SOCINFO sociedad de la información digital

CIBERAMENAZAS 2026
NUEVOS RETOS

Javier Candau
Centro Criptológico Nacional
ccn@cni.es

ESPAÑA CENTRO NACIONAL DE INTELIGENCIA

CCN centro criptológico nacional

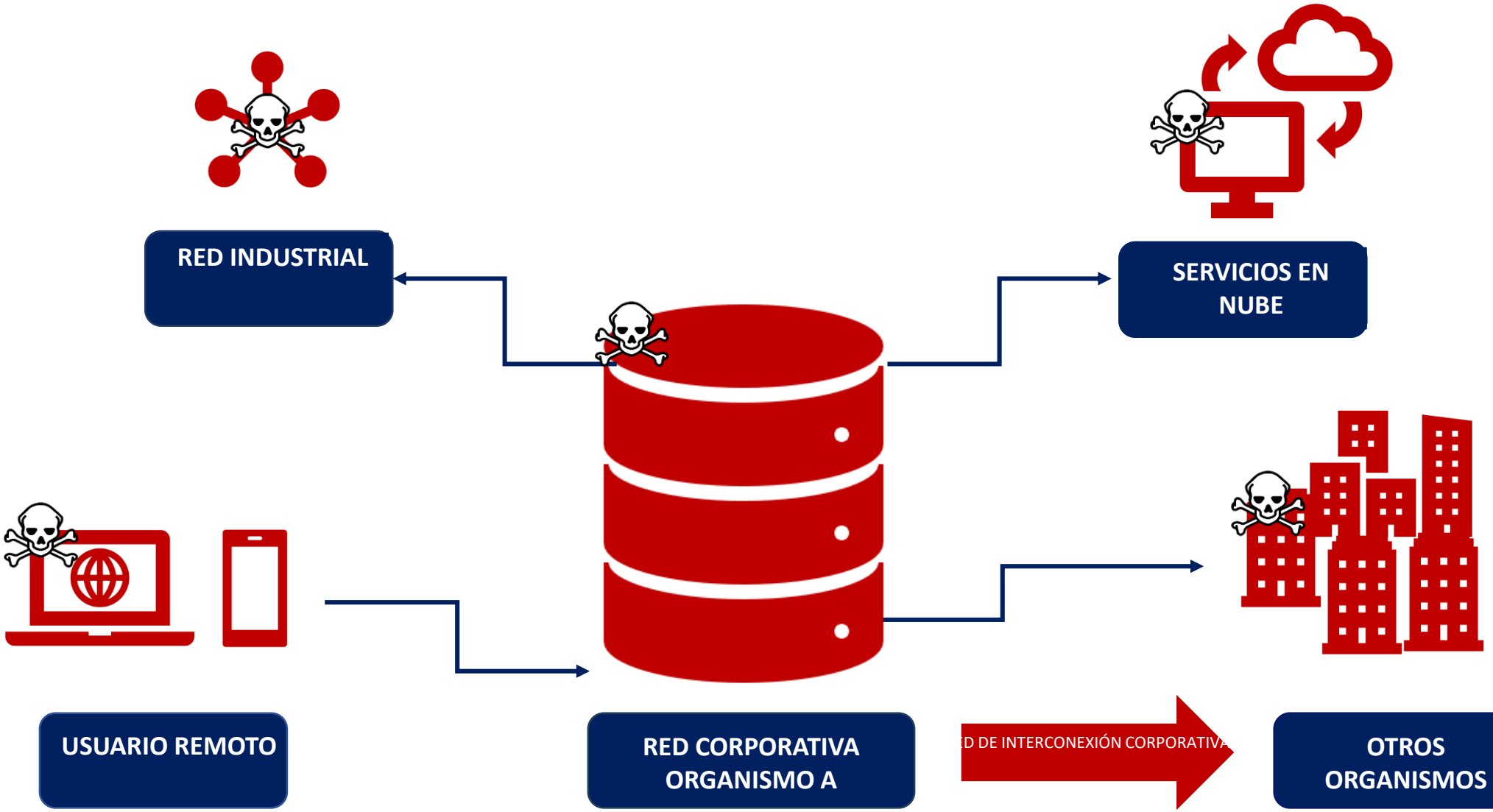
NO HAY TRANSFORMACIÓN DIGITAL SIN CIBERSEGURIDAD

RED CORPORATIVA | NEGOCIO

- USO DE LA NUBE
- TELEFONÍA MÓVIL
- RED INDUSTRIAL
- ACCESOS REMOTOS
- INTELIGENCIA ARTIFICIAL (AI)

CCN
centro criptológico nacional

DESCENTRALIZADOS, PERO HIPERCONECTADOS



INFRAESTRUCTURAS CRÍTICAS vs SERVICIOS ESENCIALES

SECTORES ALTA CRITICIDAD

1. Energía
   a) Electricidad
   b) Petróleo
   c) Gas
   d) Hidrógeno
   e) Calefacción urbana

2. Transportes
   a) Aéreo
   b) Ferrocarril
   c) Marítimo y fluvial
   d) Carretera

3. Banca

4. Infraestructuras de mercados financieros

5. Sanidad

6. Agua potable

7. Aguas Residuales

8.Infraestructuras y Servicios Digitales

9.Gestión de servicios TIC

10. Administración
   a) AGE
   b) CCAA
   c) EELL

11. Espacio

Industria nuclear

SECTORES CRITICOS

1. Servicios Postales y mensajería

2. Gestión de Residuos

3. Fabricación, producción y distribución de sustancias y mezclas químicas

4. Alimentación
   a) Producción
   b) Transformación
   c) Distribución

5. Producción
   a) Sanitarios
   b) Informat/Electr./óptico
   c) Material eléctrico
   d) Maquinaria y equipo
   e) Vehículos, remolques
   f) Otro material transporte

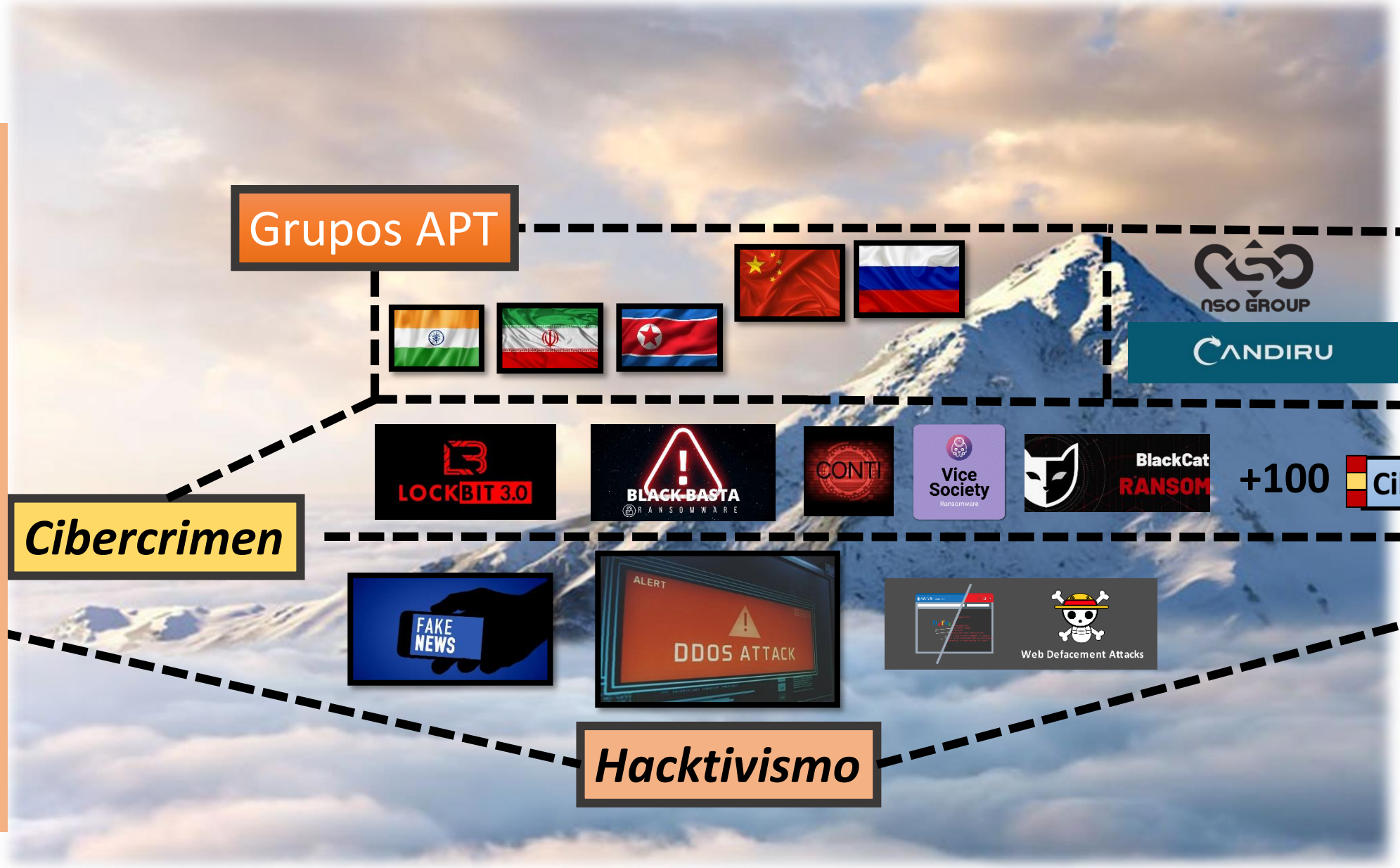
6. Proveedores de Servicios Digitales

7. Inst. Investigación

Infraestructuras críticas (2011)
Servicios esenciales NIS1.0 (2016)
Servicios esenciales NIS2.0 (2022)

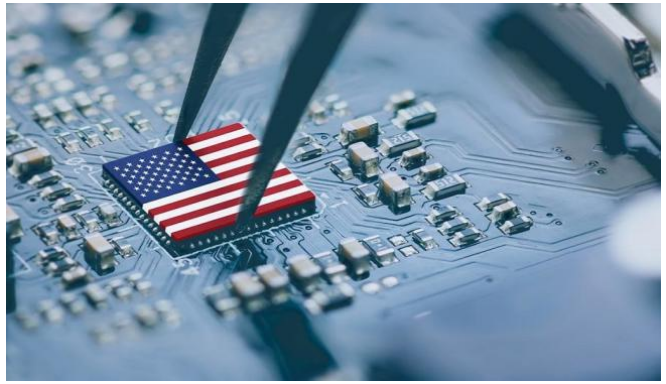
Mayoría operadores Públicos

¿CONTRA QUÉ LUCHAMOS?



¿QUE HA CAMBIADO EN 2026?

Claude
Mythos



CCN
centro criptológico nacional

EVOLUCIÓN CIBERATAQUES + IA

2019-2021
Automatización Básica

2022-2023
Auge LLMs y Phishing avanzado

2024
Deepfakes y Fraude Corporativo

2025
Adopción Masiva IA
por +50 grupos APTs
(CH, RU, NK, …)

2026

Claude Mythos

GPT-5.5 Cyber

Claude Mythos como disrupción:
(i) Descubrimiento autónomo de vulnerabilidades
(ii) Explotación de semanas a minutos
(iii) Operaciones de ataque semiautónomas reales
(iv) Adaptación dinámica a sistemas defensivos

Además **GPT-5.5 Cyber (OpenAI) e IAs especializadas / IAs sin restricciones**

CCN centro criptológico nacional

RIESGOS DE LA IA OFENSIVA AVANZADA

1. Automatización del ciberataque

(i) Generación autónoma de exploits, phishing y malware adaptativo
(ii) Ataques personalizados a gran escala (ingeniería social hiperrealista)
(iii) Reducción del tiempo entre descubrimiento y explotación (zero-day)

2. Evasión de detección

(i) Malware polimórfico impulsado por IA
(ii) Capacidad de aprender y evadir IDS/IPS y EDR en tiempo real
(iii) Simulación de tráfico legítimo para ocultación (camuflaje avanzado)

3. Escalada y persistencia

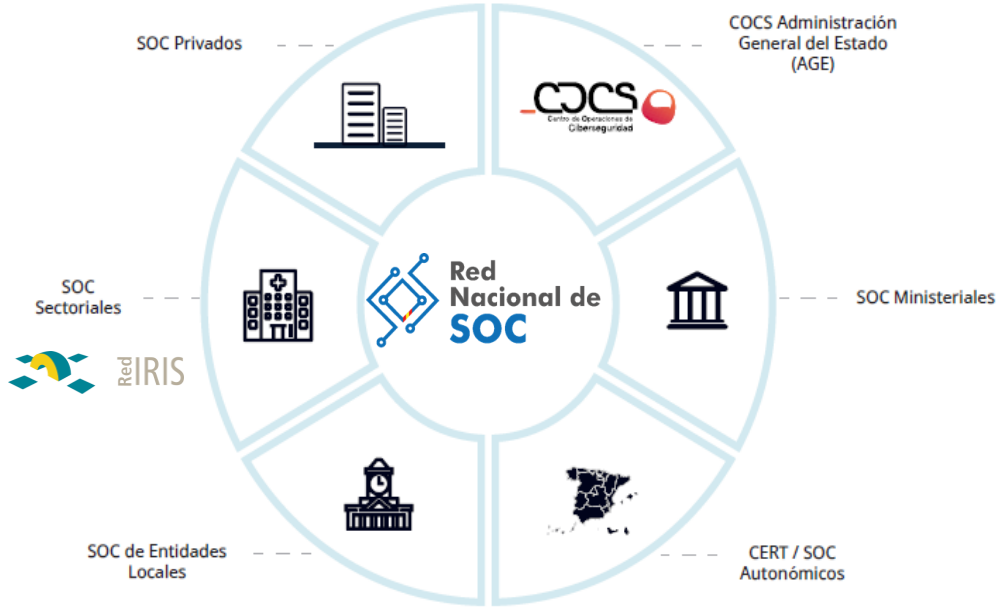
(i) Movimiento lateral inteligente en redes complejas
(ii) Identificación automática de activos críticos
(iii) Persistencia optimizada con mínima huella

4. Riesgo de dependencia tecnológica

(i) Excesiva confianza en modelos opacos (“black-box”)
(ii) Dificultad para auditar decisiones automatizadas
(iii) Posibles fallos sistémicos si la IA es comprometida

RNS – INTERCAMBIO ACTIVO

Art.	Obligación
29	**Mecanismos de intercambio de información sobre ciberseguridad**
	• Las entidades incluidas en el ámbito de aplicación de la Directiva y, cuando proceda, otras entidades no incluidas (sus proveedores o prestadores de servicios), podrán **intercambiar** entre sí **de forma voluntaria**, a través de mecanismos de intercambio facilitados por los Estados miembros, información relevante sobre ciberseguridad, en particular la relativa a ciberamenazas, cuasi-incidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, tácticas de los adversarios, información específica del agente de riesgo, alertas de ciberseguridad y recomendaciones sobre configuraciones de las herramientas de seguridad para detectar ciberataques, **siempre que tenga por objeto** prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o refuerce el nivel de ciberseguridad. • el intercambio de información se desarrollará dentro de comunidades de entidades esenciales e importantes y, cuando proceda, sus proveedores o prestadores de servicios. • las entidades esenciales e importantes **notificarán** a las autoridades competentes su participación (**incorporación** y **retirada**) en los mecanismos de intercambio de información sobre ciberseguridad.



EVOLUCIÓN EVENTOS COMPARTIDOS

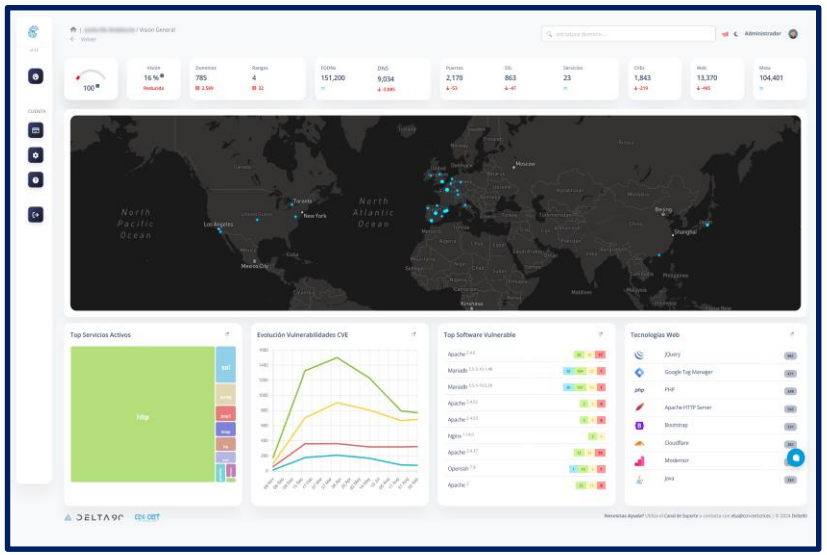
+500 eventos/día

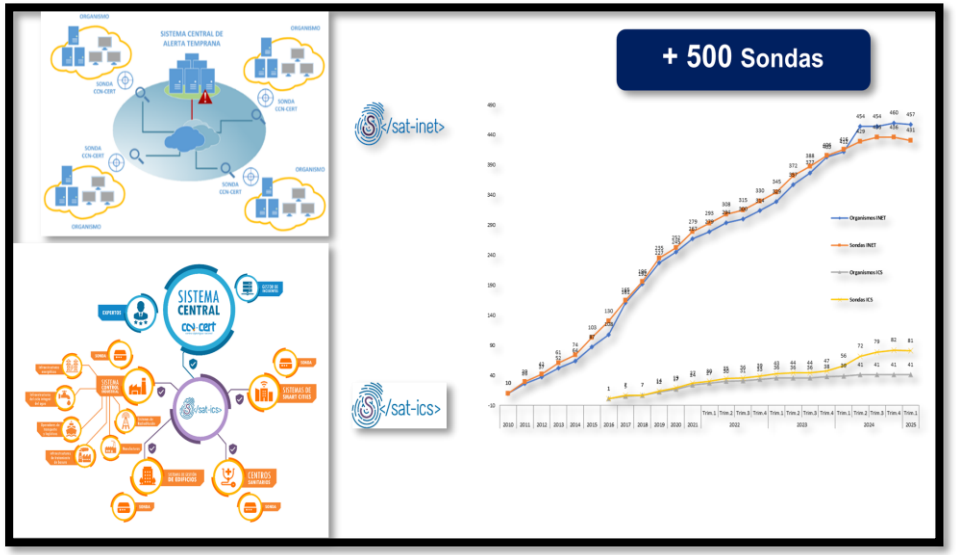
HERRAMIENTAS EN CCN-CERT

</sat-inet>

</sat-ics>

</elsa>
Exposición Local y Superficie de Ataque





SAT-INET

453 Organismos adheridos

427 Sondas desplegadas

SAT-ICS

41 Organismos adheridos

79 Sondas desplegadas

</reyes>

</lucía>

CERT/CSIRT
COMUNIDAD

ATACANTES

- Actores, motivación, financiación, formación, modus operandi,…

INFRAESTRUCTURAS

- Sistemas C&C, nodos, saltos, IPs / Dominios

CAPACIDADES

- Exploits propios, vectores infección, cifradao / RAT, persistencia,…

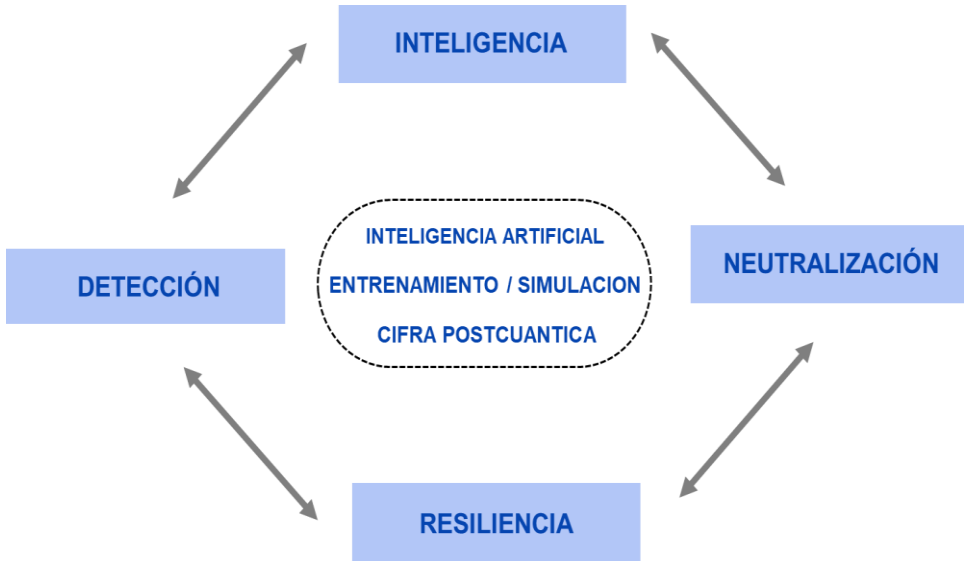
VÍCITMAS

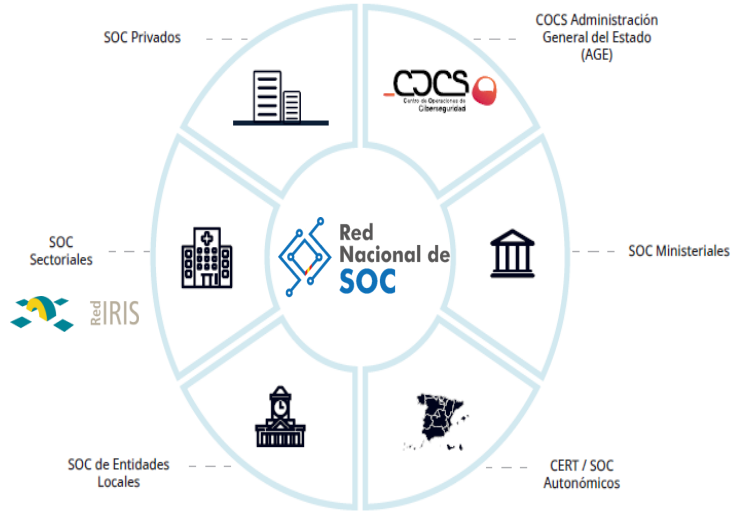
- Sectores afectados, métodos de infección

COMUNIDAD
CERT/CSIRT

CCN
centro criptológico nacional

ADAPTARNOS NUEVO ESCENARIO





DEFENSA

- Detección automática de vulnerabilidades propias
- Análisis de código y revisión de seguridad continua
- Simulación de adversarios (Red Team automatizado)
- Triage automático de alertas e incidentes
- Inteligencia de amenazas en tiempo real

SOC AGENTICO

Nuevo SOC / CSIRT

Necesidad de SOC/CSIRT inteligente con uso masivo de IA para prevención, Detección y respuesta

Necesidad de una TRANSICIÓN POSCUÁNTICA SEGURA

COMPUTACIÓN CUÁNTICA

“almacena ahora y descifra luego”

CRIPTOGRAGÍA DE CLAVE PÚBLICA
FIRMAS DIGITALES

Sin seguridad (ROTOS)

CRÍTICO

CRIPTOGRAGÍA DE CLAVE SECRETA
FUNCIONES RESUMEN (HASH)

Seguridad a la mitad

AMENAZA

Ordenador cuántico computacionalmente relevante : **2030?**

NUEVOS ALGORITMOS (2016-)

Algoritmos postcuánticos (PQC)
Distribución cuántica claves(QKD)

PLAN DE MODERNIZACIÓN CRIPTO (2021)

Cifradores Quantum Resistant (QR)
Productos QR

PLAN DE MIGRACIÓN Y MITIGACIÓN (2026)

Qué necesito proteger
Medidas seguridad adicionales

Muchas

Gracias