

JORNADA STIC

CAPÍTULO COLOMBIA

CCN-CERT. Gobernanza de la Ciberseguridad en España



En colaboración con:





Javier Candau

Jefe del Departamento de Ciberseguridad

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

2020
2030



TD + Ciberseguridad
Defensa activa
Ciberinteligencia



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

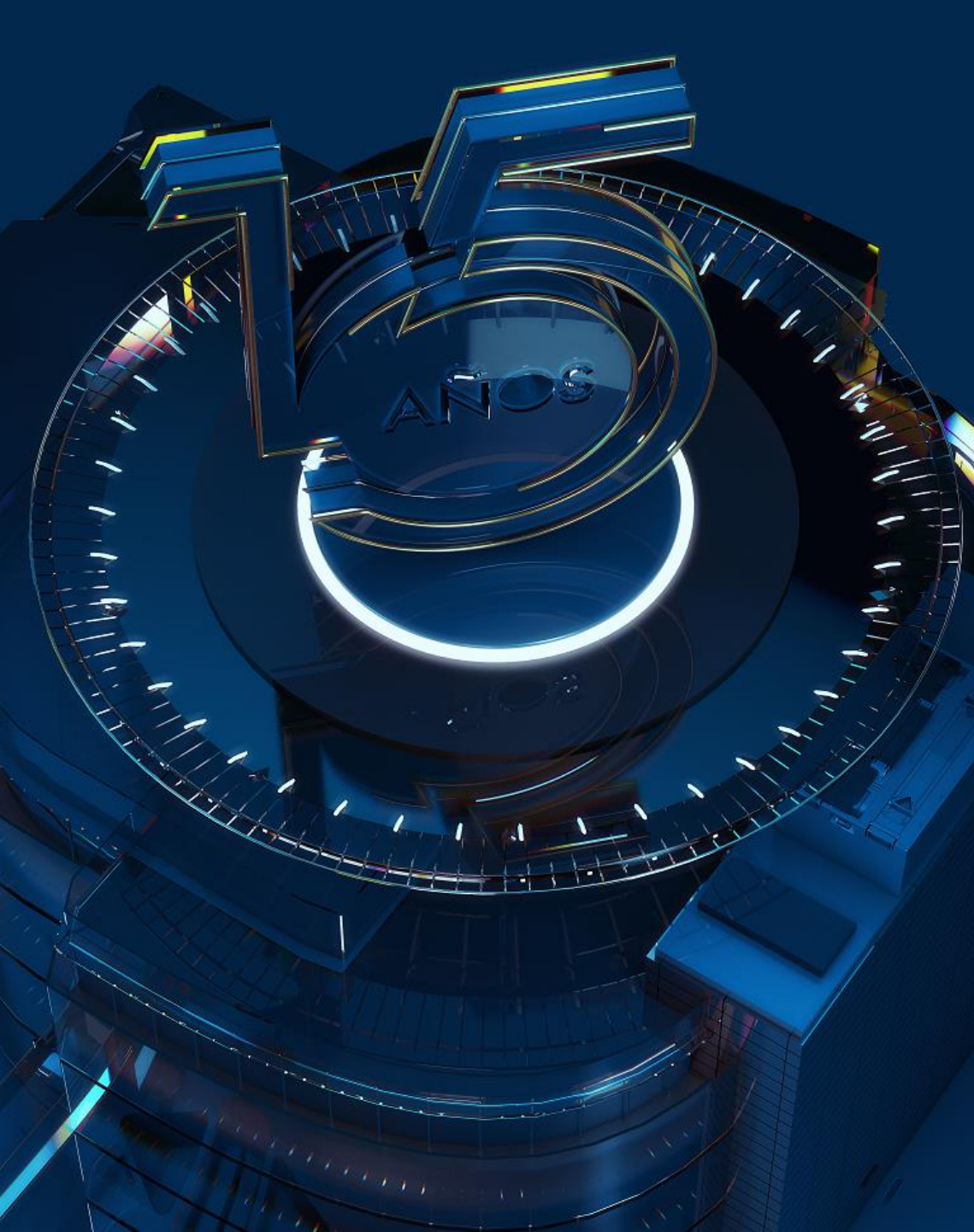
SOBRE NOSOTROS



- 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 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, en respuesta a la evolución del entorno regulatorio, las tecnologías de la información y experiencia de implantación.
- 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

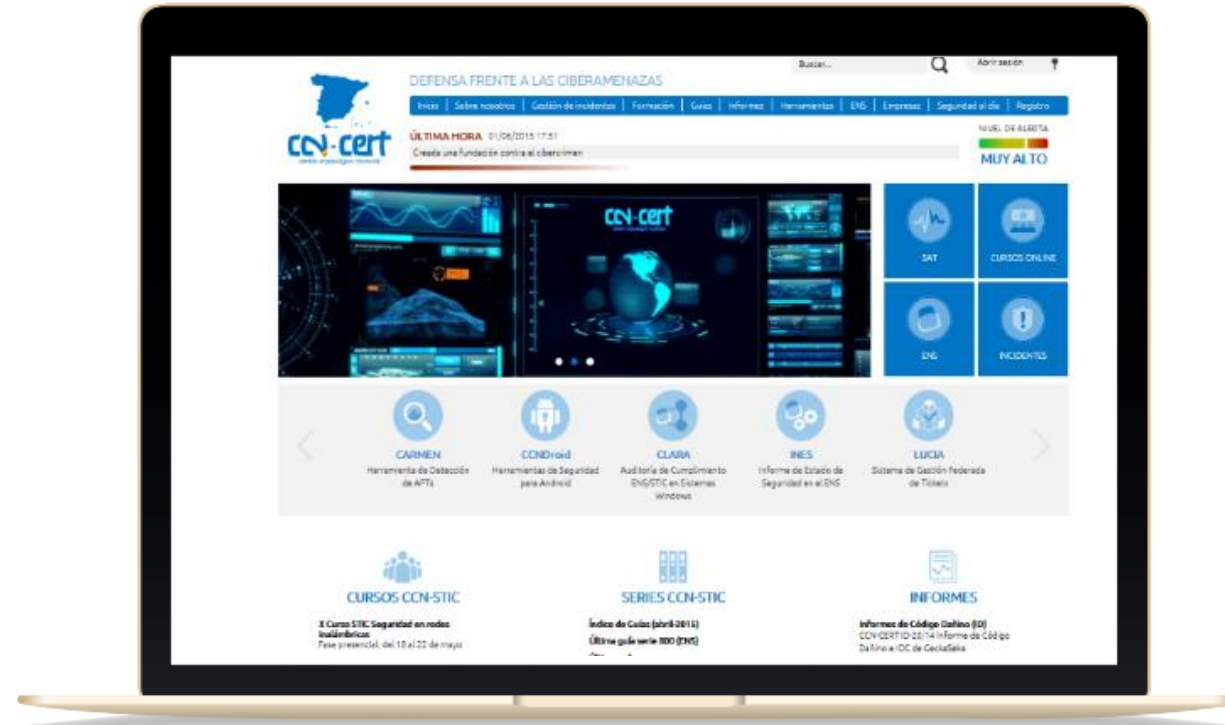
Contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al Sector Público a afrontar de forma activa las nuevas ciberamenazas.

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



www.ccn-cert.cni.es

PREVENCIÓN

Reducir la superficie de exposición



DETECCIÓN

Vigilancia Continua



RESPUESTA

Eficiente e integrada



- ✓ Proporcionar guías y estándares de seguridad
 - ✓ Avisos y vulnerabilidades
 - Amenazas | Malware | Mejores prácticas
 - ✓ Auditorías | Inspecciones
 - ✓ Formación

 - ✓ Detección y Respuesta ante ciberataques
 - ✓ Intercambio de información
 - ciberincidentes y ciberamenazas
 - **Plataforma Nacional**

 - ✓ Centro de Operaciones de Ciberseguridad
Red Nacional de COCS
 - ✓ Coordinación técnica de CERTs
-

MARCO NORMATIVO



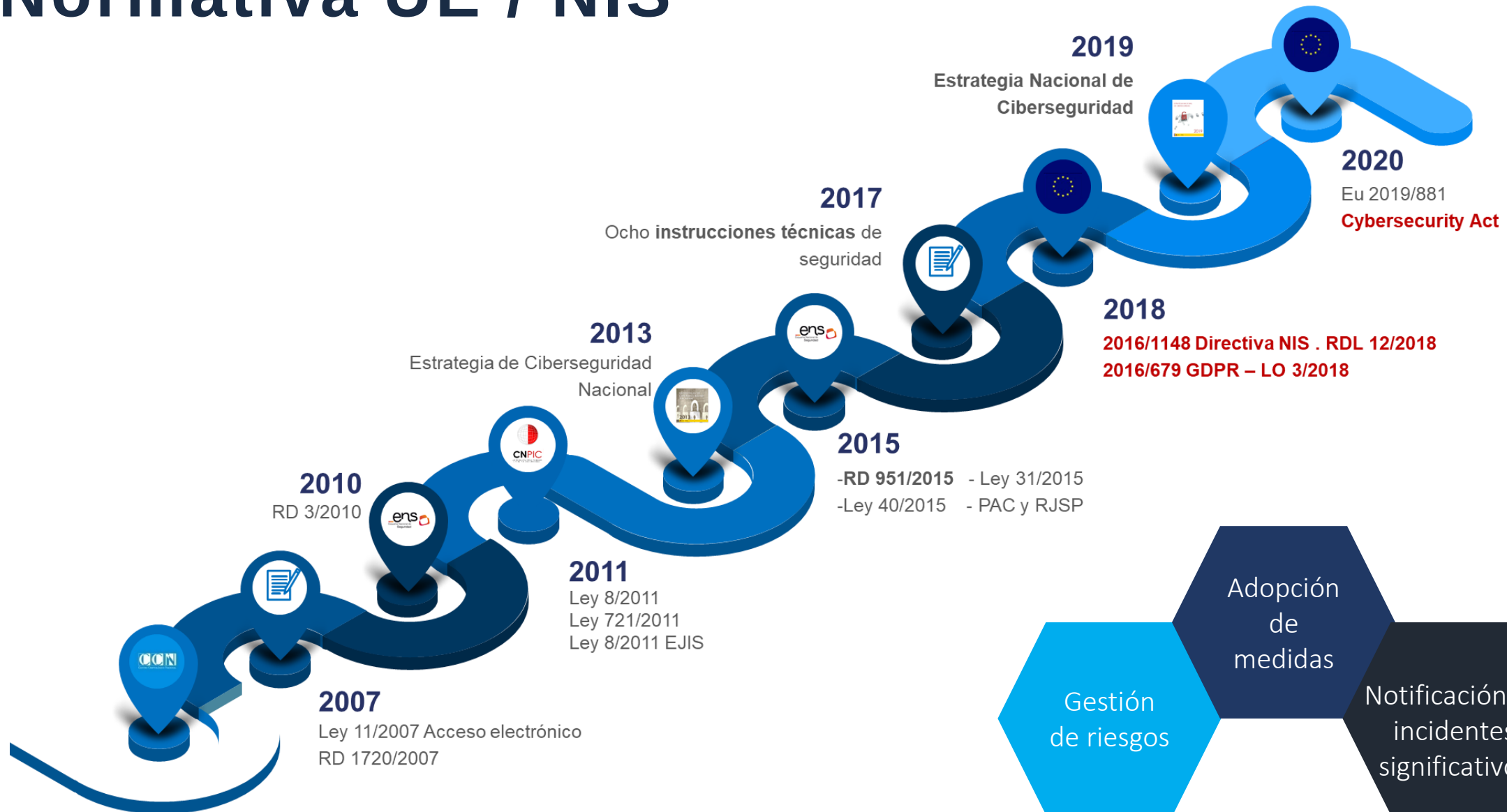
Normativa de la UE

2016/1148 Directiva NIS – RDL 12/2018

Evolución de la ciberseguridad

Gobernanza en España

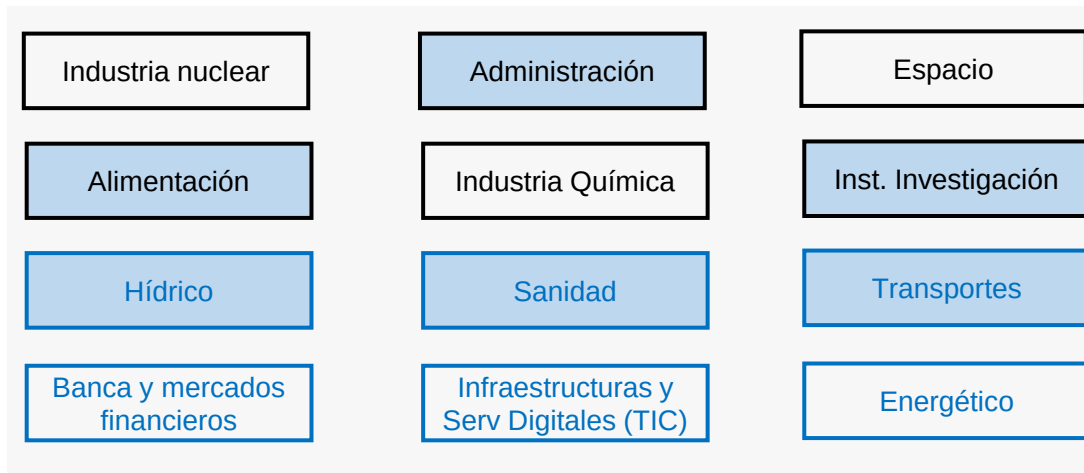
Normativa UE / NIS



2016/1148 Directiva NIS

RDL 12/2018 // RD 43/2021

Ley 11/2011 // RD 721/2011

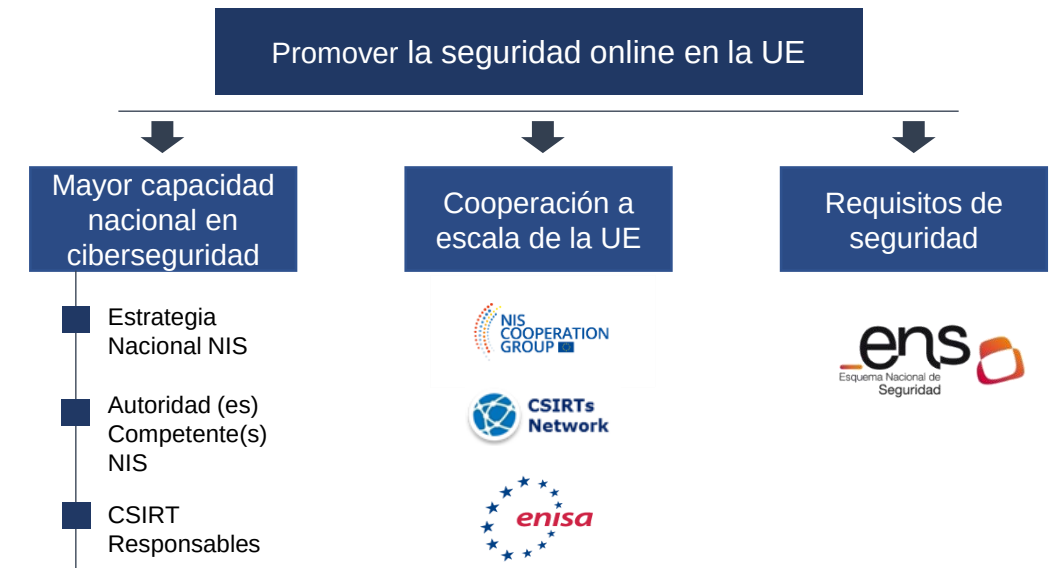


Infraestructuras críticas

Servicios esenciales

Mayoría operadores Públicos

NIS 1.0



Lecciones aprendidas NIS 1.0



[LA#1]

Criterios diferentes de Designación OSE. Mucha diferencia entre estados

[LA#2]

No hay conjunto de medidas de seguridad

[LA#3]

No se notifican vulnerabilidades

[LA#4]

Diferencias en notificación de incidentes. No hay criterios transfronterizos

[LA#5]

Informe de estado de seguridad en la UE.
Similar a informe INES

Esquema Nacional de **Ciber**Seguridad



La formación y concienciación

La respuesta a incidentes de seguridad. Papel del CCN- CERT Notificación

La Categorización de los sistemas para la adopción de medidas de seguridad proporcionadas.

Los 6 Principios básicos, que sirven de guía

Serie 800 Guías CCN-STIC (57 documentos)

El uso de productos certificados. Papel del Organismo de Certificación (CCN).

La auditoría de la seguridad que verifique el cumplimiento del ENS. Sellos de conformidad.

Los 15 Requisitos mínimos, de obligado cumplimiento.

Evolución Ciberseguridad



Ámbitos de competencia

Operadores y proveedores de servicios digitales

Sector público



Ciudadanos y empresas



Seguridad y defensa

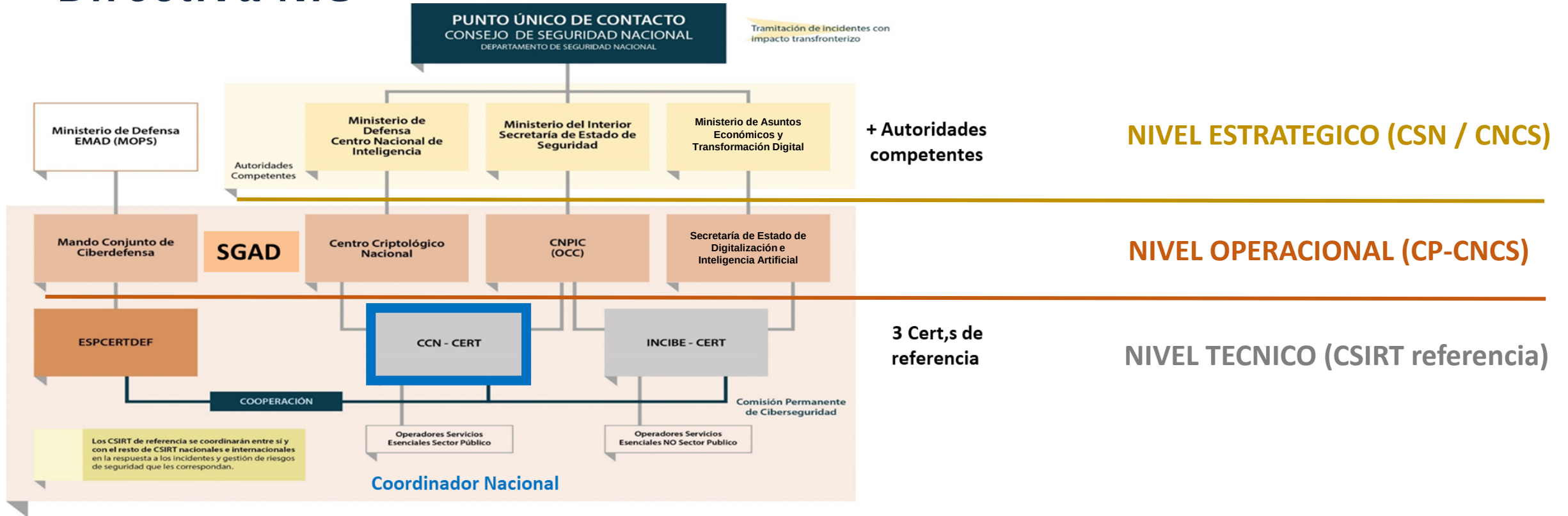


Infraestructuras críticas y sectores estratégicos



Gobernanza en España

Directiva NIS



Directiva NIS / RDL 12/2018 / RD 43/2021

INTERCAMBIO DE INCIDENTES

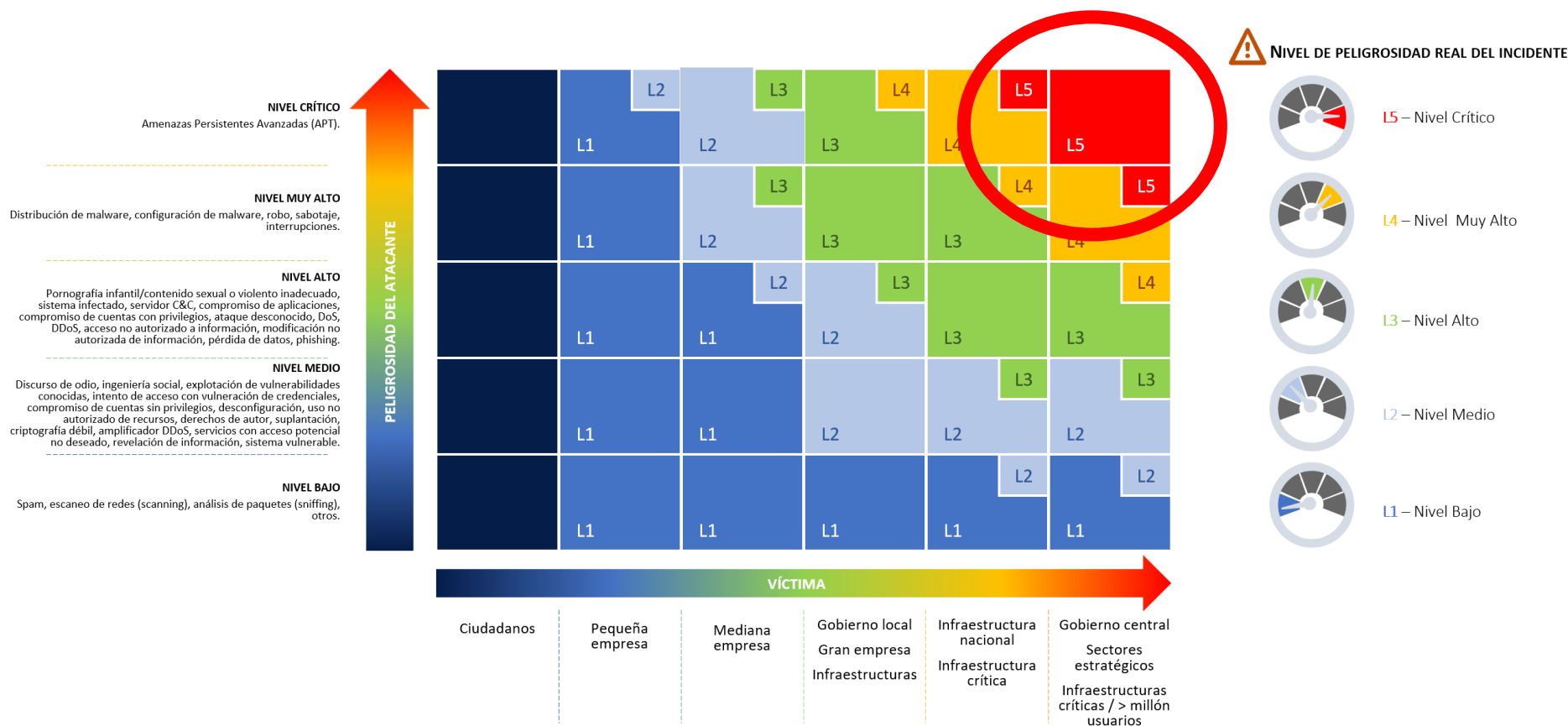


- Matriz de ciberincidentes

- Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes

- Red Nacional de Centros de Operaciones de Ciberseguridad

Intercambio Incidentes



Guía de Seguridad de las TIC
CCN-STIC 817

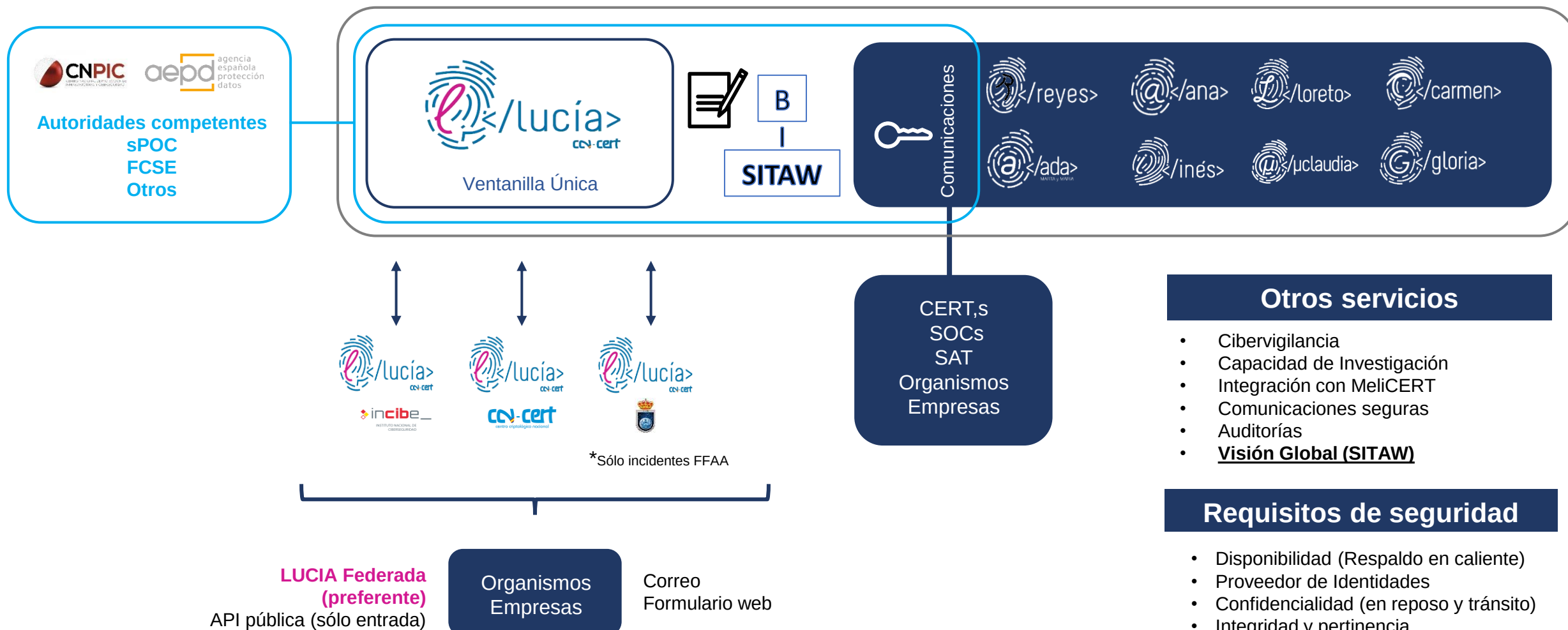
ESQUEMA NACIONAL DE SEGURIDAD
GESTIÓN DE CIBERINCIDENTES



Supuesto especial gravedad = Incidentes MUY ALTO o CRITICO

Taxonomía (ENISA) | Nivel de Peligrosidad | Nivel de impacto | Campos a notificar | Ventana temporal de reporte

Plataforma Nacional



Impulso a la Red Nacional de SOC's





CONCLUSIONES

España tiene, en los campos de gestión de riesgos, medidas de seguridad y notificación de incidentes, actividades más avanzadas que muchos países de la UE.

Conclusiones

#1

IMPULSO DE TD

Necesidad de fondos e impulso político para la ciberseguridad

FUNCIÓN DIFERENCIADA

#3

NECESIDAD

ser objetivos difíciles de atacar. Cumplimiento del ENS. Métricas

#2

PLATAFORMA NACIONAL

Intercambio de ciberincidentes e inteligencia de ciberamenazas.

Necesidad de un organismo que proporcione inteligencia utilizable en tiempo real

#4

DETECCIÓN Y RESPUESTA

Impulso a los Centros de Operaciones de Ciberseguridad (COCS y vSOC)

SOLUCIONES CCN-CERT



Auditoría



EMMA-VAR



Detección



Sonda
distribuida

Soluciones
basadas en IA



Análisis



Vigilancia



ALICIA

Soluciones
basadas en IA



Intercambio



Formación



ángeles
Formación y Talento en Ciberseguridad



JORNADA STIC

CAPÍTULO COLOMBIA

GRACIAS



En colaboración con:

