje, fraude y suplantación de identidad	De los ciudadanos y/o usuarios.

Casos de uso reales de Trend Micro en la UE

1. Nubes Soberanas e Infraestructura híbrida
2. Comunicaciones seguras
3. Soberanía y seguridad de la IA

Nubes Soberanas e Infraestructura híbrida

Nube Global Conectada	Nube aislada por jurisdicción	Entorno de Nube privada	Centro de datos local aislado (físicamente) fuera de línea
AWS, Microsoft Azure, Google Cloud Platform™ (GCP), Oracle Cloud	AWS Sovereign Cloud Oracle EU Sovereign Region	Google, AWS, Cloud privada	Hardware y Coms dedicadas

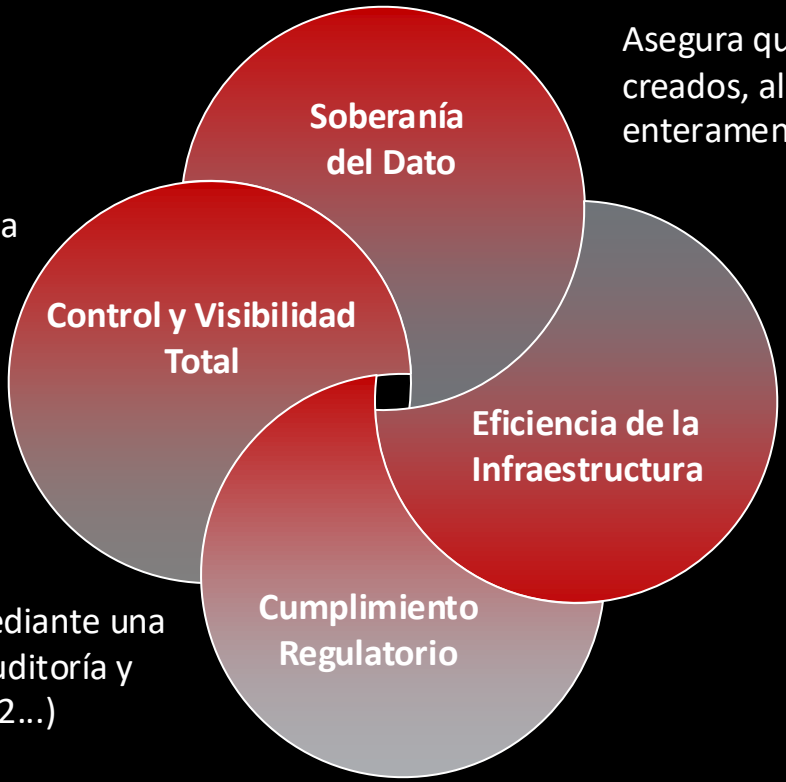
Trend Vision One ™ Sovereign and Private Cloud (SPC)

Soberanía del dato

Soberanía operacional

Soberanía tecnológica

Nubes Soberanas e Infraestructura hibrida



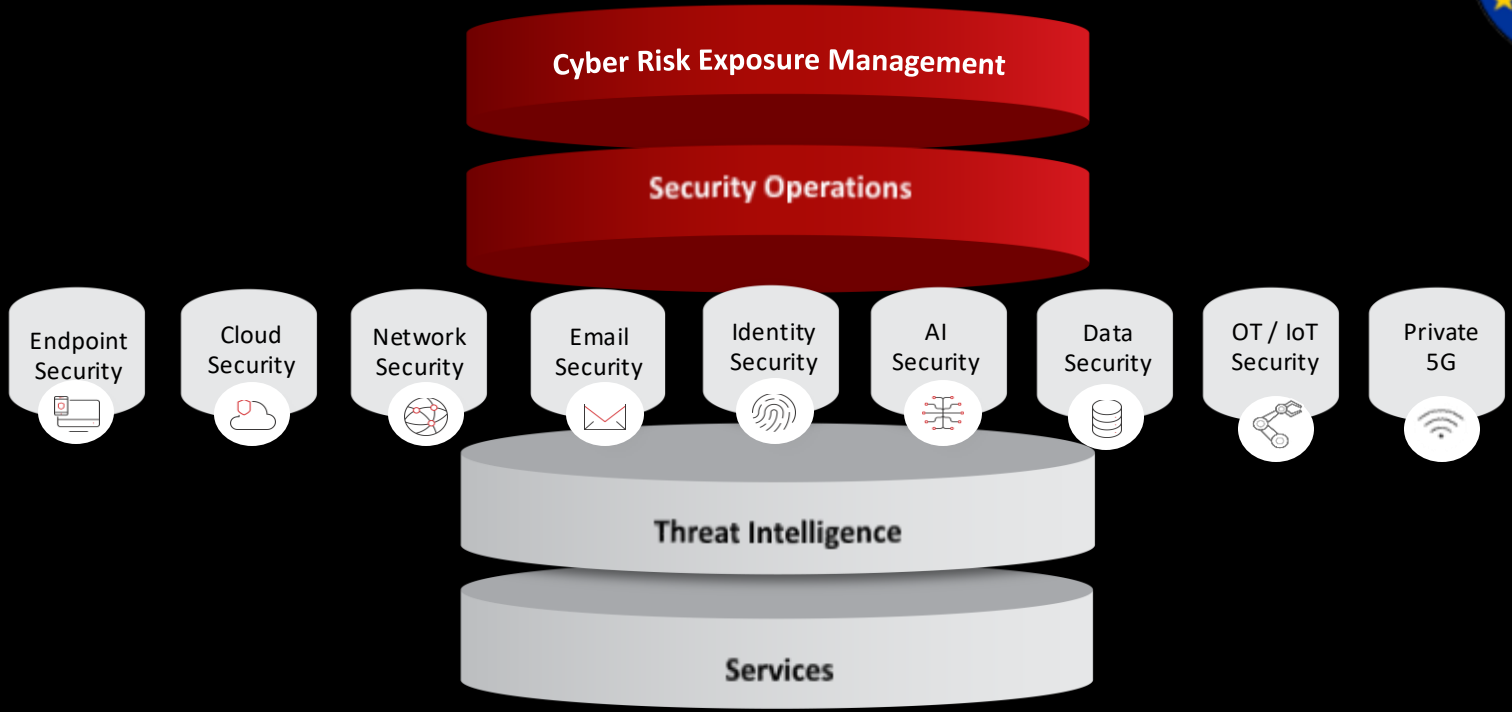
Asegura que los datos sensibles sean creados, almacenados y procesados enteramente dentro de la jurisdicción la UE.

Ciberseguridad de extremo a extremo totalmente controlada por la organización.

Integra capacidades avanzadas de ciberseguridad en las inversiones existentes.

Cumple con las regulaciones mediante una estricta localización de datos, auditoría y aplicación de políticas (ENS, NIS2…)

Nubes Soberanas e Infraestructura híbrida



Trend Vision One ™ Sovereign and Private Cloud (SPC)

Cloud pública

Cloud híbrida

On-premise

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 lideres de IA.

Barcelona Supercomputing Center

TREND MICRO | NVIDIA

TREND MICRO

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)

TREND MICRO

Seguridad para la IA

	Security Challenges	Security Controls	Trend Vision One
Data	Sensitive information blind spots	Secure Data	**Trend Vision One™ Cybersecurity Platform**
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	

TREND MICRO

Gracias!

Madrid, Septiembre 2025

Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad