Financiado por la Unión Europea
NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

Fondos NXG

Prioridades CCN-CERT

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

CCN
centro criptológico nacional

NO HAY TRANSFORMACIÓN DIGITAL SIN CIBERSEGURIDAD

RED CORPORATIVA | NEGOCIO

USO DE LA NUBE

TELEFONÍA MÓVIL

RED INDUSTRIAL

ACCESOS REMOTOS

CCN
centro criptológico nacional

- Ley 11/2002 reguladora **del Centro Nacional de Inteligencia.**
- RD 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.

- RD 311/2022 de 4 de mayo, que regula el **Esquema Nacional de Seguridad** para todo el **Sector Público +** sistemas manejan **información clasificada + Sector privado** (preste servicios S. Público). (Antecedentes: RD 3/2010 y RD 951/2015) (Desarrollo: Art 156.2 de la Ley 40/2015)
- RDL 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información. **Coordinación incidentes.**
- RDL 14/2019, de 31 de octubre, Medidas urgentes. **Coordinación CSIRT públicos y enlace con exterior**
- RD 43/2021, de 28 de enero, Desarrollo RDL 12/2018. **Plataforma Nacional**

MISIÓN

Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

COMUNIDAD

Responsabilidad en ciberataques sobre:

- **sistemas clasificados**,
- sistemas del **Sector Público**,
- empresas y organizaciones de **sectores estratégicos** para el país en coordinación con el CNPIC.

SERVICIOS CCN-CERT

PREVENCIÓN
Reducir la superficie de exposición

- Guías y estándares de seguridad
- Avisos y vulnerabilidades
  - Amenazas | Malware | Mejores prácticas
- Auditorías | Inspecciones
- Formación- ANGELES
- Implantación del ENS

DETECCIÓN
Vigilancia Continua

- Sistemas de Alerta Temprana
- Análisis de Anomalías
- Intercambio de información
  - Ciberincidentes y ciberamenazas
  - Plataforma Nacional

RESPUESTA
Eficiente e integrada

- Despliegue de equipos RRT. Ataques complejos
- Centro de Operaciones de Ciberseguridad
  - Red Nacional de COCS
- Coordinación técnica de CERTs / SOC,s
  - Ataques NO complejos

Legislación 2022 | 2023

ESPAÑA

Esquema Nacional de Seguridad

- Afecta a Información clasificada
- Afecta a empresas privadas
- Esquema de acompañamiento
- Perfiles de cumplimiento
- Necesidad de certificación

UNIÓN EUROPEA

enisa

Cyber Solidarity Act

CCN centro criptológico nacional

NO HAY TD SIN CIBERSEGURIDAD. DESAFIOS SECTOR PÚBLICO

2023

PRINCIPIOS RECTORES

Tecnología certificada

Empleo de tecnologías certificadas y sistemas con conformidad en el ENS. CCN-STIC 105

Auditoría continua

Auditorías periódicas de todo lo que entre en producción. Reducir superficie de exposición

Mínimo privilegio

Aplicación de políticas de seguridad por defecto y **ZERO TRUST**

Vigilancia continua

Vigilancia 24/7 a través de los SOC

Respuesta integrada

Intercambio continuo de incidentes e información sobre ciberamenazas

Ciberdefensa activa

Medidas de defensa activa basadas en capacidades de ciberinteligencia

Impulso al ENS / CPSTIC

Impulso al cumplimiento del ENS

- Perfiles de cumplimiento
- Plataformas que impulsen la certificación
- Plataforma de formación ANGELES

Impulso al empleo del catálogo

- Más familias
- Más productos

¿Perfil o perfiles de cumplimiento ?

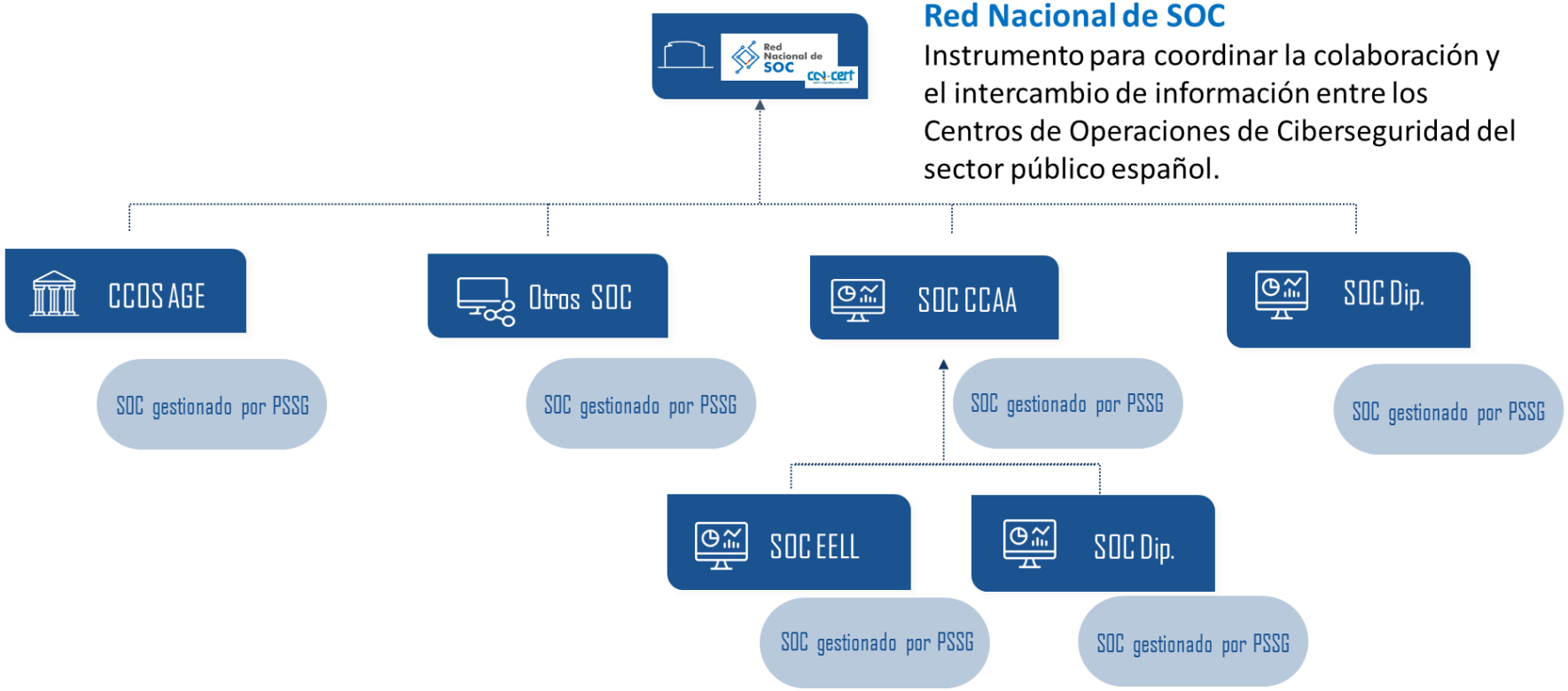
RNS y PNNSC

CCN centro criptológico nacional

Red Nacional de SOC

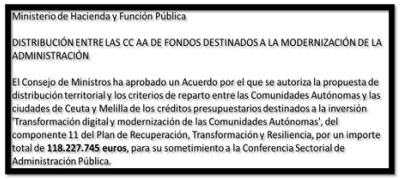
Red Nacional de SOC

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



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€

88 SECTOR PÚBLICO
Organismos y entidades

50 SECTOR PRIVADO
Empresas y proveedores

33

17

CCOS Centro de Operaciones de Ciberseguridad

GOBIERNO DE ESPAÑA · MINISTERIO DE JUSTICIA · SECRETARÍA GENERAL DE LA ADMINISTRACIÓN DE JUSTICIA · SUBDIRECCIÓN GENERAL DE NUEVAS TECNOLOGÍAS DE LA JUSTICIA

CCN centro criptológico nacional

Medidas Defensa ACTIVA

1 

DNS Administración

2 

Identificación y eliminación de servidores de mando y control

3 

Servicio común de detección de ataques basado en anomalías

4 

Superficie de exposición automática
Auditorias automatizadas servicios expuestos

5 

Servicio detección avanzada en móviles

6 

Ciberinteligencia

OTRAS MEDIDAS DE DEFENSA DE APLICACIÓN

PNNSC

PNNSC Plataforma Nacional

Salidas agregadas a Internet, consolidación CPDs

RNS. Integración capacidades

Servicios comunes de alojamiento web o correo electrónico

- Sistemas detección comunes
- Servicios antiransomware

CCN
centro criptológico nacional

1

DNS Administración

DNS ADMINISTRACIÓN – PROYECTO ALBA

Primera capa de protección ante amenazas con especial incidencia y/o foco en España

BLOQUEO DE DOMINIOS

- Distribución de exploits, malware (APTs, ransomware, spyware, cryptojacking , etc).
- Infraestructura usada por malware (command and control, covert channel, etc).
- Phishing, estafas y otras actividades fraudulentas.

DETECCIÓN TEMPRANA Y RÁPIDA RESPUESTA

- Listado de dominios dañinos por parte del CCN y otros organismos colaboradores
- Monitorización y análisis en tiempo real del tráfico generado, con modelos específicos para detectar casos de phishing y estafas con objetivos nacionales
- Canal de soporte para organismos y entidades colaboradoras

SÉCTOR PÚBLICO

Detecta equipos infectados en las infraestructuras del sector público

2

Identificación y eliminación de servidores de mando y control

IDENTIFICACIÓN DE SERVIDORES DE MANDO Y CONTROL

Capacidad de **identificación proactiva de servidores de mando y control desplegados en Internet** (ataque, explotación, cibercrimen…)

IA SOBRE EL CONJUNTO DE DATOS DEL CCN-CERT

DETECCIÓN

- Campañas de suplantación (actores de alta sofisticación)
- Anomalías léxicas para la detección de dominios potencialmente dañinos
- Anomalías de comportamiento basados en líneas base de tráfico
- Anomalías de comportamiento basados en líneas base de registros

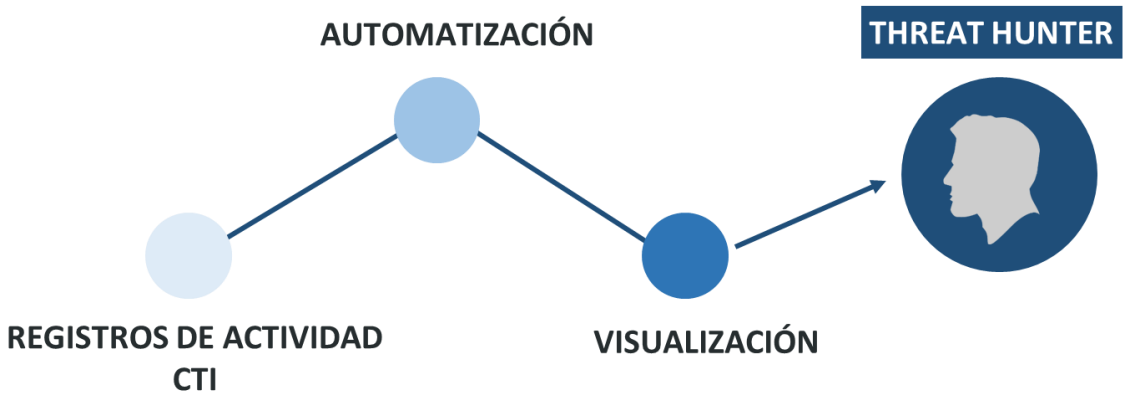
3

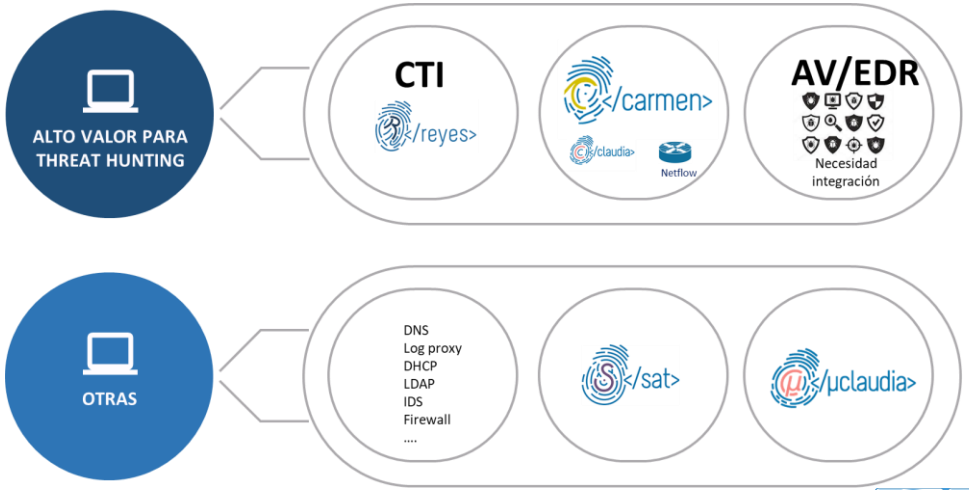
Servicio común de detección de ataques basado en anomalías

THREAT-HUNTING

Un adversario suficientemente avanzado conseguirá evadir los dispositivos y el software de seguridad y monitorización desplegado en nuestra red

Por ello, la búsqueda activa de amenazas en la red es imprescindible para anticiparnos a nuestro adversario





CCN
centro criptológico nacional

4

Superficie de exposición automática
Auditorias automatizadas servicios expuestos

Superficie Exposición. Gestión Vulnerabilidades

+150 ORGANISMOS

ANA CENTRAL
DICIEMBRE 2023

NATIONAL VULNERABILITY DATABASE
NVD
By NIST

ana@ccn-cert.cni.es

REYES. Ciberinteligencia adaptada

ACTIVOS MONITORIZADOS

+ 7,2K
IPs monitorizadas

+ 74K
Dominios monitorizados

ORGANISMOS DADOS DE ALTA

+ 290
Organismos en REYES

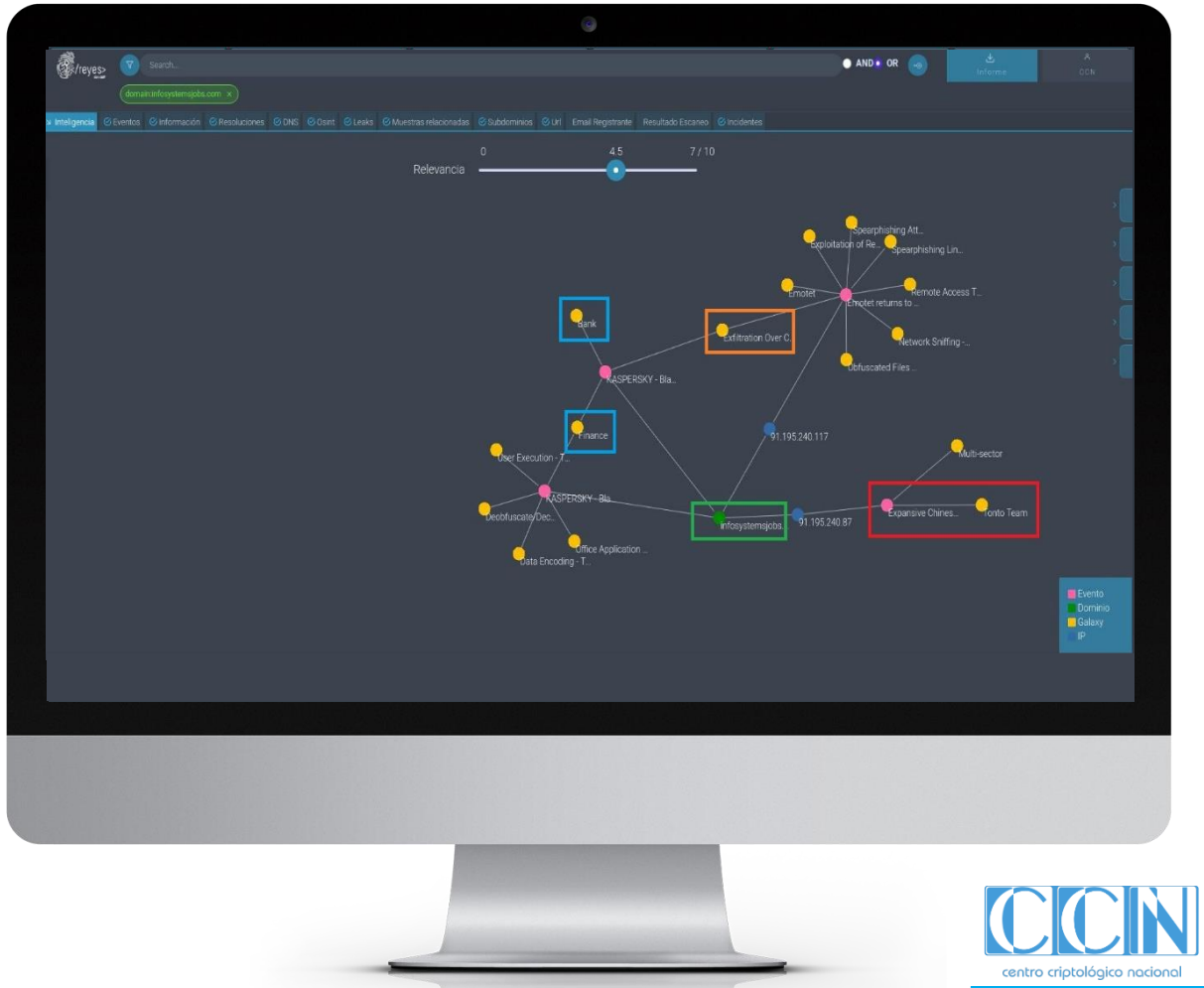
+ 130

INFORMACIÓN UTILIZABLE

Superficie de exposición

+ 70
Listas Negras

+ 2,8M
IOCs en listas negras



reyes@ccn-cert.cni.es

CONCLUSIONES

1. Tenemos que dotarnos de capacidades con los Fondos NXG

2. Prioridades:
   - Implantar ENS / CPSTIC
   - PNNSC y RNS
   - Medidas ciberdefensa activa

3. Potenciar intercambio en integración de capacidades

4. Necesidad de servicios horizontales de ciberseguridad

Muchas

Gracias

E-mails

ccn@cni.es

jdciber@ccn.cni.es

oferta.empleo@cni.es

organismo.certificacion@cni.es

cpstic.ccn@cni.es

info@ccn-cert.cni.es

sat@ccn-cert.cni.es

ens@ccn-cert.cni.es