00. CCN / CCN-CERT

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

centro criptológico nacional

SIN CLASIFICAR

1 Legislación relevante

RD 3/2010

RD 951/2015

8 Instrucciones Técnicas de Seguridad

LEY 8/2011
RD 721/2011

2016/1148
Directiva NIS
RDL 12/2018

RD 421/2004

Ley 18/2011
EJIS

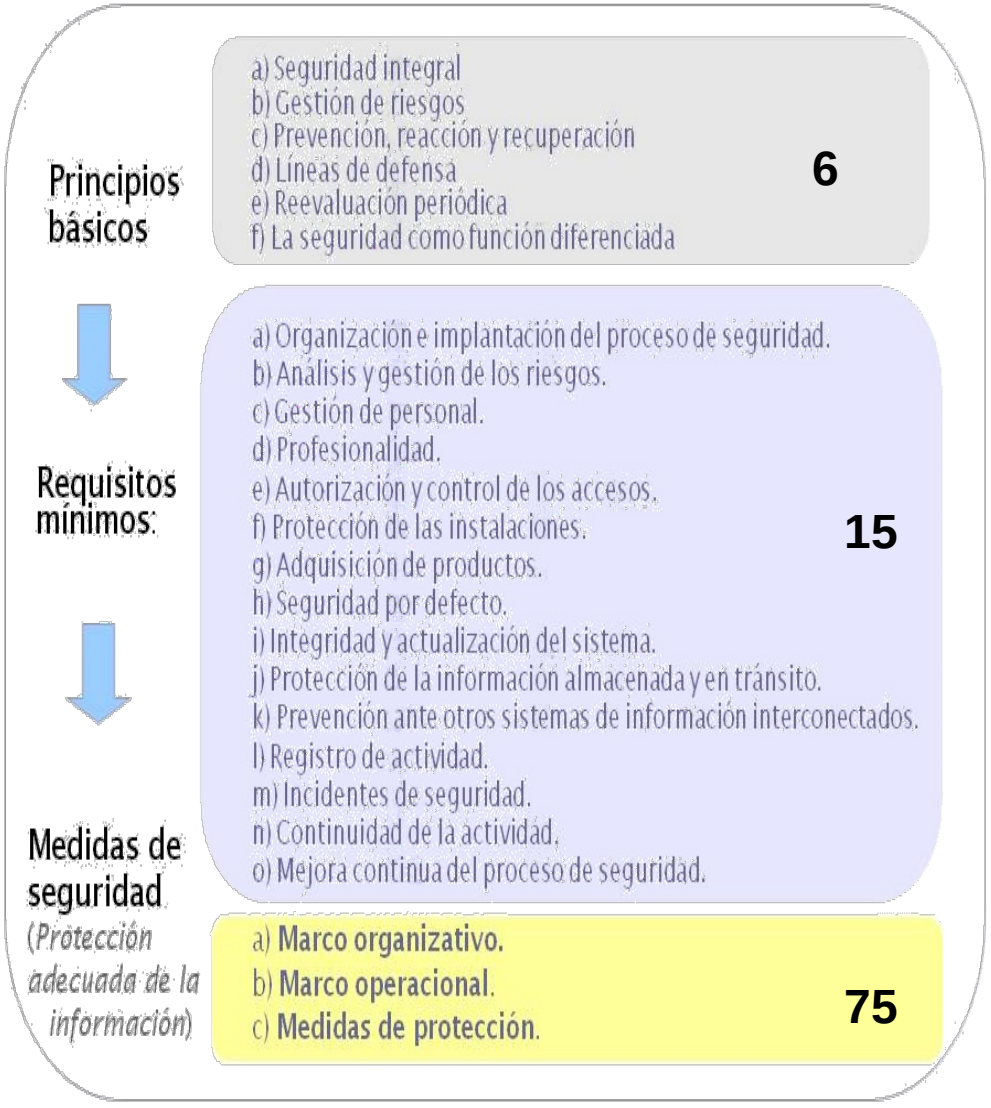
Ley 39/2015
Ley 40/2015
PAC y RJSP

LO 15/1999
RD 1720/2007

Ley 11/2007
Acceso Electronico

2016/679
GDPR
LO 3/2018

2000 2004 2008 2012 2016 2018



1. Los **Principios básicos,** que sirven de guía.
2. Los **Requisitos mínimos,** de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS.
5. La **respuesta a incidentes de seguridad**. Papel del CCN- CERT.
6. El uso de **productos certificados**. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.

2016/679
GDPR
LO 3/2018

2016/1148
Directiva NIS
RDL 12/2018

RESPONSABILIDAD PROACTIVA Y DEMOSTRABLE (Accountability principle)

Tipos de medidas:

- ✓ **Análisis de riesgo.**
- ✓ Registro de actividades de tratamiento.
- ✓ Medidas de protección de datos desde el diseño y por defecto.
- ✓ **Medidas de seguridad.**
- ✓ **Notificación de quiebras de seguridad.**
- ✓ **Evaluaciones de impacto sobre la protección de datos.**
- ✓ **Delegado de protección de datos (DPD).**
- ✓ La adhesión por parte de responsables y encargados de tratamiento a códigos de conducta.
- ✓ La creación de **mecanismos de certificación** y de sellos y marcas de protección de datos.

Energético
electricidad, gas, petróleo

Hídrico

Sanidad

Transportes
aéreo, ferrocarril, marítimo, carretera

Banca y mercados Financiero

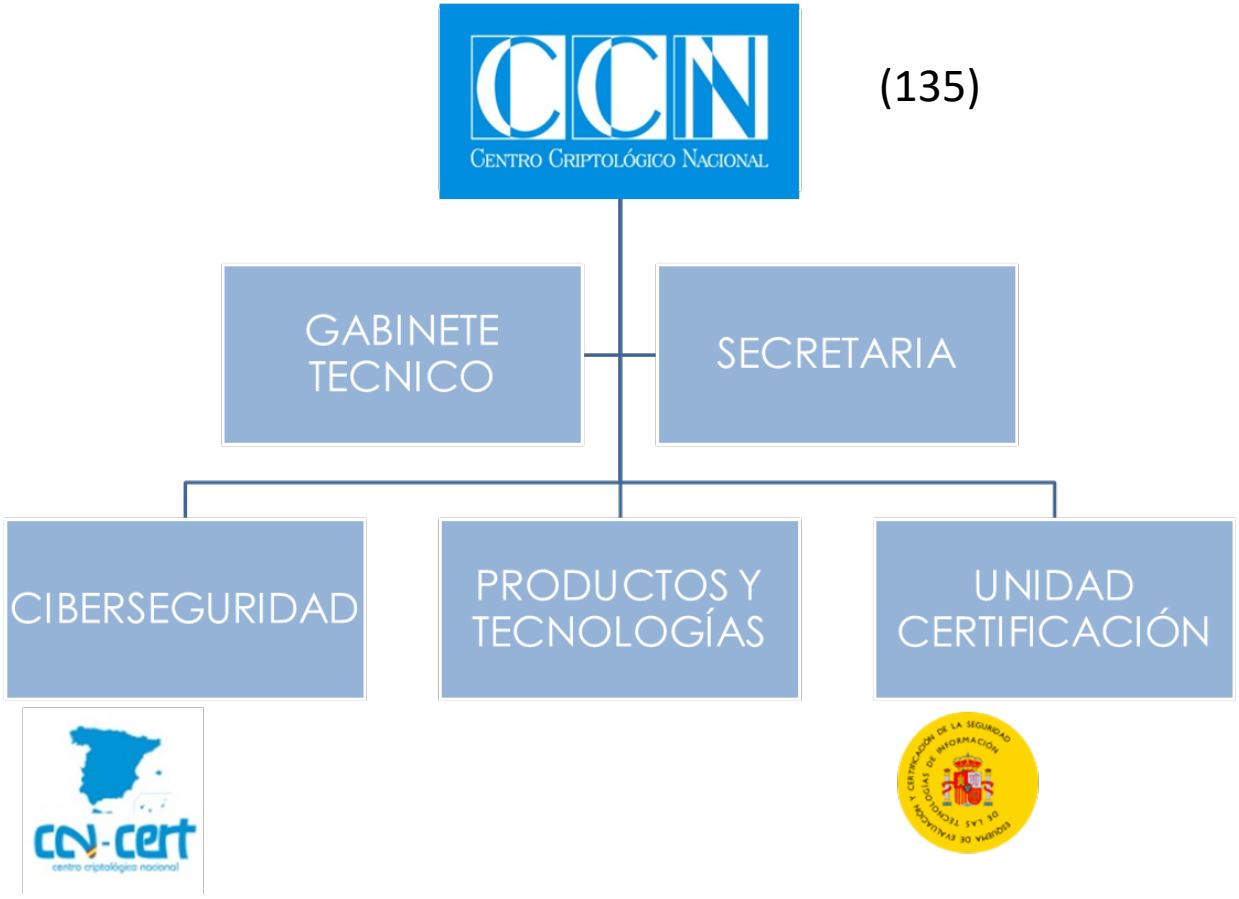
TIC (Infraestructuras y serv. Digitales)

Industria Nuclear
Administración
Espacio
Alimentación
Industria Química
Inst. Investigación

Infraestructuras Críticas
Servicios esenciales

CCN
centro criptológico nacional

ESTRUCTURA CCN



2 CCN-CERT

- Ley 11/2002 reguladora **del Centro Nacional de Inteligencia.**
- Real Decreto 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.
- Real Decreto 3/2010, 8 de Enero, que define el **Esquema Nacional de Seguridad** para la Administración Electrónica, modificado por el **RD 951/2015, de 23 de octubre.** Ampliación del ámbito de actuación con Ley 39/2015 Procedimiento Administrativo común de las AAPP y Ley **40/2015** Régimen Jurídico del Sector Público
- RDL 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. Coordinación incidentes

Establece al CCN-CERT como CERT Gubernamental/Nacional competente

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.

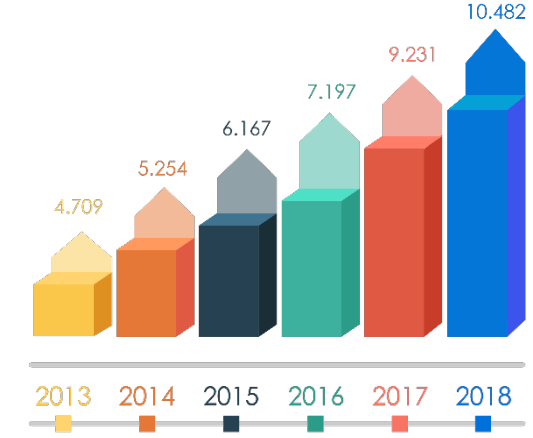
COMUNIDAD

Responsabilidad en ciberataques sobre:

- **Sistemas clasificados**
- **Sistemas del Sector Público**
- Empresas y organizaciones de **sectores estratégicos (en coordinación con CNPIC).**

2 SERVICIOS CCN-CERT

1. Proporcionar guías y estándares de seguridad
   - **Configuración segura de los sistemas**
2. Avisos y vulnerabilidades
   - **Amenazas / Malware / Mejores prácticas**
3. **Formación**
4. Respuesta rápida ante ciberataques
5. Intercambio de información
   - **Incidentes**
   - **Ciberamenazas**
6. Auditorias / Inspecciones
7. **CENTRO OPERACIONES DE SEGURIDAD AGE**



Número de usuarios registrados, por año

Proveer servicios / dar soluciones

AUDITORÍA

- inés
- pilar
- clara
- rocio
- claudia
- ana

DETECCIÓN

- sat-inet
- sat-sara
- sat-ics
- carmen

ANÁLISIS

- gloria
- maría
- marta
- reyes

INTERCAMBIO

- lucía
- loreto

FORMACIÓN

- vanesa
- ATENEA

SOC AGE
SOC SGNTJ

SOC VIRTUAL

CCN
centro criptológico nacional

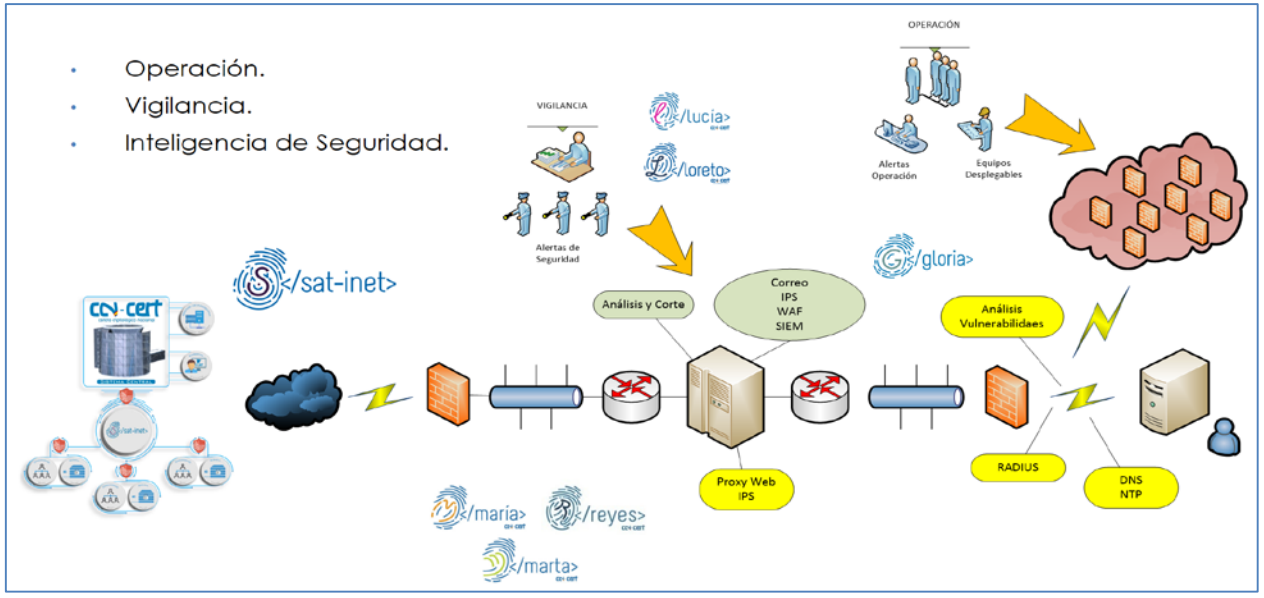
SOC AGE / SOC VIRTUALES

SOC SGNTJ. Convenio entre SGNTJ y CCN.

SOC AGE. Acuerdo de Consejo de Ministros 15.02.2019.

Iniciativa SOC VIRTUALES

SOC AGE
SOC SGNTJ



Centro de Operaciones de Seguridad de la AGE

Prevención

- Gestión de elementos de seguridad perimetral (FW, IPS, IDS, F5, …)
- Cortafuegos de aplicaciones Web (WAF) /Anti-DoS Capa 7
- Análisis de tráfico cifrado con SSL/TLS
- Gestión de elementos de seguridad internos (FW, IPS/IDS,…)
- Navegación segura (Proxy)
- Correo seguro/Sandbox
- DNS Pasivo
- Revisión automática de vulnerabilidades
- Prevención de fuga de datos (DLP)
- Seguridad de end-point /Bastionado/GPO
- Acceso remoto (VPN)
- Antivirus

Operación

- Vigilancia digital
- Monitorización y correlación de eventos (GLORIA/CARMEN)
- Monitorización de eventos internos
- Auditorías Técnicas
- Pruebas de caja blanca (Análisis de código fuente)
- Pruebas de caja negra (Pentest)

Actuación

- Gestión de incidentes de seguridad
- Investigación de ciberamenazas/Análisis forense y respuesta a incidentes
- Gestión de vulnerabilidades
- Gestión de alertas (SAT)
- Gestión de alertas anti-DOS
- Análisis de código dañino (MARTA/MARÍA)

Formación

- Formación en seguridad
- Concienciación en seguridad

Mejora

- Asesoramiento en ciberseguridad

SOC

Centro de Operaciones de Ciberseguridad

CCN
centro criptológico nacional

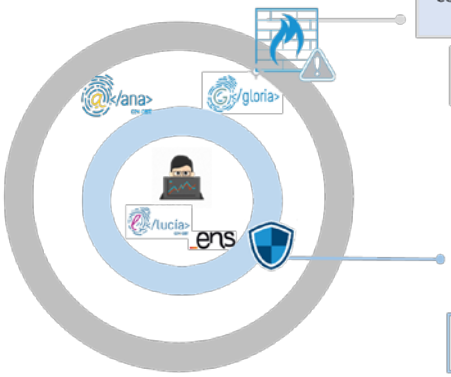
Situación de los 10k-20k

EJEA DE LOS CABALLEROS (ZGZ)	ALCAÑIZ (TER)	UTEBO (ZGZ)	JACA (HU)	CUARTE DE HUERVA (ZGZ)
16.5 k	16.0 k	18.4 k	12.9 k >55.0 k	12.5 k
110	120	155	170	60
1	1	1	1+3	1

Situación de los 10k-20k

Respuesta en EELL / Pymes

- Actuaciones / inspecciones técnicas.
- Evaluación y conocimiento del estado de seguridad.
- Valoración de la exposición.



Seguridad perimetral con administración centralizada y capacidad de detección de anomalías (sondas)

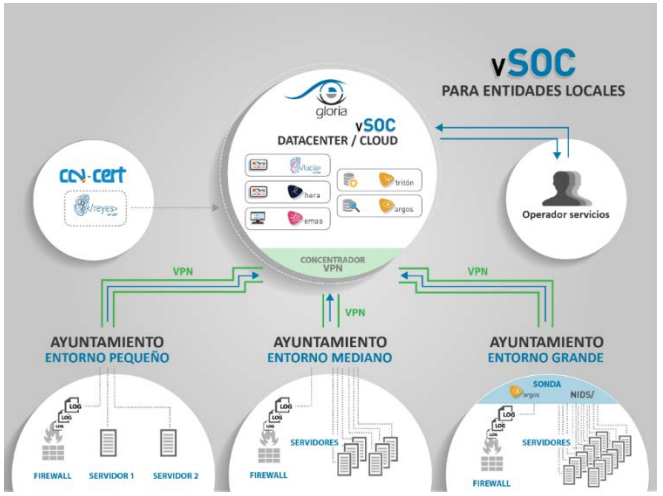
Evaluación Continua (ANA)

Gestión Eventos Seguridad Compartir Reglas

Notificación / Federación (LUCIA)

Seguridad Punto Final (Endpoint)

Capacidad forense, remediación remota y reglas de comportamiento



vSOC Inicial

- Notificación de incidentes.
- Avisos y alertas.

vSOC

- Actuación sobre el perímetro ante incidentes.
- Capacidad forense e investigación remota.
- Control de equipos infectados.

vSOC Avanzado

- Actuaciones / inspecciones técnicas.
- Evaluación y conocimiento del estado de seguridad.
- Valoración de la exposición.

Piloto a implantar:

- **Diputación de Zaragoza**
- **Diputación de Valencia**
- **Diputación de León**
- Región de Murcia
- Cabildo Insular Tenerife
- Diputación de Burgos

CCN
centro criptológico nacional

Cambio de paradigma

Hacia el paradigma de la respuesta

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

sondas@ccn-cert.cni.es

redsara@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es