CIBERESCUDO
CCN-CERT | RNS

CCN
centro criptológico nacional

# ÍNDICE

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

# APOYOS EN IBEROAMÉRICA

centro criptológico nacional

centro criptológico nacional

# 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.

CCN
centro criptológico nacional

# EL CCN-CERT EN IBEROAMÉRICA. 2026


CCN
centro criptológico nacional

# Red Nacional de SOC de España

Red Nacional de SOC

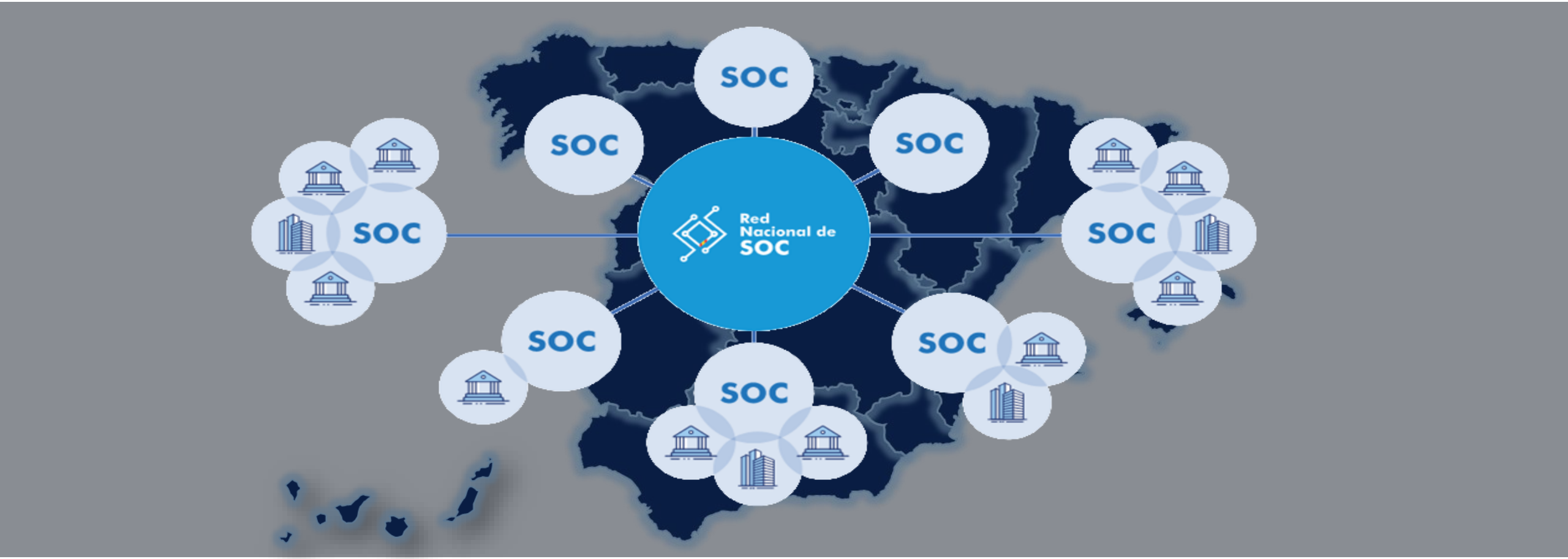
CCN-CERT

CCN
centro criptológico nacional

# 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
- Direccio
- Reglas

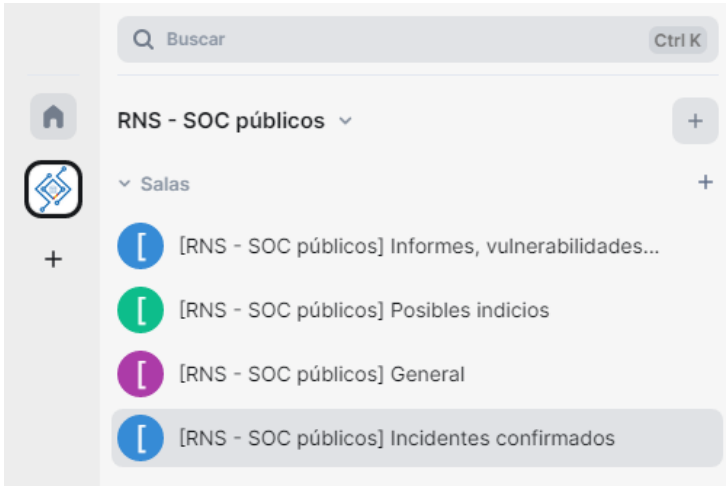
**Obligatorio!**

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

**“Sólo compa lo que yo mismo estoy ya bloqueando”**

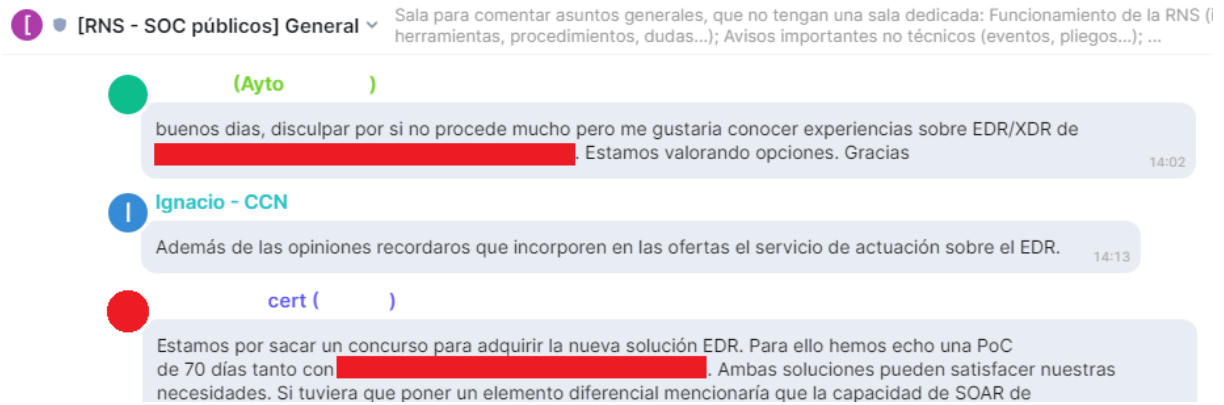
# Solución de mensajería

- ELEMENT





element



# 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 x source:red-nacional-soc x red-nacional-soc:source="misp" x |
| Info | IP maliciosas implicadas en un incidente con un Exchange comprometido |

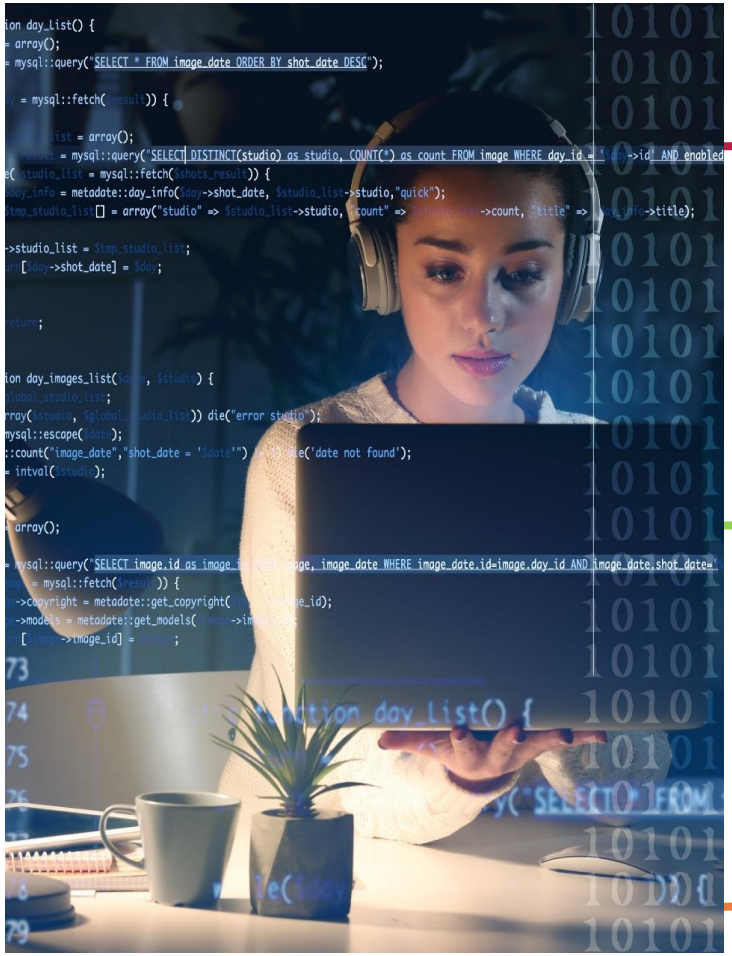
| Date | Org | Category | Type | Value | Tags | Galaxies | Com |
|---|---|---|---|---|---|---|---|
| 2022-10-10 | | Payload delivery | filename | %WINDIR%\System32\inetsrv\iprest.dll | | | |
| 2022-10-10 | | Payload delivery | filename | iprest.dll | | | |
| 2022-10-10 | | Payload delivery | md5 | 45b6f589f39c2fcd64dbe61fa8c22725 | | | |
| 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

# Intercambio de información técnica

- ¿cuál es la idea?



MISP Threat Sharing

element

Red Nacional de SOC

CCN-CERT

CCN centro criptológico nacional

# Miembros de la RNS

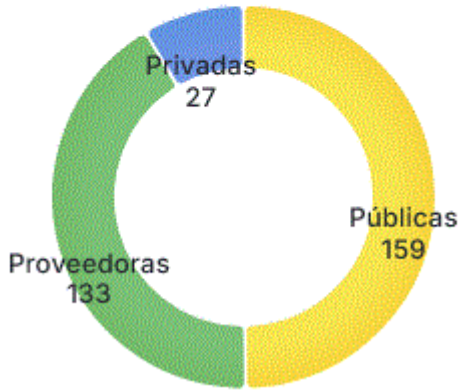
- Evolución

Red Nacional de SOC

Entidades (Total)

319

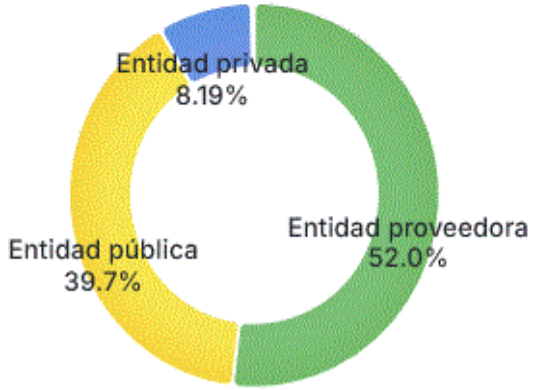
Entidades por categoría




Personas (Total)

1135

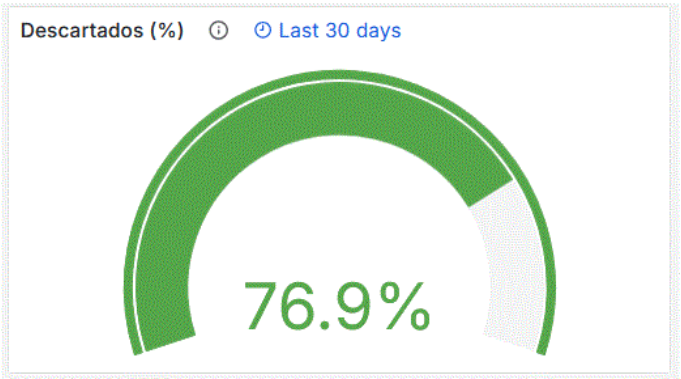
Personas por categoría

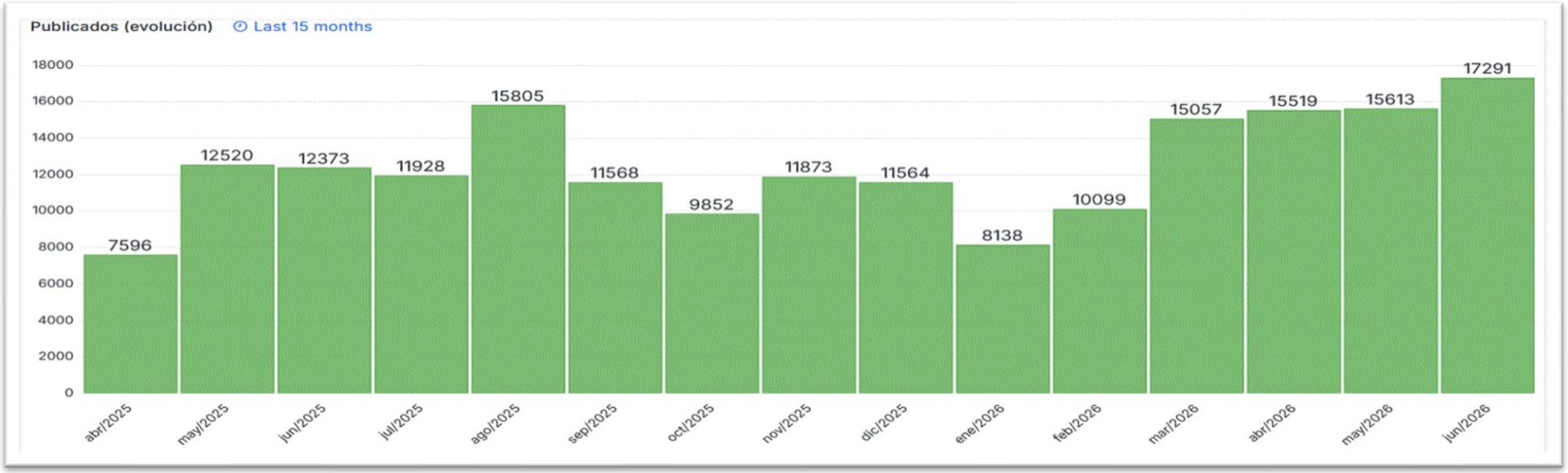



CCN centro criptológico nacional

# MISP de la RNS

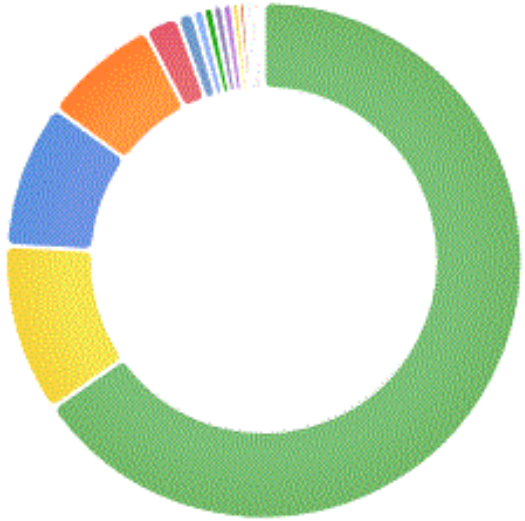
- Datos intercambio

# 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%

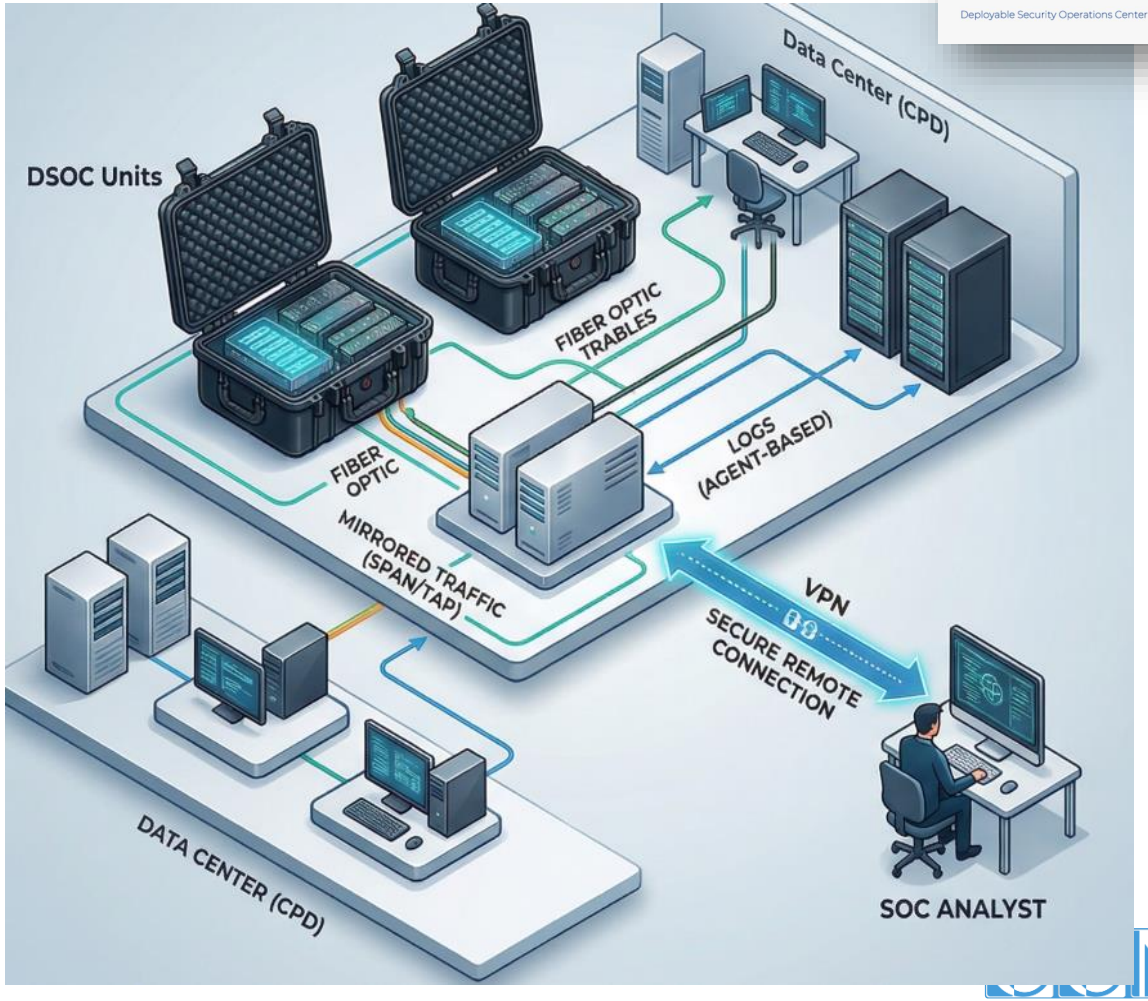
# SOC Desplegable (DSOC)

DSOC
Deployable Security Operations Center

CCN
centro criptológico nacional

# SOC DESPLEGABLE

- DETECCIÓN

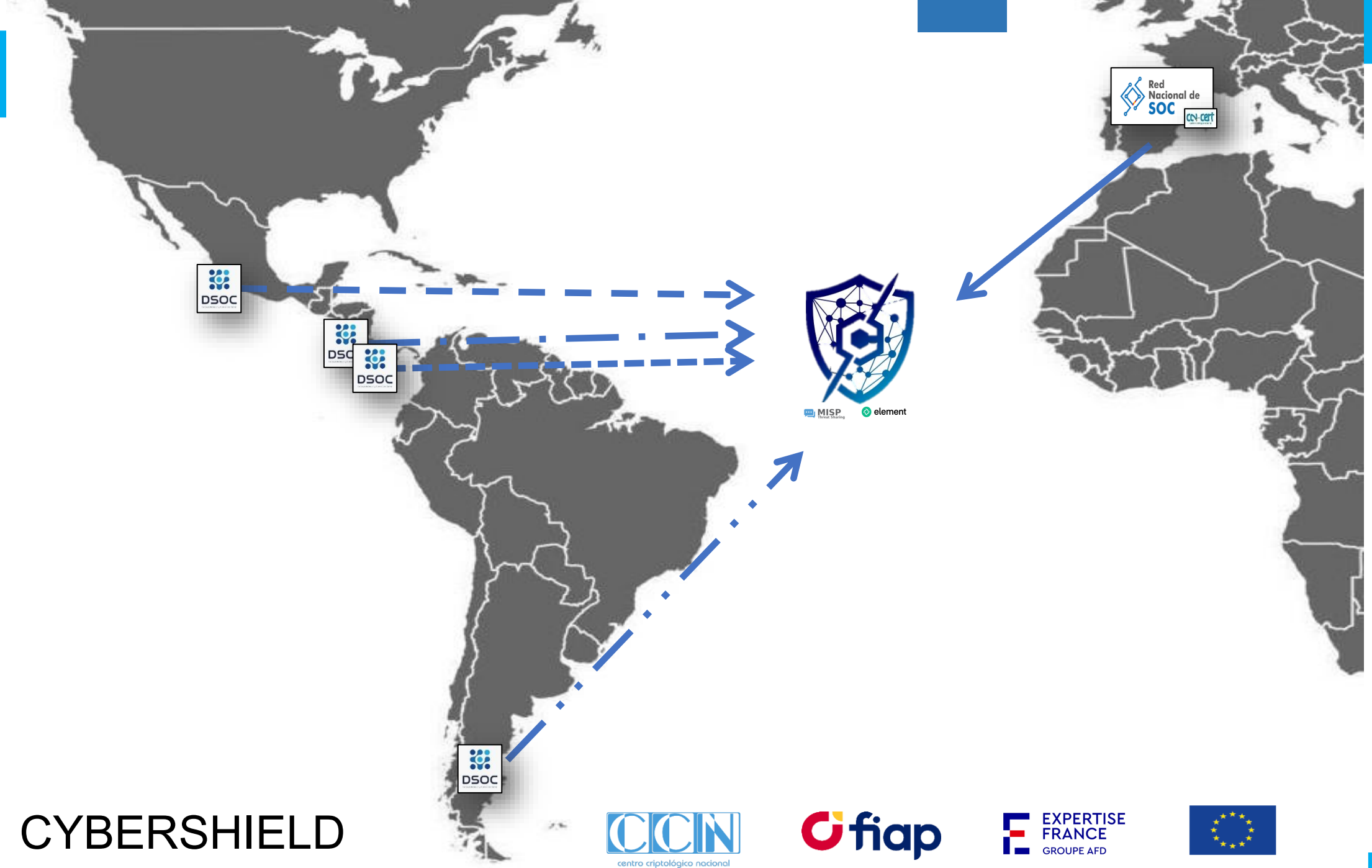




DSOC
Deployable Security Operations Center

centro criptológico nacional

# CIBERESCUDO

CCN
centro criptológico nacional




CYBERSHIELD

CCN centro criptológico nacional

fiap

EXPERTISE FRANCE GROUPE AFD

CCN centro criptológico nacional

# CIBERESCUDO


## 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 »

CCN
centro criptológico nacional

# CIBERESCUDO

Event Actions | Dashboard | Galaxies | Input Filters | Global Actions | Sync Actions | Administration | API | Bookmarks | MISP | Carlo

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

# CIBERESCUDO

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