



CIBERESCUDO
CCN-CERT | RNS



CCN
centro criptológico nacional

ÍNDICE

- Apoyos en Iberoamérica
- Red Nacional de SOC
- SOC Desplegable (DSOC)
- Ciberescudo



APOYOS EN IBEROAMÉRICA



EL CCN-CERT EN IBEROAMÉRICA. 2026



- **MÉXICO:** Participación en el Congreso de Ciberseguridad. Proyecto SDOC Desplegable.
- **GUATEMALA:** Proyecto SOC Nacional. Financiación UE. Proyecto SOC Desplegable.
- **HONDURAS:** Proyecto SOC Desplegable.
- **REPÚBLICA DOMINICANA:** Proyecto SOC Nacional.
- **COSTA RICA:** Proyecto formación. Laboratorios. RNS. Financiación UE.
- **ECUADOR:** Proyecto de Capacitación. Proyecto CTI. Asesoramiento. Financiación UE.
- **COLOMBIA:** Proyecto piloto SAT. Financiación BID.
- **BRASIL:** Proyecto piloto SAT. Financiación BID.
- **ARGENTINA:** Proyecto SOC Desplegable.
- **CHILE:** Auditoría y asesoramiento en SOC.

EL CCN-CERT EN IBEROAMÉRICA. 2026





Red Nacional de SOC de España

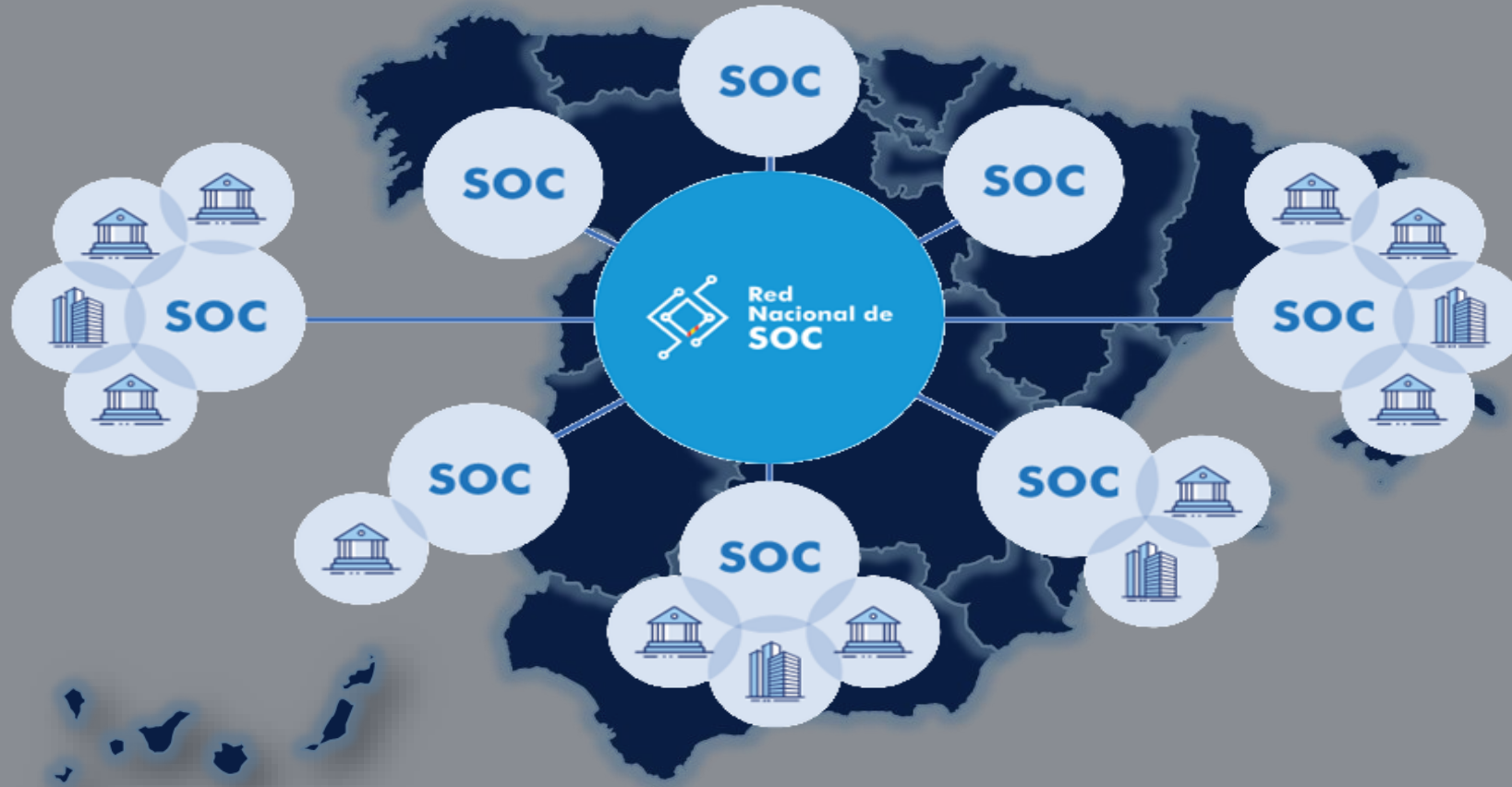


La necesidad ...



Plataforma que integra los SOC de las AAPP

- Bloqueo inmediato de actividad anómala



Alertas, no Incidentes

- Indicadores de Compromiso/Indicadores de Ataque



- Direcciones IP
- Dominios
- URL
- Hashes
- Direcciones
- Reglas

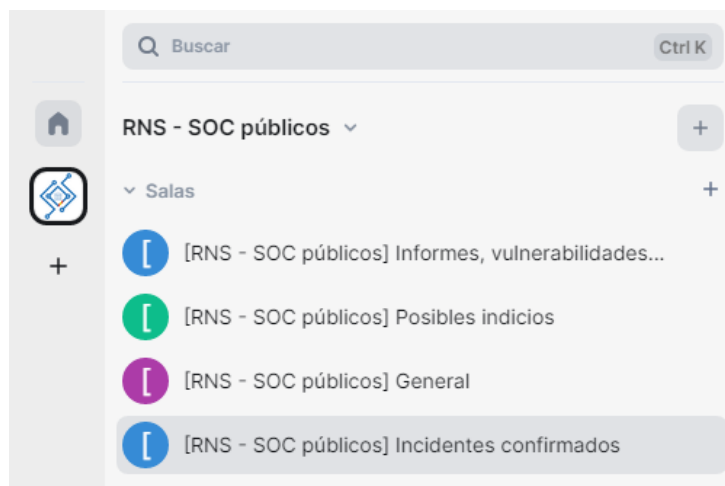
Obligatorio!

- **No** datos personales / **víctimas**
 - Lo filtra cada uno
- **No** compartir **informes** genéricos

“Sólo comparto lo que yo mismo estoy ya bloqueando”

Solución de mensajería

- ELEMENT



[RNS - SOC públicos] Incidentes confirmados Sala para intercambiar información relevante sobre incidentes confirmados, que permita poner en guardia al resto de miembros y activar las medidas preventivas.

mar. 18 de oct. de 2022

Álvaro - CCN-CERT

Buenas tardes. Estamos gestionando un incidente del ransomware Hive 14:39

Por ahora hemos identificado un C2 de SystemBC: 104[.]238.140.73 14:39

👍 1

NO estaba en las listas negras de REYES, lo incluiremos ahora 14:40

Hay una muestra de hace un mes asociada en VT:
<https://www.virustotal.com/gui/file/c1f83eca657eb74769e9df053eb430c11cbcb123004179f2196fec6f45e48099>

Si encontramos algo más os iremos informando

[RNS - SOC públicos] General Sala para comentar asuntos generales, que no tengan una sala dedicada: Funcionamiento de la RNS (herramientas, procedimientos, dudas...); Avisos importantes no técnicos (eventos, pliegos...); ...

(Ayto)

buenos días, disculpar por si no procede mucho pero me gustaria conocer experiencias sobre EDR/XDR de [redacted]. Estamos valorando opciones. Gracias 14:02

Ignacio - CCN

Además de las opiniones recordaros que incorporen en las ofertas el servicio de actuación sobre el EDR. 14:13

cert ()

Estamos por sacar un concurso para adquirir la nueva solución EDR. Para ello hemos echo una PoC de 70 días tanto con [redacted]. Ambas soluciones pueden satisfacer nuestras necesidades. Si tuviera que poner un elemento diferencial mencionaría que la capacidad de SOAR de

Solución de intercambio

- MISP



Event ID	3405						
UUID	8da26aaa-f6b1-4984-a6c7-42242f5c1c7b  						
Creator org	RNS (Red Nacional de SOC)						
Owner org	RNS (Red Nacional de SOC)						
Tags	 tlp:amber   source:red-nacional-soc   red-nacional-soc:source="misp" 						
Info	IP maliciosas implicadas en un incidente con un Exchange comprometido						
☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies
☐	2022-10-10		Payload delivery	filename	%WINDIR%\System32\inetsrv\iprest.dll	  	 
☐	2022-10-10		Payload delivery	filename	iprest.dll	  	 
☐	2022-10-10		Payload delivery	md5	45b6f589f39c2fcd64dbe61fa8c22725	  	 
☐	2022-10-10		Network activity	ip-dst	212.193.139.92	  	 
☐	2022-10-10		Network activity	ip-dst	195.209.103.197	  	 

Página web

- <https://rns.ccn-cert.cni.es>



Buscar en la RNS



ÁREA PRIVADA

SALIR

ESP

SOBRE LA RNS

IMPLANTACIÓN DE UN SOC

DIVULGACIÓN

CONTACTA

SOLICITUD DE ADHESIÓN

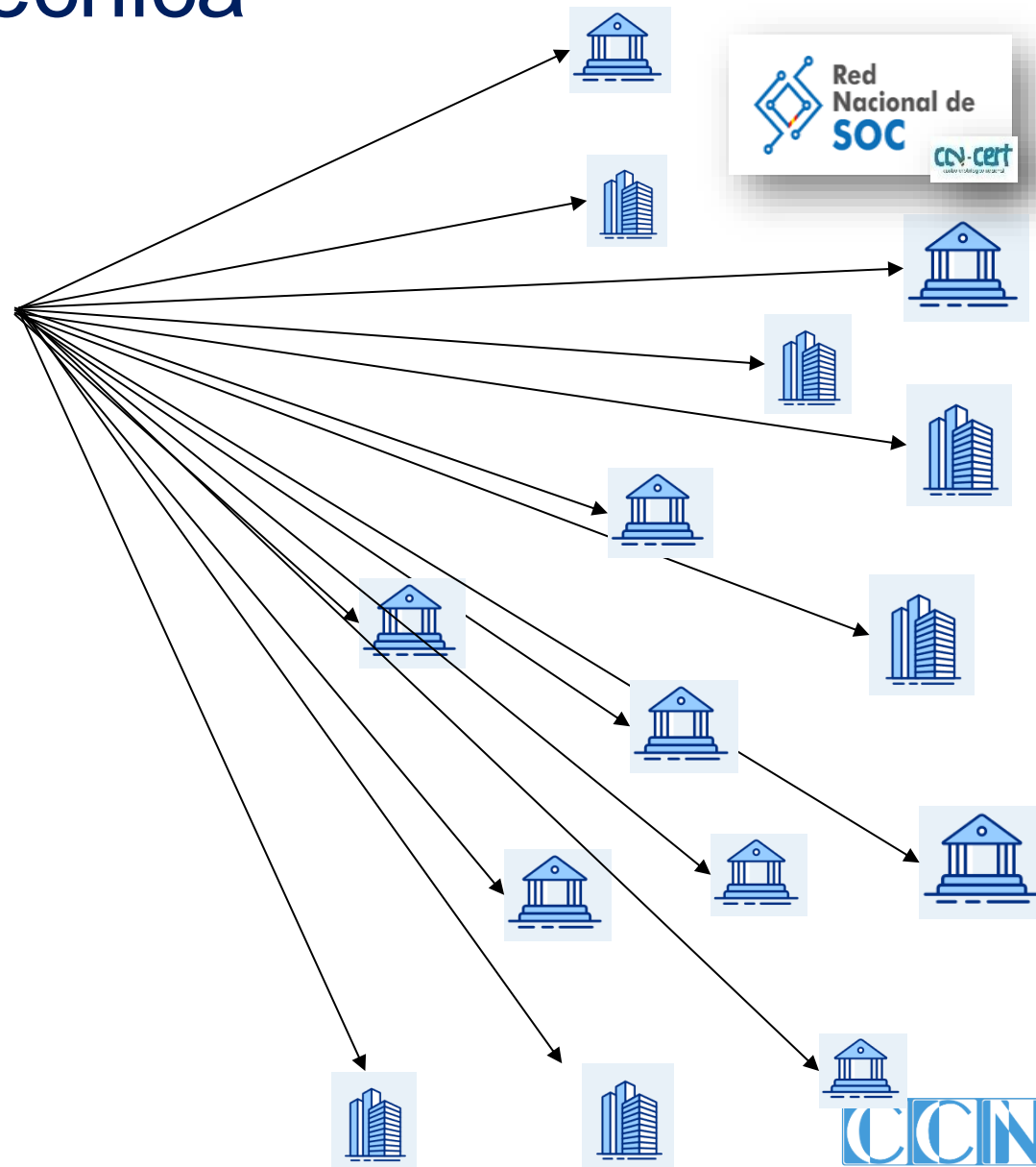
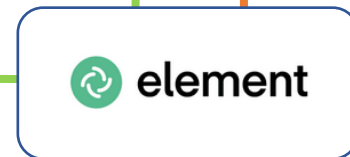
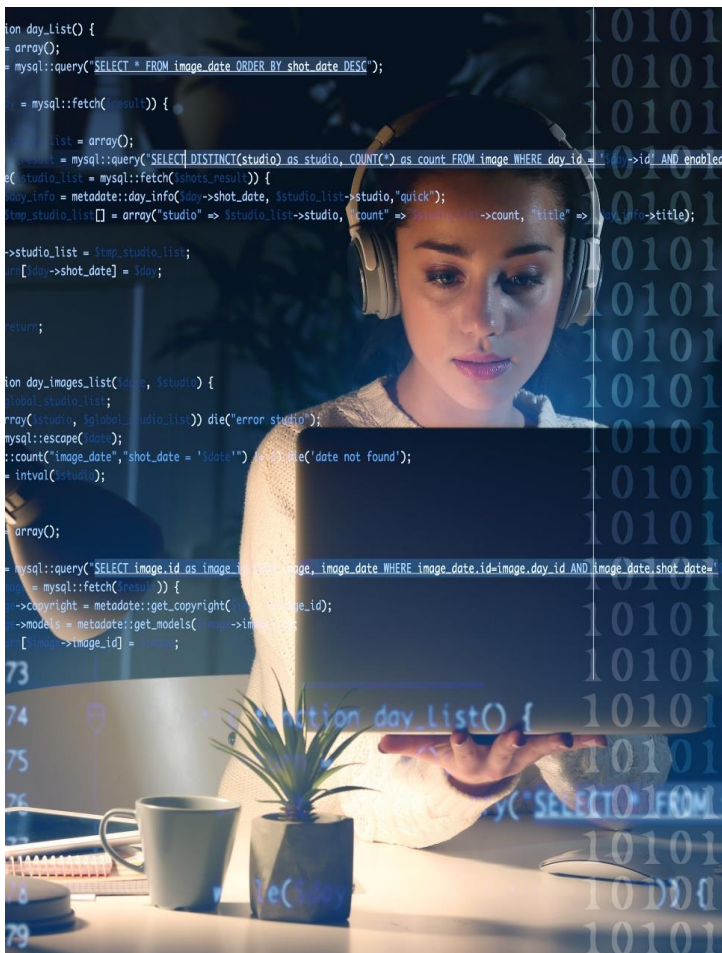
Red Nacional de SOC

Instrumento para coordinar la colaboración y el intercambio de información entre los Centros de Operaciones de Ciberseguridad del sector público español.



Intercambio de información técnica

- ¿cuál es la idea?



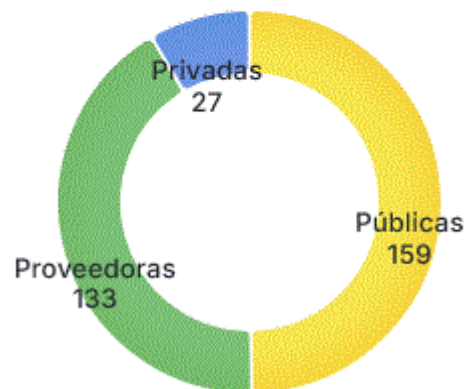
Miembros de la RNS

- Evolución

Entidades (Total)

319

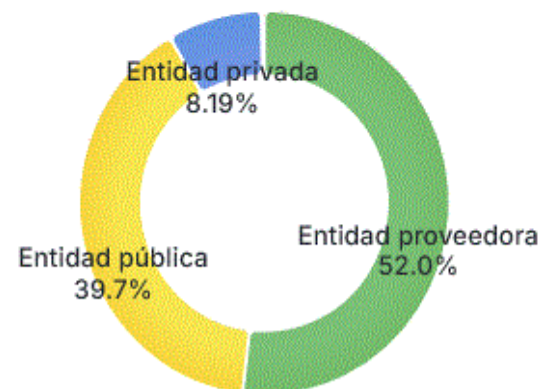
Entidades por categoría



Personas (Total)

1135

Personas por categoría



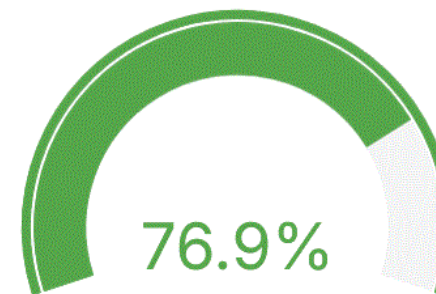
MISP de la RNS

- Datos intercambio

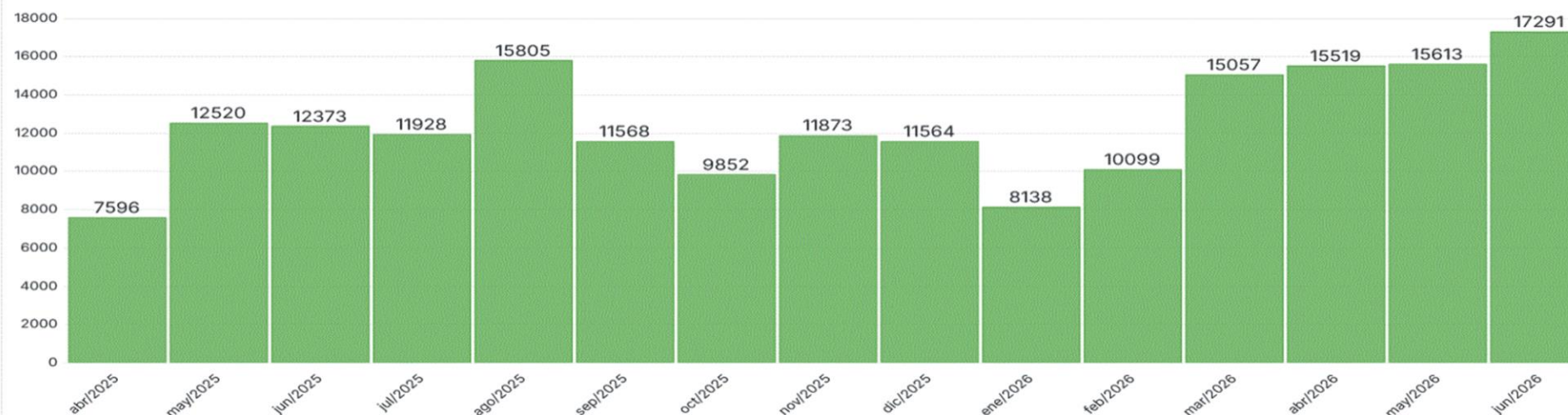


515

Descartados (%) ⓘ ⓘ Last 30 days

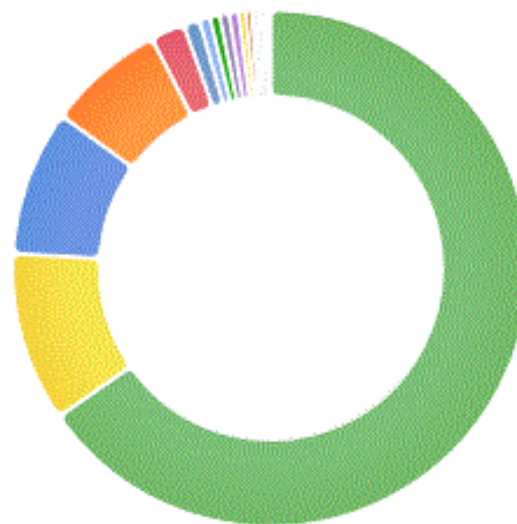


Publicados (evolución) ⓘ ⓘ Last 15 months



Tipos de ataques mas comunes

Por clasificación (CCN-STIC 817) ⌚ Last 30 days



- Intento de intrusión - Intento de acceso con vulneración de credenciales 66%
- Obtención de info. - Escaneo de redes (scanning) 11%
- Fraude - Phishing/Suplantación 9%
- Intento de intrusión - Explotación de vuln. conocidas 7%
- Contenido abusivo - Spam 2%
- Intento de intrusión - Ataque desconocido 1%
- Fraude - Uso no autorizado de recursos 1%
- Intrusión - Compromiso de aplicaciones 1%
- Intrusión - Compromiso de cuenta sin privilegios 1%

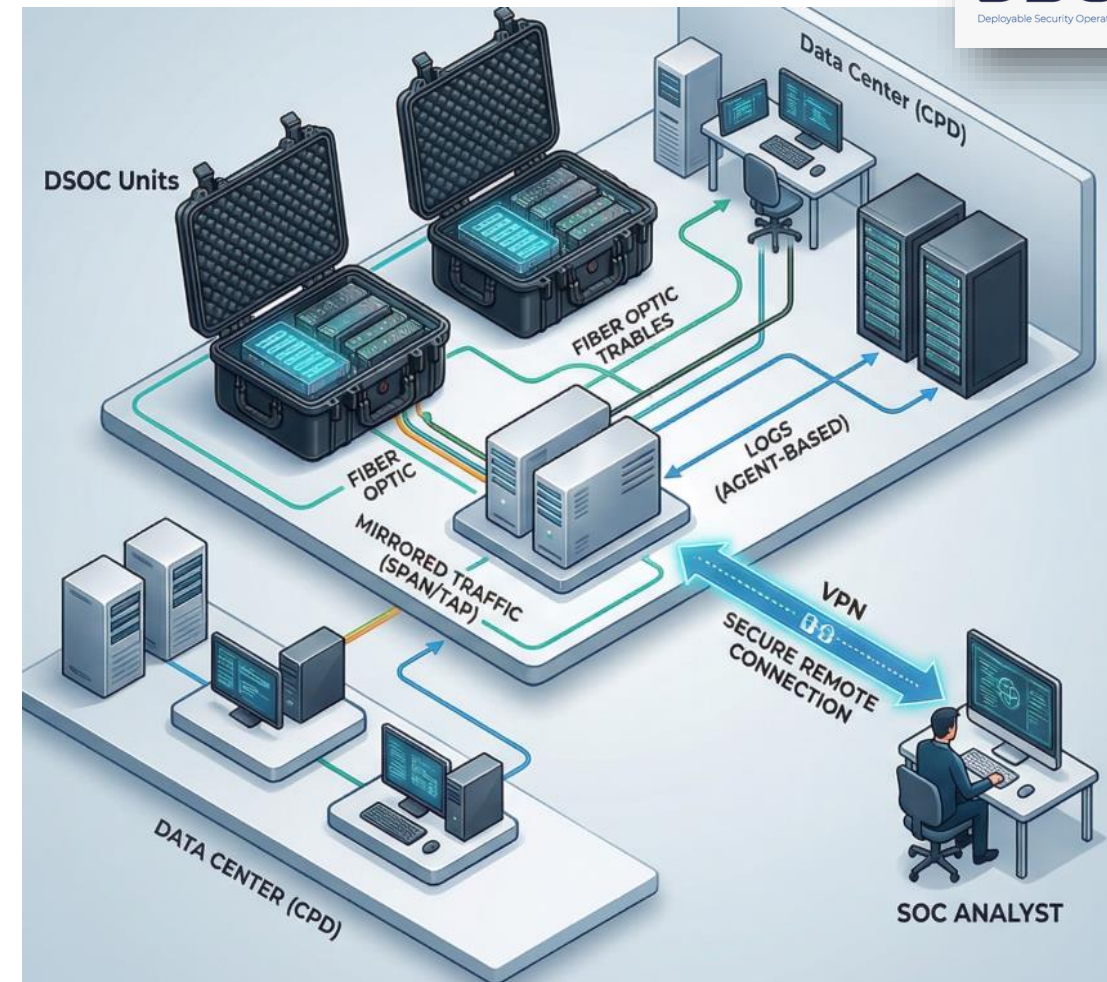


SOC Desplegable (DSOC)



SOC DESPLEGABLE

- DETECCIÓN

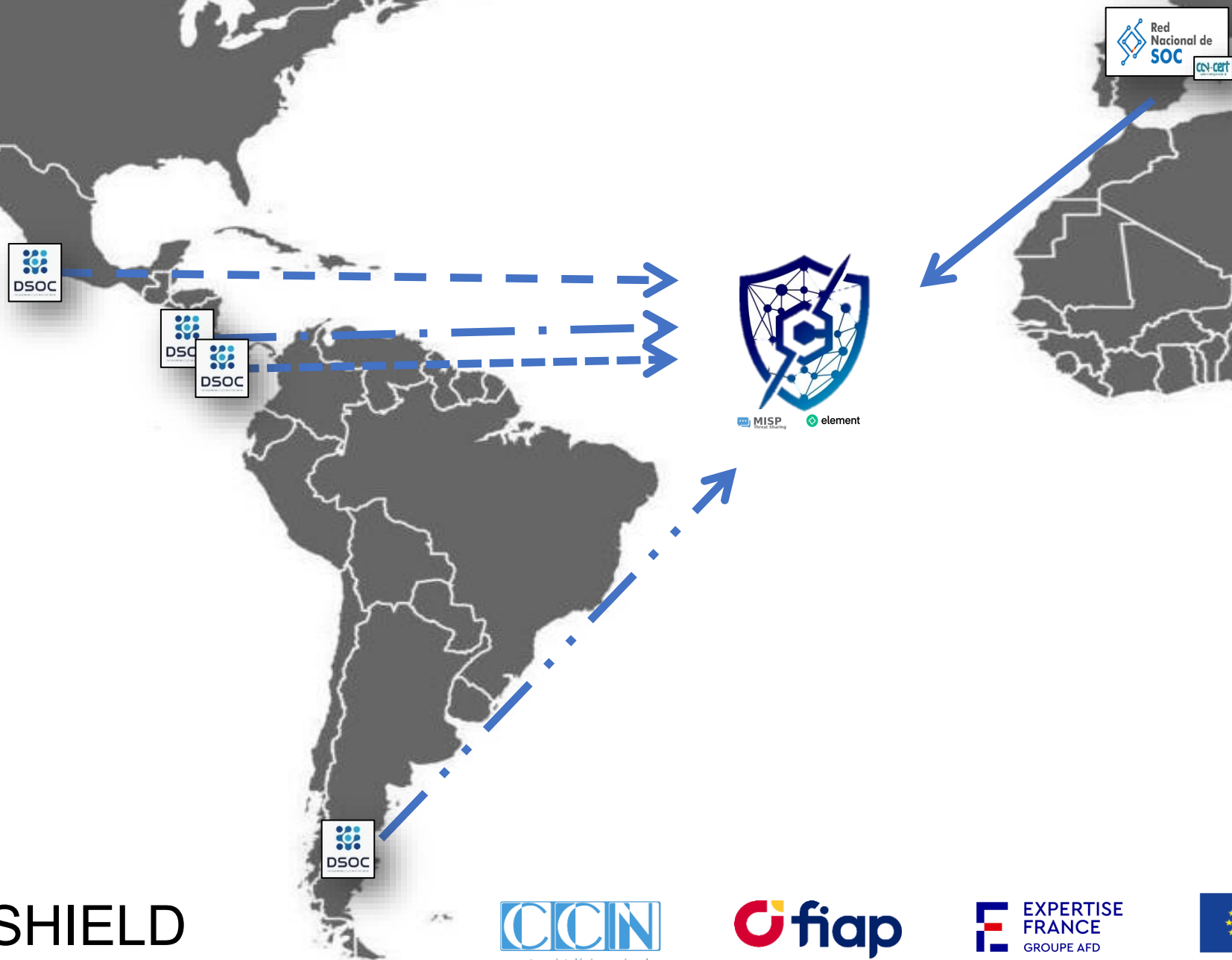




CIBERESCUDO



CYBERSHIELD





Local organisations, both local and remote

« previous next »

+ Add

Local organisations

Known remote organisations

All organisations

ID	Name	UUID	Description	Nationality	Sector
5	CCN-CERT (España)	17843f96-d914-4aab-8257-3023485ecf78		 Spain	
2	Ciberescudo	93efa70e-8a7b-4569-b9fd-c2a3c0544405			
6	SOC - MICITT (Costa Rica)	01e6bfc5-63d8-45c9-868a-0996d5f33c44		 Costa Rica	
3	SOC - SEFIN (Honduras)	d52bcbde-2218-4455-9d89-ce8867472da0		 Honduras	
4	SOC - SIE (Guatemala)	0c4eaa06-d5e9-4e92-86cb-e2fd65ec813b		 Guatemala	

Page 1 of 1, showing 5 records out of 5 total, starting on record 1, ending on 5

« previous next »

CIBERESCUDO

[Event Actions](#)[Dashboard](#)[Galaxies](#)[Input Filters](#)[Global Actions](#)[Sync Actions](#)[Administration](#)[API](#)[Bookmarks ▾](#)[MISP](#)[Carlo](#)

		ciberescudo:status="ongoing" ciberescudo:source="element" source:ciberescudo ciberescudo:status="Publicado" ciberescudo:org="SOC - SEFIN (Honduras)"				
☐	✓ Ciberescudo ? 19	tlp:green PAP:GREEN ciberescudo:status="ongoing" ciberescudo:source="element" source:ciberescudo ciberescudo:status="Publicado" ciberescudo:org="SOC - MICITT (Costa Rica)"	4	2026-05-26	TCLBANKER Troyano Bancario WhatsApp Outlook	All
☐	✓ Ciberescudo ? 18	tlp:green PAP:GREEN ciberescudo:status="ongoing" ciberescudo:source="element" source:ciberescudo ciberescudo:status="Publicado" ciberescudo:org="SOC - MICITT (Costa Rica)"	133	2026-05-26	Phantom Panda IOC parte 2 de 2	All
☐	✓ Ciberescudo ? 17	tlp:green PAP:GREEN ciberescudo:status="ongoing" ciberescudo:source="element" source:ciberescudo ciberescudo:status="Publicado" ciberescudo:org="SOC - MICITT (Costa Rica)"	150	2026-05-26	Phantom Panda IOC parte 1 de 2	All
☐	✓ Ciberescudo ? 12	tlp:green PAP:GREEN ciberescudo:status="ongoing" ciberescudo:source="element" source:ciberescudo ciberescudo:status="Publicado" ciberescudo:org="SOC - SIE (Guatemala)"	1	2026-05-22	IOC	All
☐	✓ Ciberescudo ? 14	tlp:green PAP:GREEN ciberescudo:status="ongoing" ciberescudo:source="element" source:ciberescudo	1	2026-05-22	IOC	All

- <https://ciberescudo.ccn-cert.cni.es/ciberescudo>



Estás en: [Inicio](#) > C

INICIO

CIBERESCUDO

MEMBRESÍA

INFORMACIÓN A COMPARTIR

INFRAESTRUCTURA TECNOLÓGICA

BENEFICIOS DE PARTICIPAR

ADHESIÓN

puesta rápida, coordinada y global. Ante la necesidad de mejorar las
CiberEscudo, una iniciativa impulsada para interconectar los Centros de
 América.

servicio de protección de sus miembros mediante el bloqueo casi inmediato de
 ectando en cualquier punto de la red. Al compartir inteligencia sobre amenazas
 en un país o sector pueda ser mitigado preventivamente en toda la región

