Estrategia de Ciberseguridad. Red Nacional de SOC

Javier Candau
Jefe Departamento Ciberseguridad
Centro Criptológico Nacional
ccn@cni.es

CCN
centro criptológico nacional

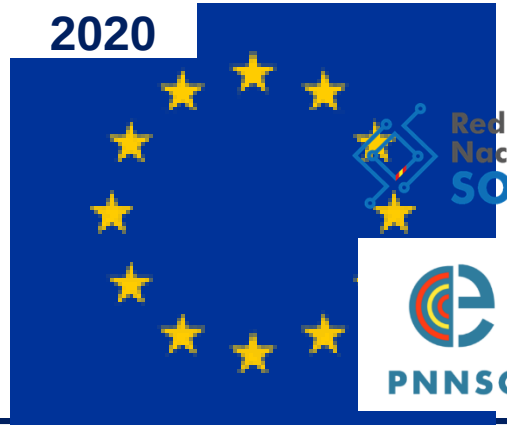
CONCEPTOS

1990
2005

Infosec
Information assurance

- Prohibir
- Inspeccionar
- Autorizar
- Poca seguridad REAL

2005
2020



Ciberseguridad
Ciberdefensa

- Acompañar
- Responsabilidad compartida
- **Auditoria continua**
- Vigilar y responder
- **Notificar ciberincidentes**

2022

TD + Ciberseguridad
Defensa activa
Ciberinteligencia

- Accesos remotos / Uso de la nube
- **Auditoria / vigilancia continua**
- **Respuesta integrada**
- Zero Trust
- Seguridad por defecto (CERTIFICACIÓN)
- **Intercambiar ciberincidentes**

CCN
centro criptológico nacional

APROXIMACIÓN PRÁCTICA
A LA CIBERSEGURIDAD

https://www.ccn.cni.es/index.php/es/menu-ccn-es/aproximacion-espanola-a-la-ciberseguridad

CCN
centro criptológico nacional

Aproximación pragmática… No resignarse

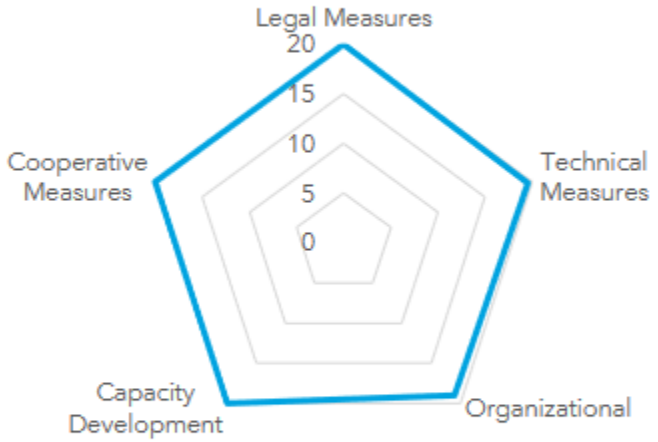
1

1. Estrategia de ciberseguridad.
2. Gobernanza de la ciberseguridad.
3. Desarrollo regulatorio POSIBILISTA
4. CSIRT de referencia, CSIRTs sectoriales y SOC.
5. Capacidad de detección y alerta temprana.
6. Mayor vigilancia a través de SOC.
7. Formación y certificación de personas.
8. Búsqueda de talentos.
9. Asociación público-privada. (**comunidad**)
10. Intercambio de información. (**confianza**)

¿Cómo estamos posicionados en Ciberseguridad?

2020

Spain



Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development, Technical Measures

Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12

CCN
centro criptológico nacional

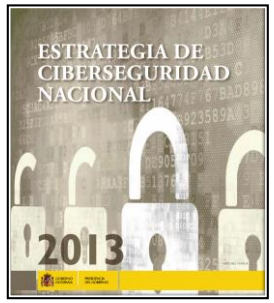
ESTRATEGIA CIBERSEGURIDAD EN ESPAÑA

En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

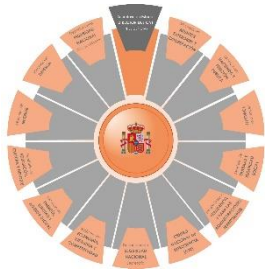
- LA 1 ***Reforzar las capacidades ante las amenazas provenientes del ciberespacio.***
- LA 2 ***Garantizar la seguridad y resiliencia de los activos estratégicos para España.***
- LA 3 ***Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.***
- LA 4 ***Impulsar la ciberseguridad de ciudadanos y empresas***
- LA 5 ***Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.***
- LA 6 ***Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.***
- LA 7 ***Desarrollar una cultura de ciberseguridad.***

CCN
centro criptológico nacional

4 ASPECTOS CLAVES ENCS ESPAÑOLA



02.2014



10.2014

Plan Nacional de Ciberseguridad

07.2015

9 Planes derivados

Plan NACIONAL

COMISIÓN PERMANENTE

CSIRT.es

Entelgy CERT
S2 Grupo CERT
Telefónica CERT
S21Sec CERT
Prosegur CERT
Eulen CERT
ITS-CERT
CyberSOC Deloitte
eSOC INGENIA
..//..

BBVA CERT
Caixabank CERT
MAPFRE-CCG-CERT
..//..

CCN centro criptológico nacional

+1.000 m€

PLAN NACIONAL DE CIBERSEGURIDAD EN ESPAÑA

+150 medidas

Acciones más relevantes:

- La creación de la **plataforma nacional de notificación y seguimiento de ciber incidentes** y de amenazas que permita intercambiar información, en tiempo real, entre organismos públicos y privados.
- Puesta en marcha del **Centro de Operaciones de Ciberseguridad de la Administración General** del Estado y sus Organismos Públicos.
- El desarrollo de un sistema integrado de indicadores de ciberseguridad a nivel nacional.
- Incrementar la creación de **infraestructuras de ciberseguridad en las comunidades y ciudades autónomas** y **las entidades locales**.
- Impulsar la ciberseguridad de pymes, micro pymes y autónomos.
- Promover un mayor nivel de cultura de ciberseguridad.

CCN
centro criptológico nacional

Seguridad, refuerzo de capacidades y resiliencia

¿Qué se recoge en la Estrategia Nacional de Ciberseguridad sobre la seguridad, refuerzo de capacidades y la resiliencia?

[Ob_1] Objetivo 1

Seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales

[LA_1]

Reforzar las capacidades ante las amenazas provenientes del ciberespacio

Medidas de la [LA_1]

1. Ampliar y mejorar las capacidades de detección y análisis de cibereamenazas de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz.
2. **Potenciar la colaboración de los centros de excelencia e investigación** en la lucha contra las ciberamenazas
3. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.
4. **Asegurar la coordinación técnica** y operacional de los organismos con responsabilidades en ciberseguridad, las empresas y la sociedad.
5. Desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional.
6. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.
7. Promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen, acompañadas de requerimientos legales que las regulen.
8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española.
9. **Impulsar el desarrollo de plataformas de notificación**, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial.
10. Desarrollar instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación enfocados a la gestión de crisis para el ámbito de la ciberseguridad en el marco de la Seguridad Nacional.
11. **Garantizar la coordinación, la cooperación y el intercambio** de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales, fomentando la prevención y la alerta temprana.
12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

NECESIDAD:

Consolidar un marco nacional coherente e integrado para garantizar la protección de la información manejada por el sector público y los servicios esenciales

Esta línea de acción responde al Objetivo I de la Estrategia

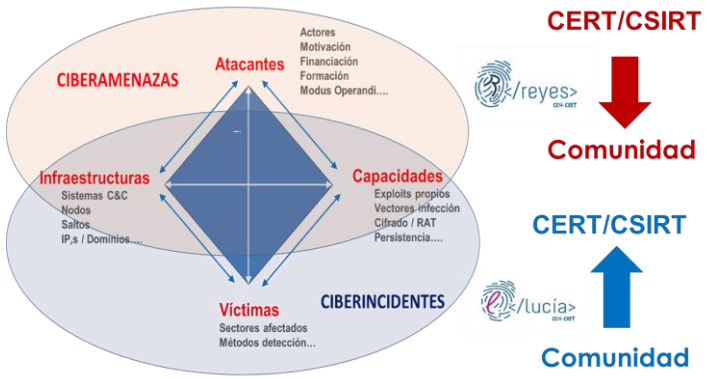
CCN centro criptológico nacional

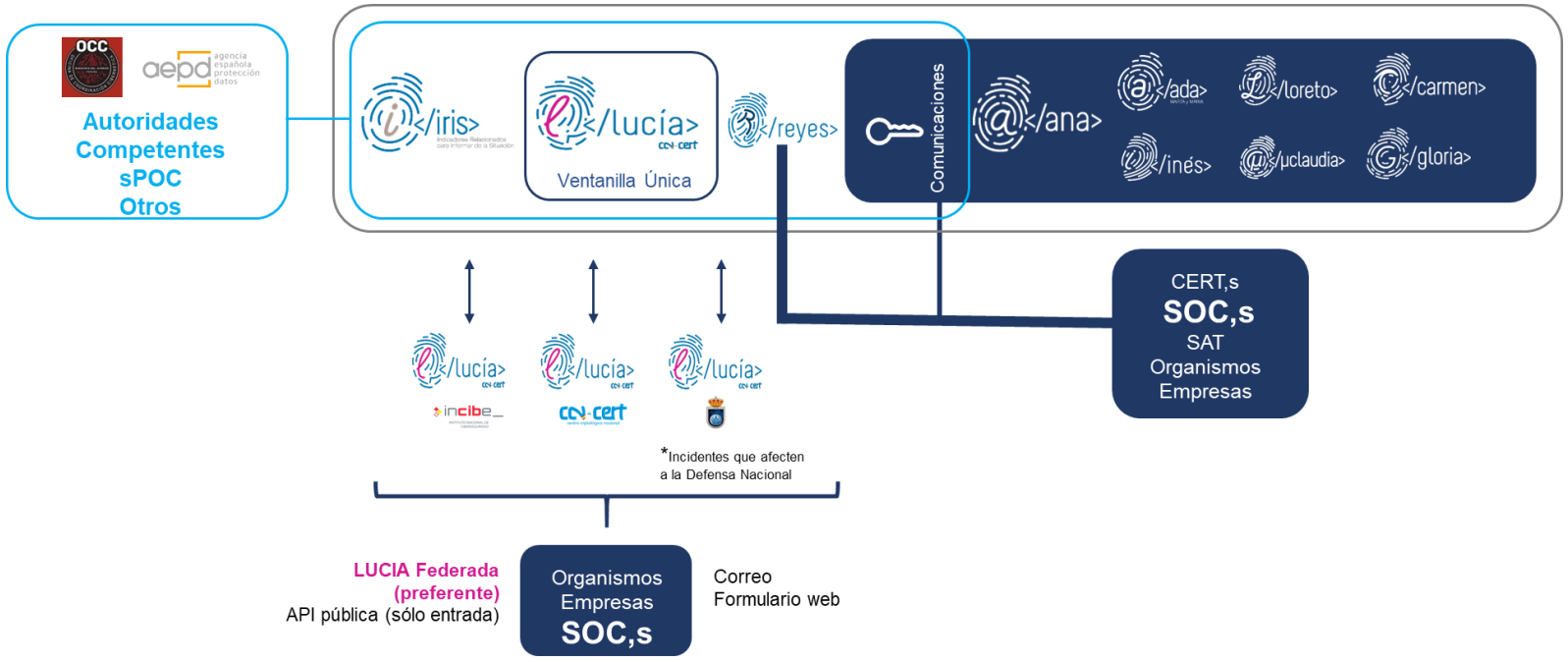
LÍNEA DE ACCIÓN 1

Reforzar las capacidades técnicas ante las amenazas provenientes del ciberespacio.

2-8. Cooperación, coordinación…..Mejores prácticas ….. Respuesta ante incidentes / Red CSIRT

9. Impulsar el **desarrollo de plataformas de notificación**, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial (RD 43/2021. Art 11).





Seguridad, refuerzo de capacidades y resiliencia

¿Qué se recoge en la Estrategia Nacional de Ciberseguridad sobre la seguridad, refuerzo de capacidades y la resiliencia?

[Ob_1] Objetivo 1

Seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales

[LA_2]

Garantizar la seguridad y resiliencia de los activos estratégicos para España

Medidas de la [LA_2]

1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información.
3. Asegurar la plena implantación del ENS, del Sistema de Protección de Infraestructuras Críticas y el cumplimiento y armonización que las soportan.
4. Potenciar la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas y Entidades Locales y en sus organismos vinculados, o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
5. Desarrollar el Centro de Operaciones de Ciberseguridad de la AGE que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de estos centros en el ámbito autonómico y local.
6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las AA.PP., potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.
7. Impulsar el desarrollo de un sistema de métricas de las principales variables de ciberseguridad que permitan a autoridades competentes determinar el nivel de seguridad y su evolución.
8. Comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte la provisión de servicios esenciales.
9. Desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales.
10. Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.
11. Promover la realización de ciberejercicios y evaluaciones de ciberseguridad
12. Asegurar la protección de Infraestructuras Científico-Técnicas Singulares y los centro de referencia del I+D+i

NECESIDAD:

Consolidar un marco nacional coherente e integrado para garantizar la protección de la información manejada por el sector público y los servicios esenciales

Esta línea de acción responde al Objetivo I de la Estrategia

CCN centro criptológico nacional

CSIRT.es (62)

(13)

(6)

GT Seguridad CSAE (+120)

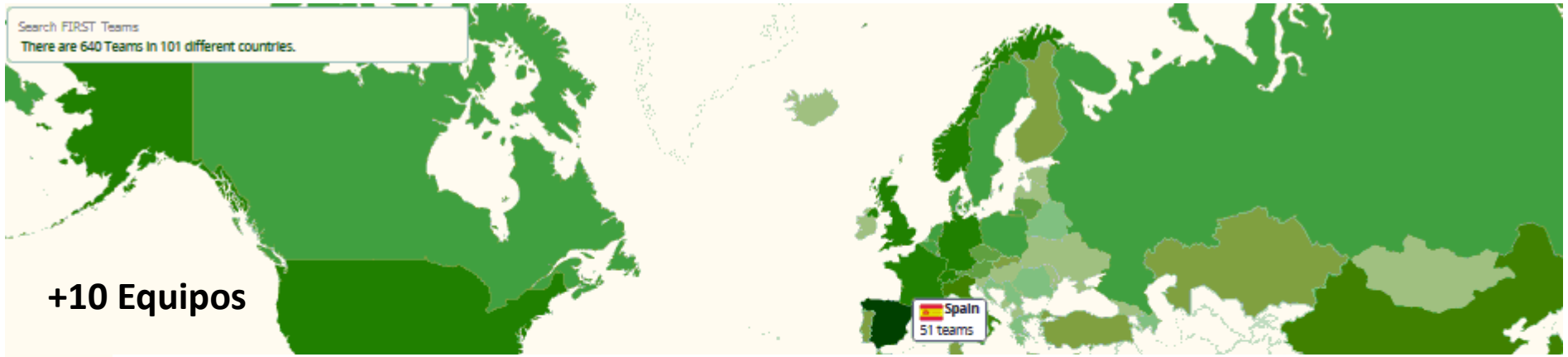
- CCAA
- Universidades (CRUE)
- EELL (FEMP)
- Sector Salud

GT COCS-CDTIC (+60)

- SGAD
- Ministerios
- Agencias

(43)

CCN centro criptológico nacional



+10 Equipos

640 / 51

Equipos en FIRST / España

101

Países

Team	Official Team Name	Country
ACKCERT	Ackcent CERT	ES
BBVA CERT	BBVA CERT	ES
BCSC	Basque CyberSecurity Centre	ES
BE:SEC-CSIRT	BE:SEC-CSIRT	ES
CaixaBank Team CSIRT	CAIXABANK TEAM CSIRT	ES
CATALONIA-CERT	Agència de Ciberseguretat de Catalunya	ES
CCN-CERT	CCN-CERT (Spanish Government National Cryptologic Center - Computer Security Incident Response Team)	ES
CERT OESÍA	CERT OESÍA	ES
CERT-Aiuken	Aiuken Cybersecurity	ES
Cipher CERT	Cipher CERT	ES
CSA-CSIRT	CSA Equipo de Seguridad	ES
CSIRT-BDE	CSIRT Banco de España	ES
CSIRT-CV	Centro de Seguridad TIC de la Comunitat Valenciana	ES
CSIRT-SATEC	CSIRT-SATEC	ES
CSIRTNEXT	CSIRTNEXT	ES
Deloitte ECC	Deloitte ECC	ES
DXC Technology Iberia CSIRT	DXC Technology Iberia CSIRT	ES
Entelgy Innotec CSIRT	Entelgy Innotec CSIRT	ES
ERIS-CERT	Equipo de Respuesta a Incidentes - Sothis	ES
esCERT-UPC	CERT of the Polytechnic University of Catalonia	ES
eSOC Ingenia	eSOC Ingenia	ES

https://csirt.es/
first.org

CCN
centro criptológico nacional

RESPUESTA. CSIRT.ES ->Evolución

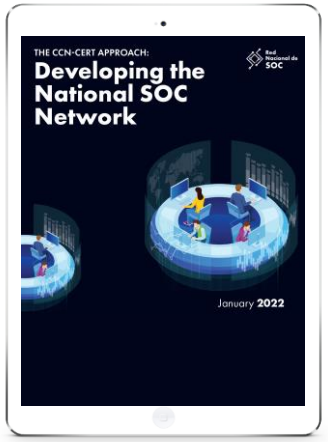
CSIRT.es (62)

(13)

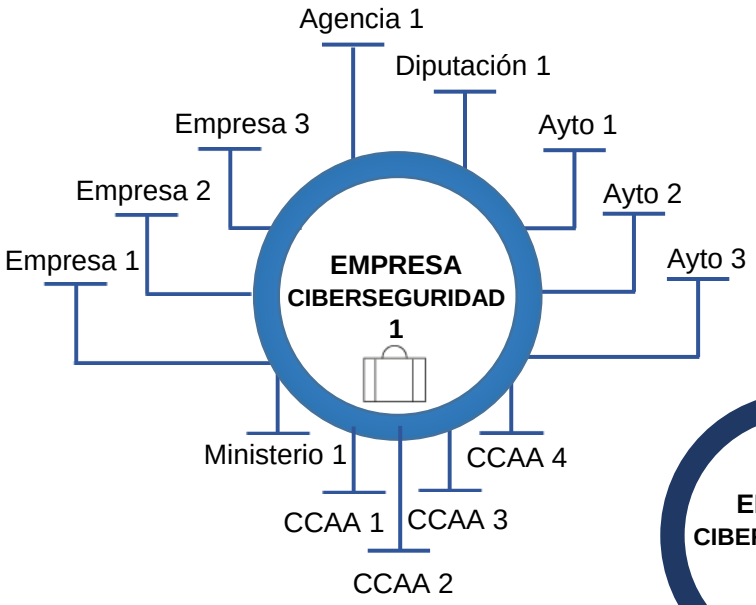
(6)

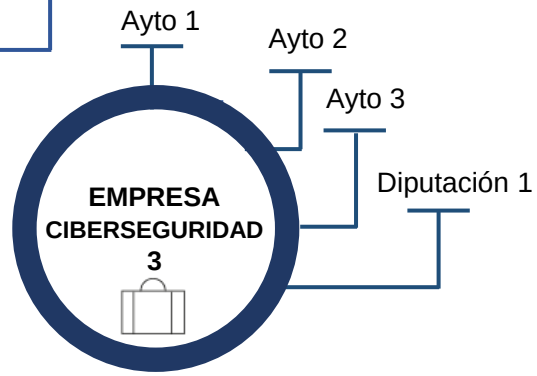
(43)

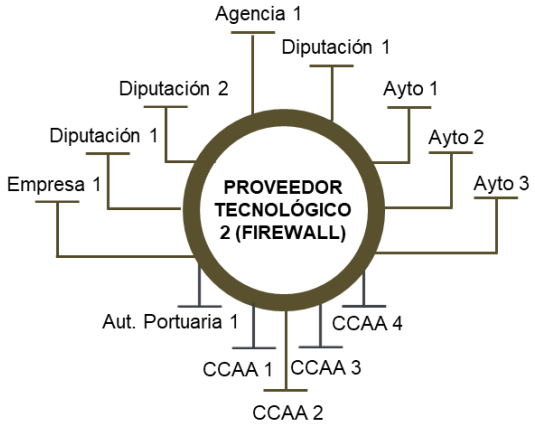
Red Nacional de SOC

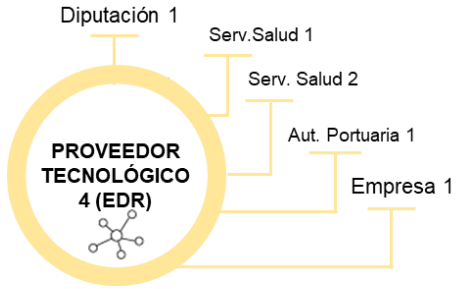


¿Funciona este modelo?









DEFENSORES

- Organizados entorno a empresa de servicios
- Poca ciberseguridad en los procesos TIC. LENTOS
- Nulo o muy escaso Intercambio
- Dependencia sector privado. La ciberseguridad es un servicio más y muchas veces externo

ATACANTES

- Organizados para rentabilizar inversión
- Muy rápidos y ágiles ante vulnerabilidades
- Intercambio de información y herramientas
- Automatizan procedimientos de ataque

Servicios de ciberseguridad

- Personal cualificado
- Mejor tecnología
- Mejores procedimientos
- Mejor Información técnica de la amenaza
- Dependencia

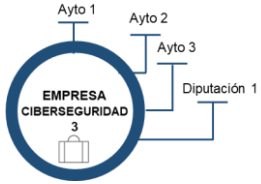
RESPUESTA. Cambio de modelo

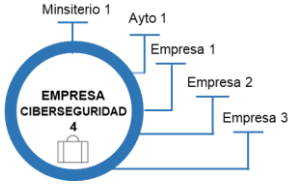
Red Nacional de SOC

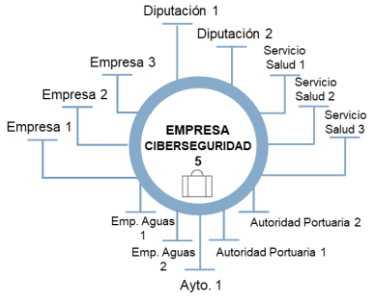
PLATAFORMA NACIONAL

CCN-CERT | SOC MINISTERIAL | SOC CCAA | SOC EELL | SOC SECTORIAL | SOC PRIVADOS

EMPRESAS CIBERSEGURIDAD

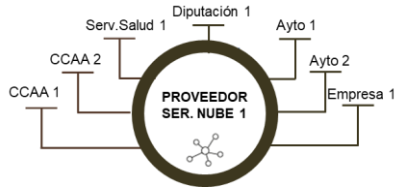


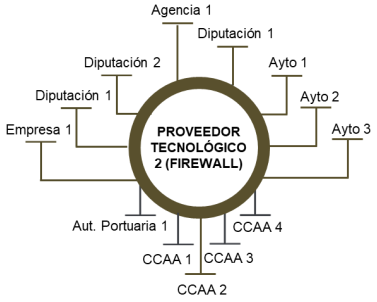


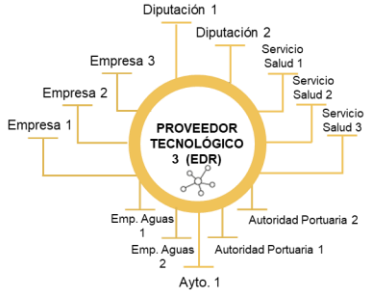


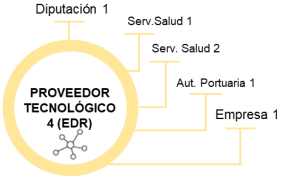
CSIRT.es

PROVEEDORES TECNOLÓGICOS









CCN-STIC 105
Primar intercambio información ciberataques

CCN centro criptológico nacional

Aproximación

Mediante la RNS se pretende **mejorar la seguridad colectiva de TODOS los Organismos Públicos, mediante la superposición de las distintas capacidades.**

Aplicando un **modelo federado**, se coordinarán los flujos de información entre todos los SOC en tres campos:

- ✓ **Notificación de incidentes**. Visibilidad de los incidentes para poder reaccionar a tiempo en el resto de organismos.
- ✓ **Ciberinteligencia**. .
- ✓ **Visibilidad**: Elaborar el mapa de situación de la ciberseguridad a escala nacional.
- ✓ Uso **herramientas comunes y compartidas** + CCN-STIC 105

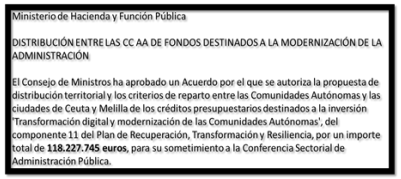
Coordinación con empresas privadas que (generalmente) gestionan la ciberseguridad de los organismos públicos mediante el **intercambio activo de indicadores** de ciberincidente, anonimizando a la víctima y antes de que se pueda extender a otros organismos.

The EU's Cybersecurity Strategy for the Digital Decade
- **RED SUPERSOC,S EN UNIÓN EUROPEA**

Tipos de SOC,s

20% Capacidad SOC

92,7 M€



Ministerio de Hacienda y Función Pública

DISTRIBUCIÓN ENTRE LAS CC AA DE FONDOS DESTINADOS A LA MODERNIZACIÓN DE LA ADMINISTRACIÓN

El Consejo de Ministros ha aprobado un Acuerdo por el que se autoriza la propuesta de distribución territorial y los criterios de reparto entre las Comunidades Autónomas y las ciudades de Ceuta y Melilla de los créditos presupuestarios destinados a la inversión 'Transformación digital y modernización de las Comunidades Autónomas', del componente 11 del Plan de Recuperación, Transformación y Resiliencia, por un importe total de **118.227.745 euros**, para su sometimiento a la Conferencia Sectorial de Administración Pública.

118,2 M€

CCCS Centro de Operaciones de Ciberseguridad

Puertos del Estado

Cabildo de Tenerife

Diputación de Cádiz

Diputación de Córdoba

Diputación de León

AndalucíaCERT Centro de Seguridad TIC

Agència de Ciberseguretat de Catalunya

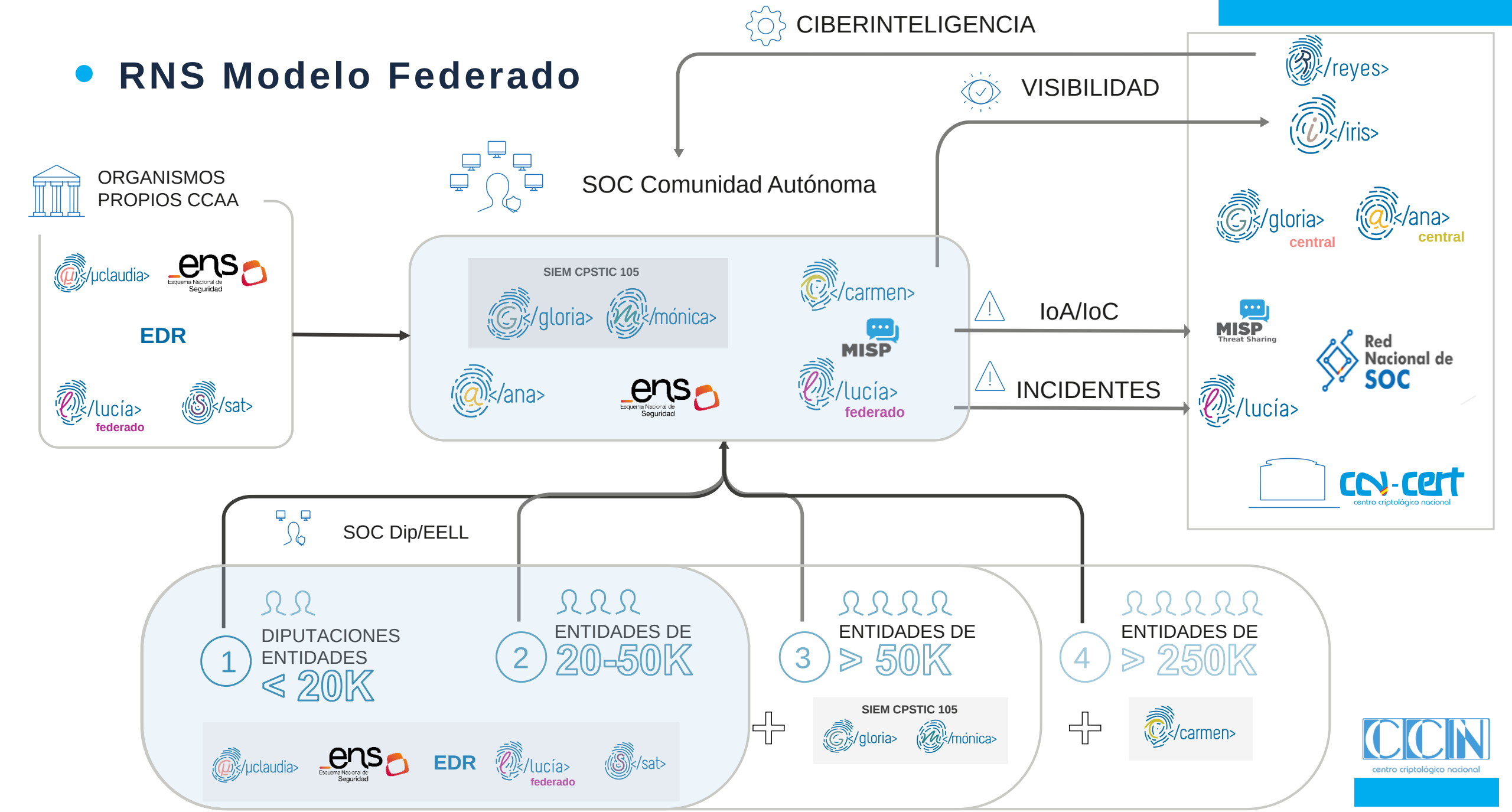
CSIRT-CV Centre Seguretat TIC de la Comunitat Valenciana

CSIRT CARM

CSIRT.gal

CCN centro criptológico nacional

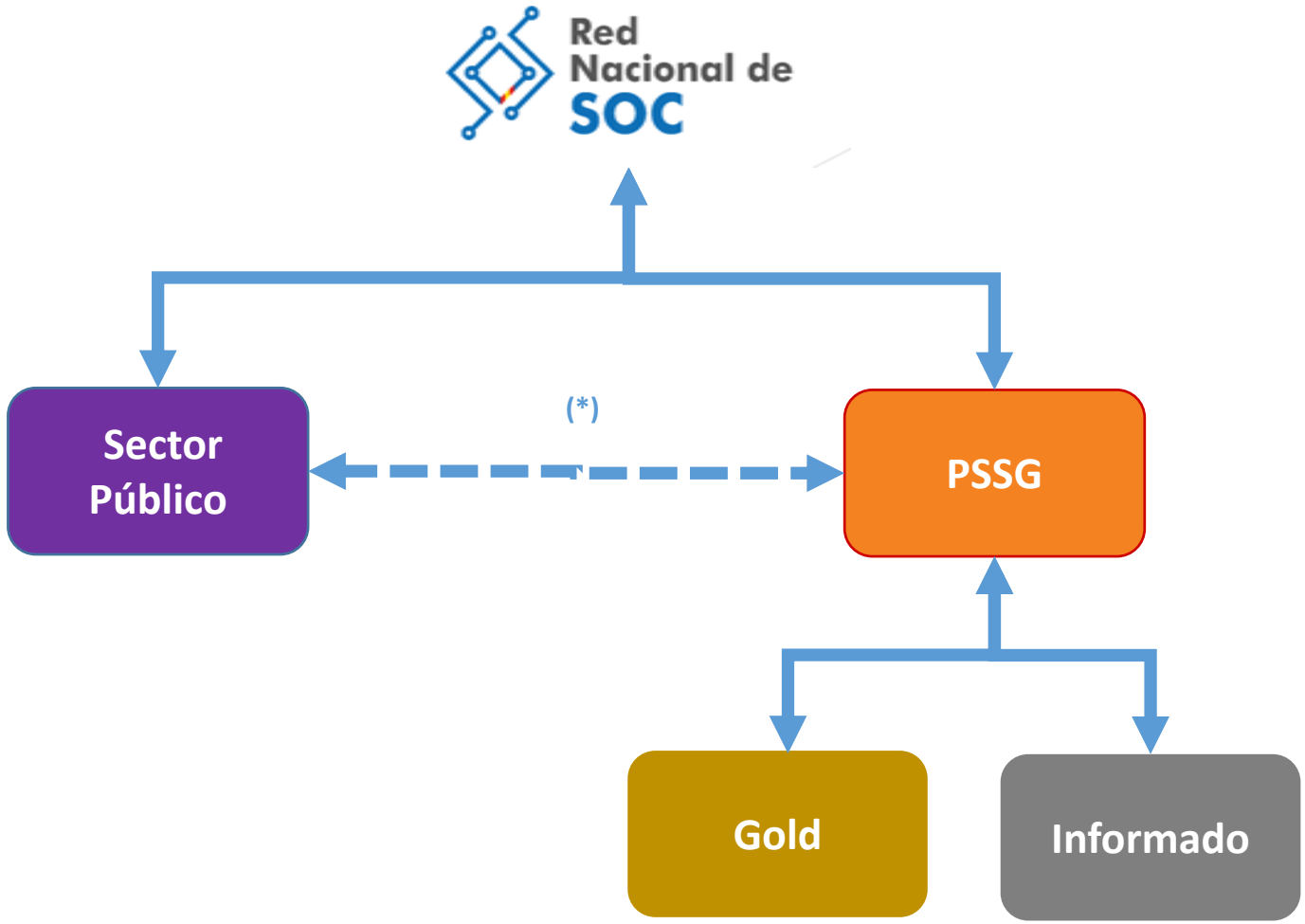
RNS Modelo Federado



RNS Organización

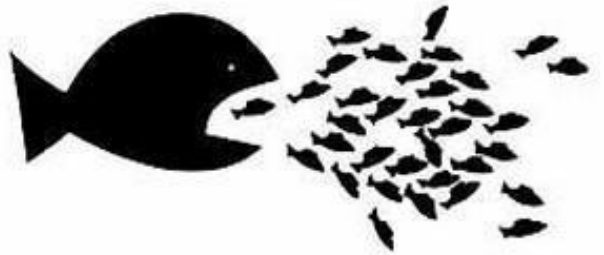
Para organizar la información la RNS tiene 2 categorías de pertenencia:

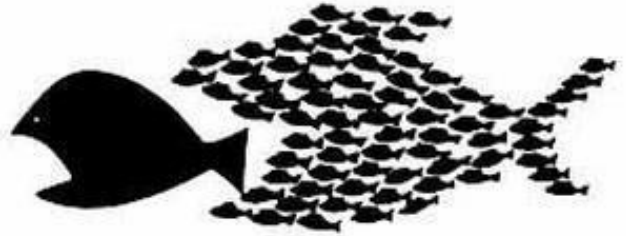
- ***Sector Público***: con todos los SOC de los Organismos Públicos. **Modelo federado**
- ***Proveedores de Servicios de Seguridad Gestionada (PSSG)***: con las empresas que gestionan SOC de un Organismo Público. **Niveles**:
  - ✓ ***Gold***: empresas de alta participación dentro de la RNS
  - ✓ ***Informado*** : empresas con una participación moderada dentro de la RNS



(*): El Organismo público exigirá a la empresa que gestiona su SOC la participación activa en la RNS

CONCLUSIONES





Red Nacional de SOC

PNNSC

CIBERINTELIGENCIA

No hay ciberseguridad sin ciberinteligencia. Necesidad ciberinteligencia utilizable de forma automática.

INTERCAMBIO

Intercambio automático de **ciberincidentes** y ciberamenazas. Plataforma Nacional

RESPUESTA

Impulso a la detección y respuesta de ciberincidentes. **Centros de Operaciones de Ciberseguridad** (SOC / CERT / CSIRT)

INTEGRACIÓN

Integración capacidades nacionales en **PNNSC / RNS**. **Intercambio fluido**

COLABORACIÓN

La colaboración público-privada es FUNDAMENTAL. Pero se tiene que cambiar el modelo. Ciberinteligencia debe ser un servicio horizontal donde todos aporten.

CCN centro criptológico nacional

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es