CCN centro criptológico nacional 15 años

ccn-cert
centro criptológico nacional

Legislation & Incident reporting

CCN
centro criptológico nacional

Cybersecurity Index 2018

rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
9	Canada	0.892	0.195	0.189	0.200	0.172	0.137
10	Australia	0.890	0.200	0.174	0.200	0.176	0.139

CCN
centro criptológico nacional

Prevención en seguridad

165 auditorías de seguridad y páginas web

ens

873	11	94	28
organismos	entidades de certificación	empresas certificadas	sector público certificado

Guías y estándares de seguridad propios

335 Guías CCN-STIC actualizadas permanentemente

consultadas **+300.000** veces

1.025 Informes de Seguridad (Amenazas, Código Dañino, Técnicos y Buenas Prácticas)

Formación

7.324	224	8	18
alumnos presenciales	cursos presenciales	cursos online	cursos a distancia (VANESA)

Talento Atenea

+70	+60	+5.000
retos de seguridad avanzados	retos de seguridad básicos (Atenea Escuela)	usuarios

Respuesta a ciberincidentes

SOC Justicia 27 Analistas / Operadores

SOC AGE

SOC Virtuales 6 Diputaciones / CC.AA.

Detección de ciberataques

139.742 Ciberincidentes gestionados (Sector Público y sectores estratégicos)

2.5 Incidentes diarios, críticos o muy altos (APT, DDoS, Código dañino específico)

8.100 Troyanos anuales

2.500.000 Eventos de seguridad recibidos diariamente

+300 Avisos y Alertas

20.580 Vulnerabilidades

Sistemas de Alerta Temprana

Sector Público y empresas de interés estratégico

206	50	9
Organismos y empresas adscritos	Áreas de conexión	Organismos

19 Herramientas propias: detección, análisis, auditoría e intercambio de información

CCN centro criptológico nacional

15 años

2004-2019

Quince años fortaleciendo la ciberseguridad nacional

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

Promoción de productos y tecnologías seguras. Evaluación y Certificación

220	93	202
Productos Certificados Common Criteria	Productos aprobados para manejar información clasificada	Productos cualificados

Reconocimiento internacional de España como "Crypto Producing Nation"

1.845 certificaciones Zoning de Instalaciones y Equipos

Punto de referencia en ciberseguridad

20	+65
Grupos de trabajo (UE, OTAN, Galileo, Satélites, Programas, Inteligencia, Empresas, etc.)	Acuerdos internacionales

Cooperación diaria en la gestión de incidentes

Cultura de Ciberseguridad

2.464	66	+1.000	10.482
Asistentes Jornadas CCN-CERT	Jornadas de sensibilización	Participación en mesas redondas/jornadas	Usuarios registrados portal CCN-CERT

23.840 Solicitudes de registro portal CCN-CERT

11.774 Seguidores
10.264 Seguidores
96.204 Reproducciones

352.440 Promedio visitas mensuales portal CCN-CERT

CCN centro criptológico nacional

- **Agenda**

1. CCN / CCN-CERT Services
2. National Legislation / EU Legislation
3. Cyber incident notification

CCN
centro criptológico nacional

CCN Legal support

- Law 11/2002 regulating the **National Intelligence Centre**.
- Royal Decree 421/2004, March 12, which regulates and defines the scope and functions of the **CCN**.
- Royal Decree 3/2010, January 8, which defines the **National Security Framework** for Electronic Administration, modified by RD 951/2015, of October 23, in response to the evolution of the regulatory environment, information technologies and implementation experience.
- RDL 12/2018 NIS DIRECTIVE Transposition. (09.2018). Defining CERT community. **Technical coordination role** in CCN-CERT.

Establish CCN-CERT as competent Governmental / National CERT

MISSION

To contribute to the improvement of **Spanish cybersecurity**, being the national alert and response centre that cooperates and helps to respond quickly and efficiently to the **Public Sector** to actively address the new cyber threats.

CONSTITUENCY

In charge of cyber attacks on **classified systems**, **Public Sector** systems and companies and organizations of **strategic sectors** for the country **in coordination with the CNPIC**.

CCN-CERT Services

Minimize the exposure surface

01 To provide security guides and standards
- Secure system configuration

02 Warnings and vulnerabilities
- Threats / Malware / Better practices

03 Security Audits and inspections

04 Training

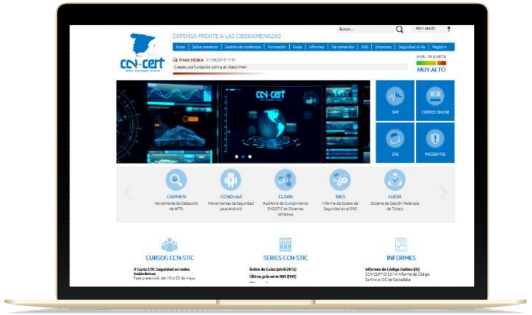
Continuous surveillance

05 Cyber Incident Response

06 Information sharing
- Incidents and cyber threats

Efficient response

07 Security Operation Centre



www.ccn-cert.cni.es

CCN
centro criptológico nacional

01 Security Guides and Standards

Reports published in 2019

26
Malware Reports

41 /365
New and updated guides

6
Good Practices Reports

81
Technical Reports

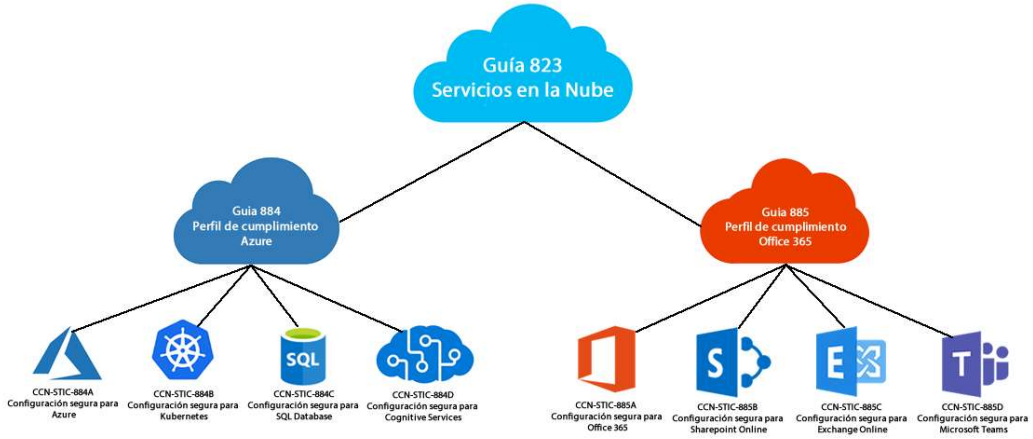
73
Threat Report

Total reports figures (2019)

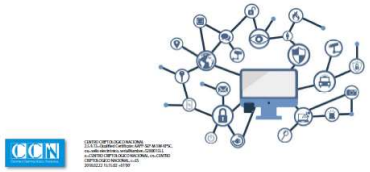
227
Total Reports

1.200.000
downloads

Cloud Services Adaptation



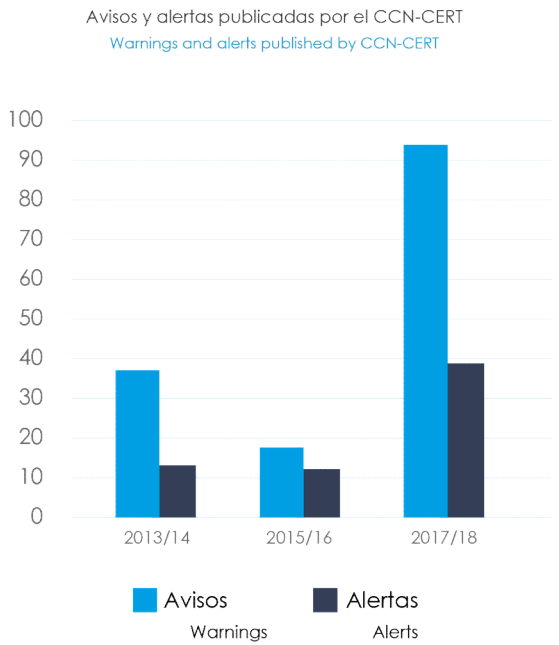
LISTADO DE GUÍAS CCN-STIC

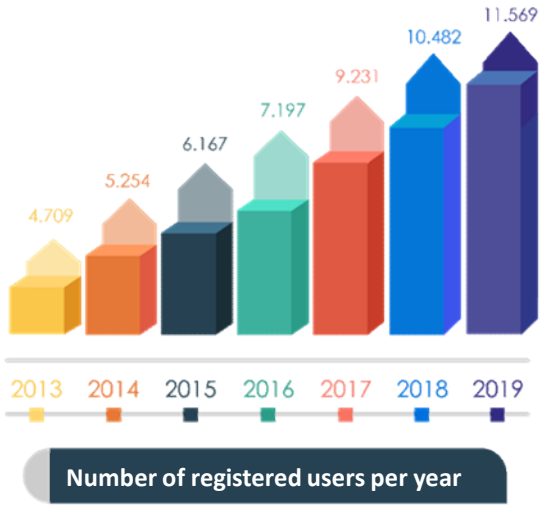


centro criptológico nacional

02 Warnings and vulnerabilities

All users registered on the CCN-CERT website, receive cybersecurity notifications and warnings, informing them of newly detected threats.





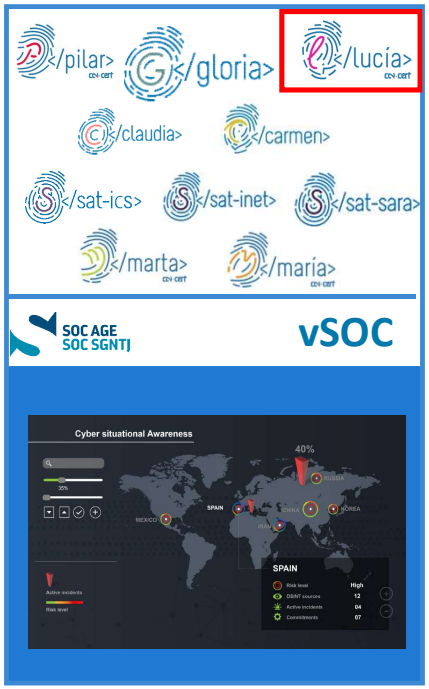
centro criptológico nacional

How do we manage cybersecurity?

Auditing solutions	Detection solutions	Analysis solutions	Surveillance solutions	Exchange solutions	Training solutions
/inés>	/sat-inet>	/gloria>	/carmen>	/lucía>	/vanesa>
/pilar>	/sat-sara>	/maría>	/claudia>	/loreto>	ATENEA
/amparo>	/sat-ics>	/marta>	/reyes>		
/clara>			/elisa>		
/rocío>					
/emma>					
/ana>					

centro criptológico nacional

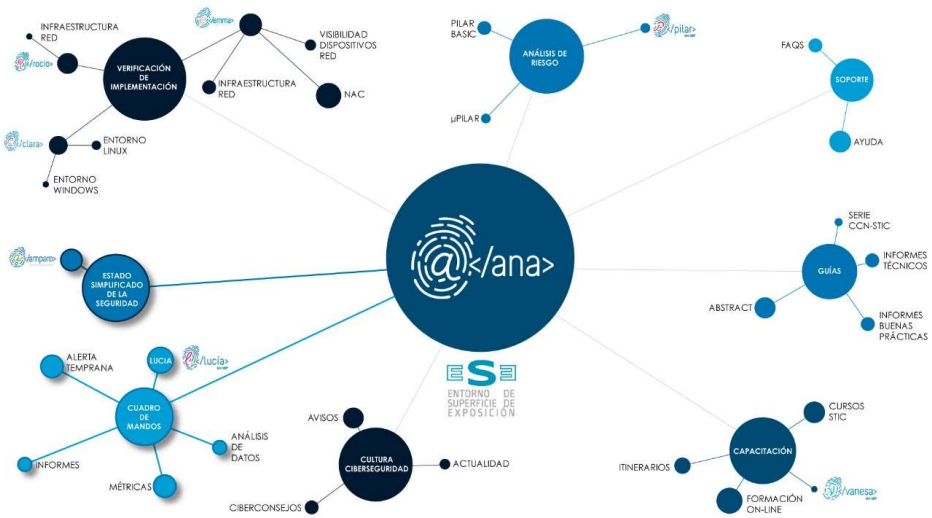
Cybersecurity Environments



ens
Esquema Nacional de Seguridad

CCN
centro criptológico nacional

03 Security audits and inspections



Exposure surface Environment

National Security Framework Validation Environment

centro criptológico nacional

04 Training

2019 figures

Face to face Course

21 + 7 (600)
Face-to-face courses

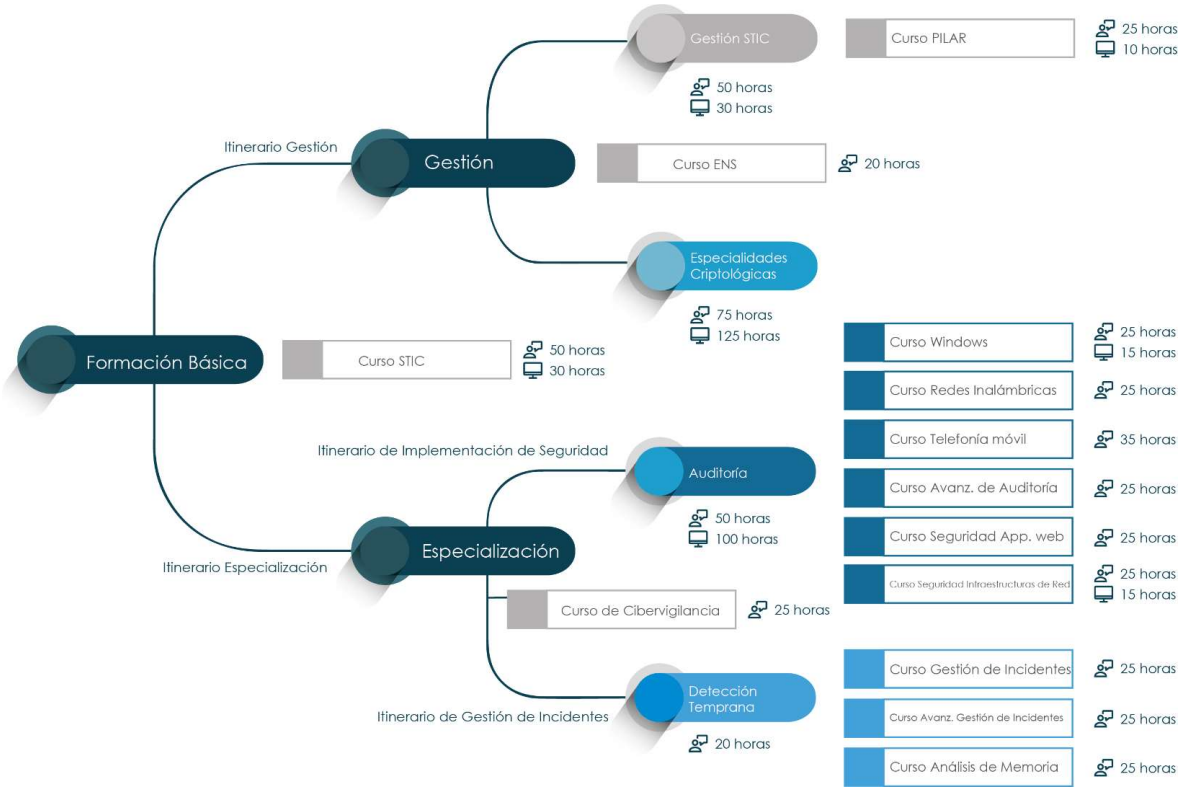
Online Training

21 (+4.000)
Distance learning course

ATENEA

+9.200
users

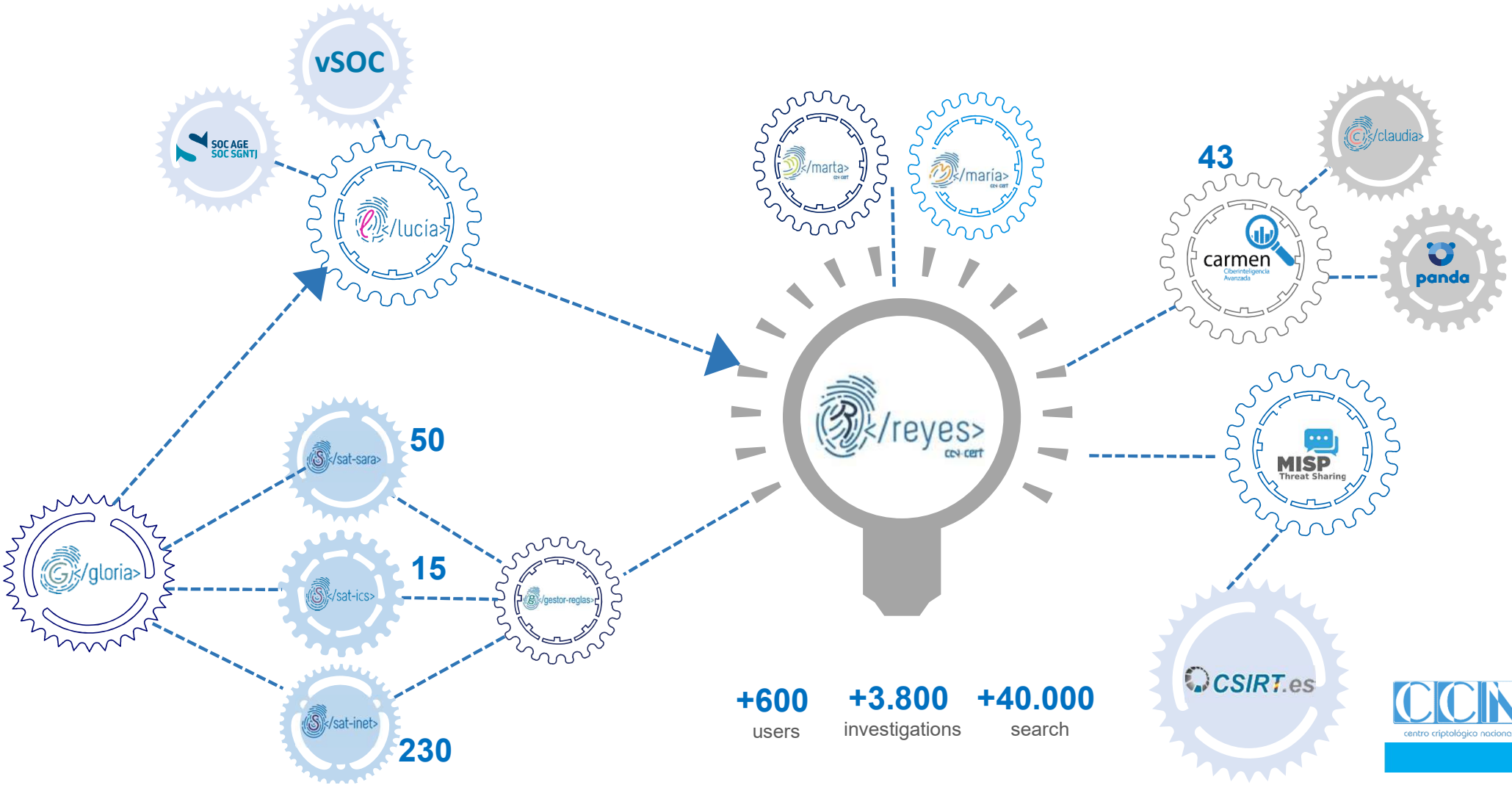
101
Security challenges



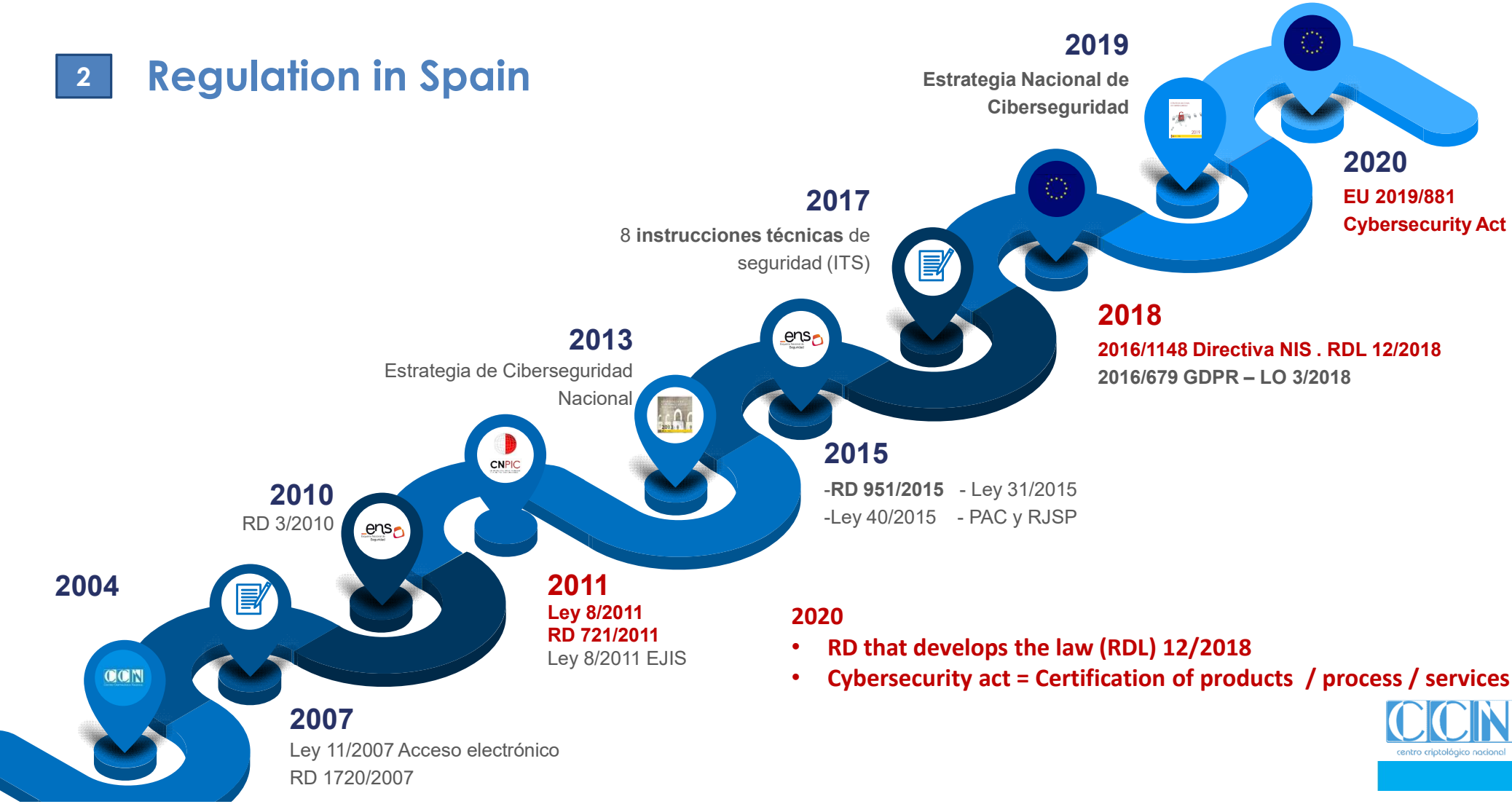
Training itineraries

centro criptológico nacional

Continuous surveillance. Detection



2 Regulation in Spain

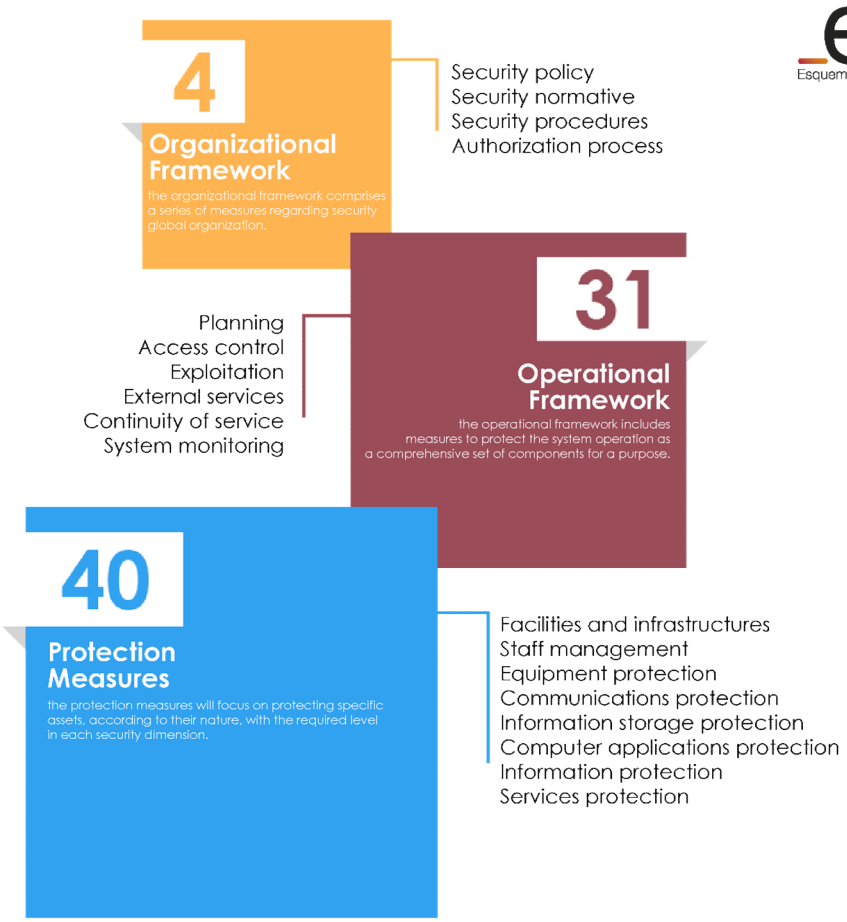


2020

- **RD that develops the law (RDL) 12/2018**
- **Cybersecurity act = Certification of products / process / services**

National Security Scheme

75 Security measures

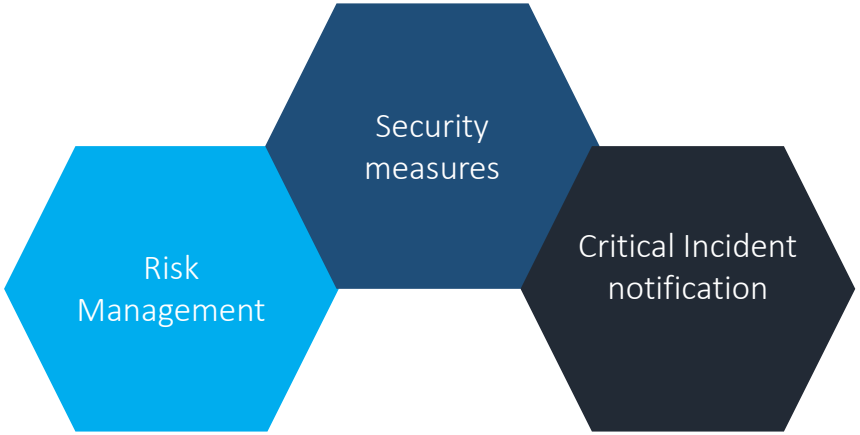


¿Why National Cybersecurity Framework?

- **Create the conditions of trust** in the use of electronic means, through **measures** to guarantee **security**, allowing the citizens and the AAPP, **the exercise of rights and the fulfillment of duties.**
- Promote the **continuous management of security**, apart from specific impulses, or their absence.
- Contemplate the aspects of **prevention**, **detection** and **Respond**.
- Promote a **homogenous treatment** of security that facilitates cooperation when dealing with different entities, through a **common language and common elements**, to facilitate the implementation of measures and the interaction between AA.PP. and the private sector.
- Provide **leadership** in the area of **good practices**.

CCN
centro criptológico nacional

2016/679 GDPR –LO 3/2018



Proactive and demonstrable responsibility.

Security measures:

- **Risk analysis**
- Personal Data managing activity log
- **Data protection security measures: from the design & by default**
- **Notification of cyber security incidents (security breaches)**
- Evaluation of impact about risk data treatment
- **Data protection Officer**
- Build certification schemes in data protection

1ST Additional Provision: NSF (ENS) security measures must be applied in Public sector.

Notification vs Sharing

CCN centro criptológico nacional

2016/1148 NIS Directive – RDL 12/2018

Nuclear Energy	Public Administration	Space
Feeding	Chemical Industry	Investigation Facilities
Water	Health	Transport
Banking & financial market	Digital Service & IT infrastructure)	Energy

Critical Infrastructure (CI)
Essential Services (ES)

Most public operators

To promote on line security in EU

- Greater National Capacity in cyber security
  - **NIS National Strategy**
  - **NIS Competent authorities**
  - **Responsible CSIRT**
- Cooperation at EU level
  - NIS COOPERATION GROUP
  - CSIRTs Network
  - enisa
- Security requirements
  - ens Esquema Nacional de Seguridad

Risk Management

Security measures

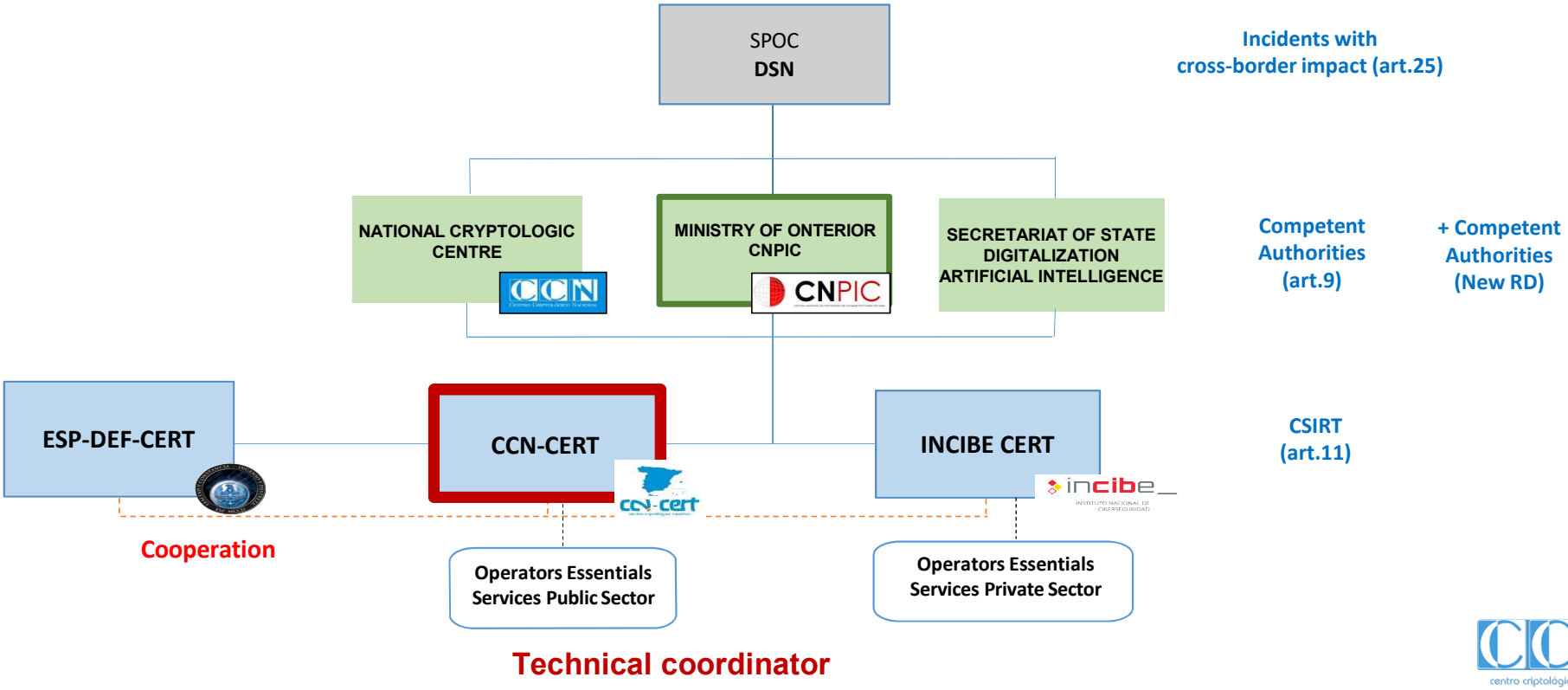
Critical Incident notification

Law 8/2011 CI
RD 721/2011 CI

CCN centro criptológico nacional

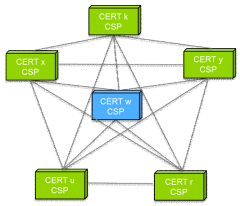
Spanish application NISD

2016/1148 NISD – RDL 12/2018



Actors in National Cybersecurity

Technical Response



CSIRT Network CSP

EGC group

Operational / Political level

ccn-cert
centro criptológico nacional

Critical Infrastructures

LEA

CNPIC

incibe_

Public Sector

SOC AGE

CSIRT-CV

cesicat

Defence & Armed Forces

Private Sector

CSIRT.es

CCN
centro criptológico nacional

RD that develops the law (RDL) 12/2018

Objectives:

- Establish competent authorities.
- **Provide a common platform to notify and sharing cyber incidents**. Tool to coordinate Competent authority & responsible CSIRT**.**
  - **Supposed special risk/impact = VERY HIGH & CRITICAL cyber incidents**
- Single point of contact missions.
- Security measures for DSP & ESO
  - **Minimum set of cybersecurity measures: ANEX II ENS**
- Chief Information Security Officer (CISO = ENS Security Officer). Missions.
- Technical Instruction about notification & sharing cyber incidents**.**
  - **Incident to notify: HIGH, VERY HIGH & CRITICAL**
  - Taxonomy (ENISA)
  - **Risk Level**
  - **Impact level**
  - Information to notify
  - Maximum time to notify

Nivel de peligrosidad o impacto	Notificación inicial	Notificación intermedia	Notificación final
CRÍTICO	Inmediata	24 / 48 horas	20 días
MUY ALTO	Inmediata	72 horas	40 días
ALTO	Inmediata	-	-
MEDIO	-	-	-
BAJO	-	-	-

centro criptológico nacional

National cyber incidents Platform

Cyber threat information exchange modules

Vulnerabilities report & registry module

Massive data sharing module

Cyber incident handling module

Sample analysis module

Secure communications

Statistics & reports

Main Functions:

- Taxonomy
- Criticality
- Federation
- Other authorities
- Metrics in incident handling.

Classification of incidents

When it is a crisis ?

CRITICAL

- APT with information exfiltration
- Distributed Denial of Service (DDoS) (sustained)
- Ransomware?

VERY HIGH

- Targeted Attack
- Denial of Service (DoS)
- Customized Malware

LOW / MEDIUM / HIGH

- External attacks with no consequences
- Generic Malware
- Most incidents

Guideline CCN-STIC-817– Common Criteria for incident handling

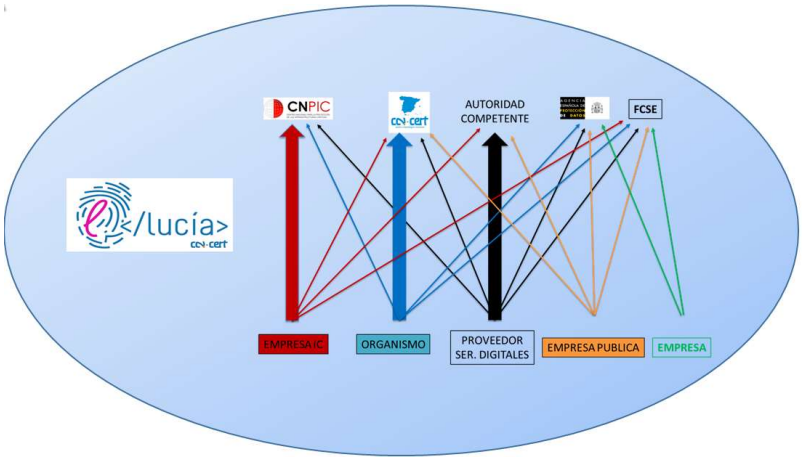
CCN
centro criptológico nacional

Need of a Common Platform

A common platform in order to facilitate and automate the reporting, communication and incident handling processes.

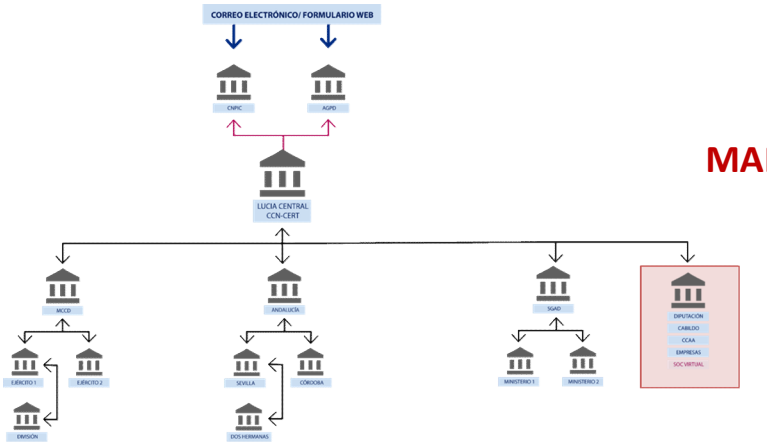
(Operator decides what and when reporting / sharing)

SINGLE NOTIFICATION



In this way operators should not keep several notifications depending on the authority to which they should be addressed.

FEDERATION



MANY ENTITIES

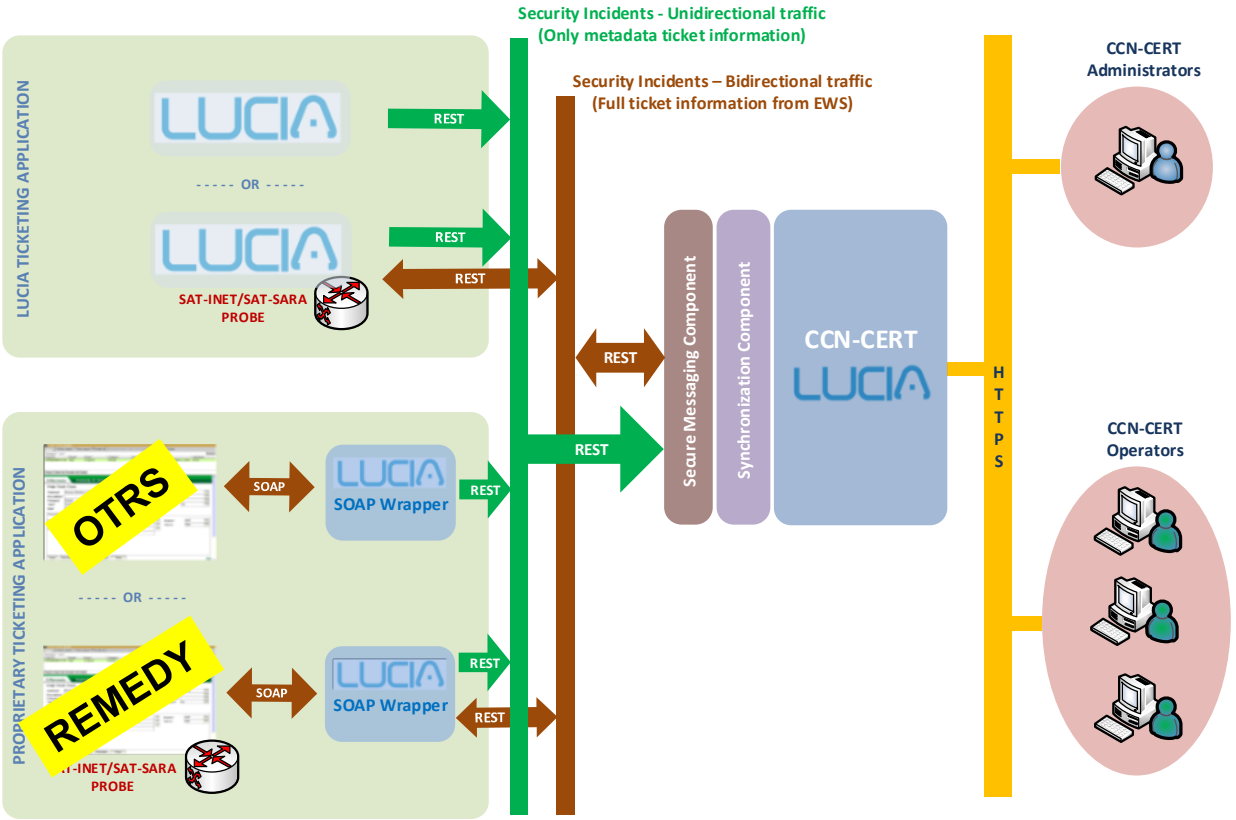
Other authorities in the loop.
VIRTUAL SOC

centro criptológico nacional

LUCIA - Module Description

- **LUCIA** (Unified List for Incident and Threat Coordination) is a solution developed by CCN-CERT (Spanish National Government CERT) for the **management of cyber incidents** in the entities participating in the National Security Framework.
- Key aspects:
  - Based on RT for Incident Response (RTIR): offers a common language to assess risk level and classify incidents, and enables traceability and monitoring.
  - Allows carrying out tasks automatically and can be integrated into already installed systems
  - Federated model: entities can run their own instance and sync it with others'.
  - **Allows entities to manage several types of cyber incidents** (currently):
    - incidents arisen from the own Institution, detected by their own means.
    - incidents arisen from CCN-CERT's Early Warning System (SAT)

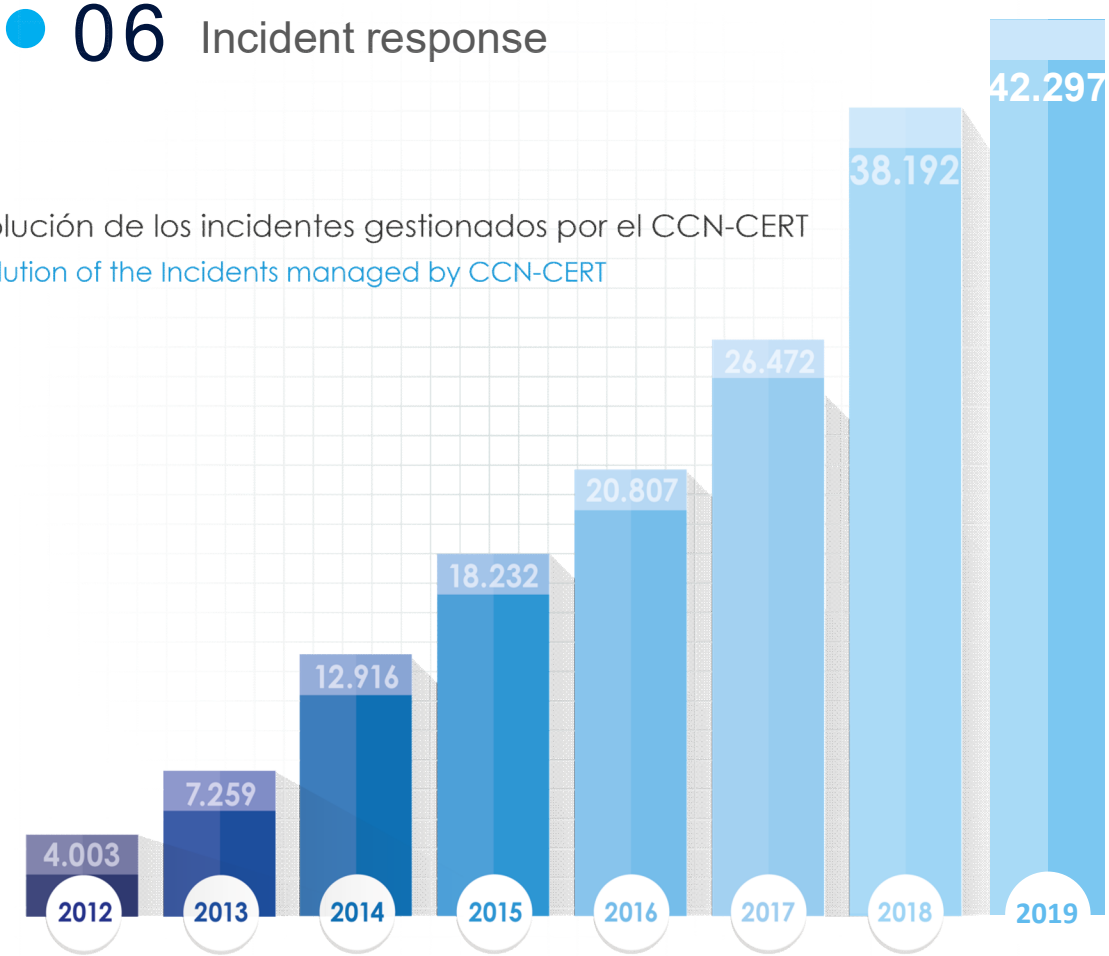
Architecture



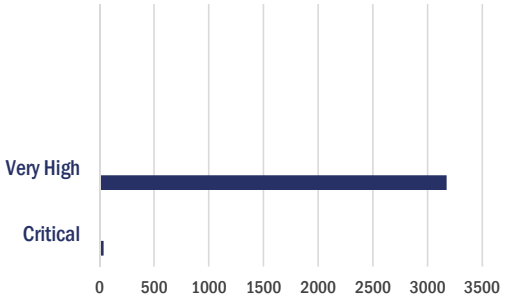
06 Incident response

Evolución de los incidentes gestionados por el CCN-CERT

Evolution of the Incidents managed by CCN-CERT



Level of danger - Incidents managed by CCN-CERT in 2019



2019

37 Crítical Incidentes

3.172 Very High Incidents

37 Interventions

34%
2019

13.500

/lucía>
ccn-cert

CCN
centro criptológico nacional

Thank You

E-mails

info@ccn-cert.cni.es

ccn@cni.es

sat-inet@ccn-cert.cni.es

sat-sara@ccn-cert.cni.es

sat-ics@ccn-cert.cni.es

organismo.certificacion@cni.es

Web Pages:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

INCIDENT CLASIFICATION CRITERIA

Cómo utilizar la matriz de clasificación

1. Evaluar el efecto conocido o probable del incidente:
- La naturaleza de lo que está ocurriendo y el efecto en el sistema o sistemas de destino
- Si los efectos son continuos, empeoran o se mueven lateralmente
- La importancia de los sistemas, servicios o datos de destino
- Considerar la atribución (capacidad e intención) o cualquier interés operativo

2. Evaluar la(s) víctima(s) del incidente:
- El número de víctimas
- La relevancia de la(s) víctima(s)
- Considerar tanto a las víctimas primarias como a las secundarias

3. En situaciones excepcionales, añada un indicador ALTO o CRÍTICO:
- Puede ser aplicado a cualquier categoría o incidente
- Se utiliza en circunstancias excepcionales cuando se requieren mayores recursos o una respuesta rápida de emergencia

La atribución (y la intención deliberada en particular) puede ser un factor adicional en la escalada de incidentes

Ataques complejos, extracción masiva de datos e interrupción sostenida de los sistemas esenciales y los servicios asociados

Extracción o eliminación de datos sensibles o propiedad intelectual

Malware, beaconing u otra intrusión activa en la red: interrupción temporal del sistema/servicio

Ataque malicioso de bajo nivel: reconocimiento selectivo, suplantación de identidad, phishing, y pérdida de datos no sensibles

Escaneo o reconocimiento

AUMENTO DEL EFECTO CONOCIDO O PROBABLE Y/O IMPORTANCIA DEL SERVICIO/DATOS IMPACTADOS

L0 (Irrelevante)	L1 (Bajo)	L2 (Medio)	L3 (Alto)	L4 (Muy Alto)	L5 (Crítico)
L0 (Irrelevante)	L1 (Bajo)	L2 (Medio)	L3 (Alto)	L3 (Alto)	L4 (Muy Alto)
L0 (Irrelevante)	L1 (Bajo)	L1 (Bajo)	L2 (Medio)	L3 (Alto)	L3 (Alto)
L0 (Irrelevante)	L0 (Irrelevante)	L1 (Bajo)	L2 (Medio)	L2 (Medio)	L2 (Medio)
L0 (Irrelevante)	L0 (Irrelevante)	L0 (Irrelevante)	L1 (Bajo)	L1 (Bajo)	L1 (Bajo)

VÍCTIMA

Ciudadanos	Pequeña empresa	Mediana empresa	Gobierno autonómico, gran empresa, infraestructuras	Gobierno central, servicios esenciales	Sectores estratégicos, Infraestructuras críticas
	-20.000 hab	-75.000 hab	+75.000 hab		

A medida que aumenta la importancia y/o el número de víctimas, escalar a la derecha

- L0 Irrelevante
- L1 Bajo
- L2 Medio
- L3 Alto
- L4 Muy Alto
- L5 Crítico

Cómo utilizar la matriz de clasificación

MUY ALTO

Prioridad o perfil alto
Compromiso extremadamente generalizado
Impacto que cambia la vida de las víctimas
Vinculado a un actor de amenaza estratégicamente importante

Calendario y contexto (por ejemplo, eventos)
Alta visibilidad pública
Potencial de alto impacto, pero aún no se ha materializado

CRÍTICO

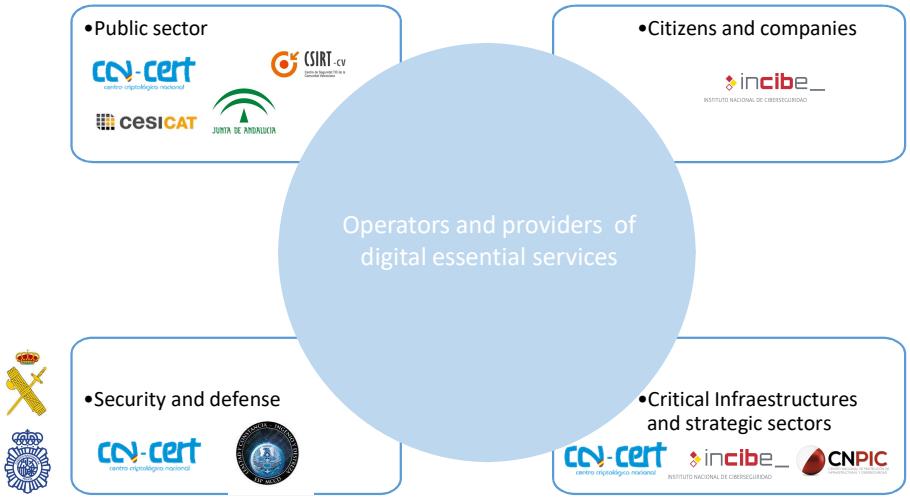
Extrema sensibilidad en el tiempo

Los impactos en la vida real son continuos o inminentes, o se requiere una contención rápida.
Amenaza a la vida o individuo(s) vulnerable(s)
Daños graves a la propiedad intelectual o servicios esenciales, extracción masiva de datos.

centro criptológico nacional

05 Information exchange

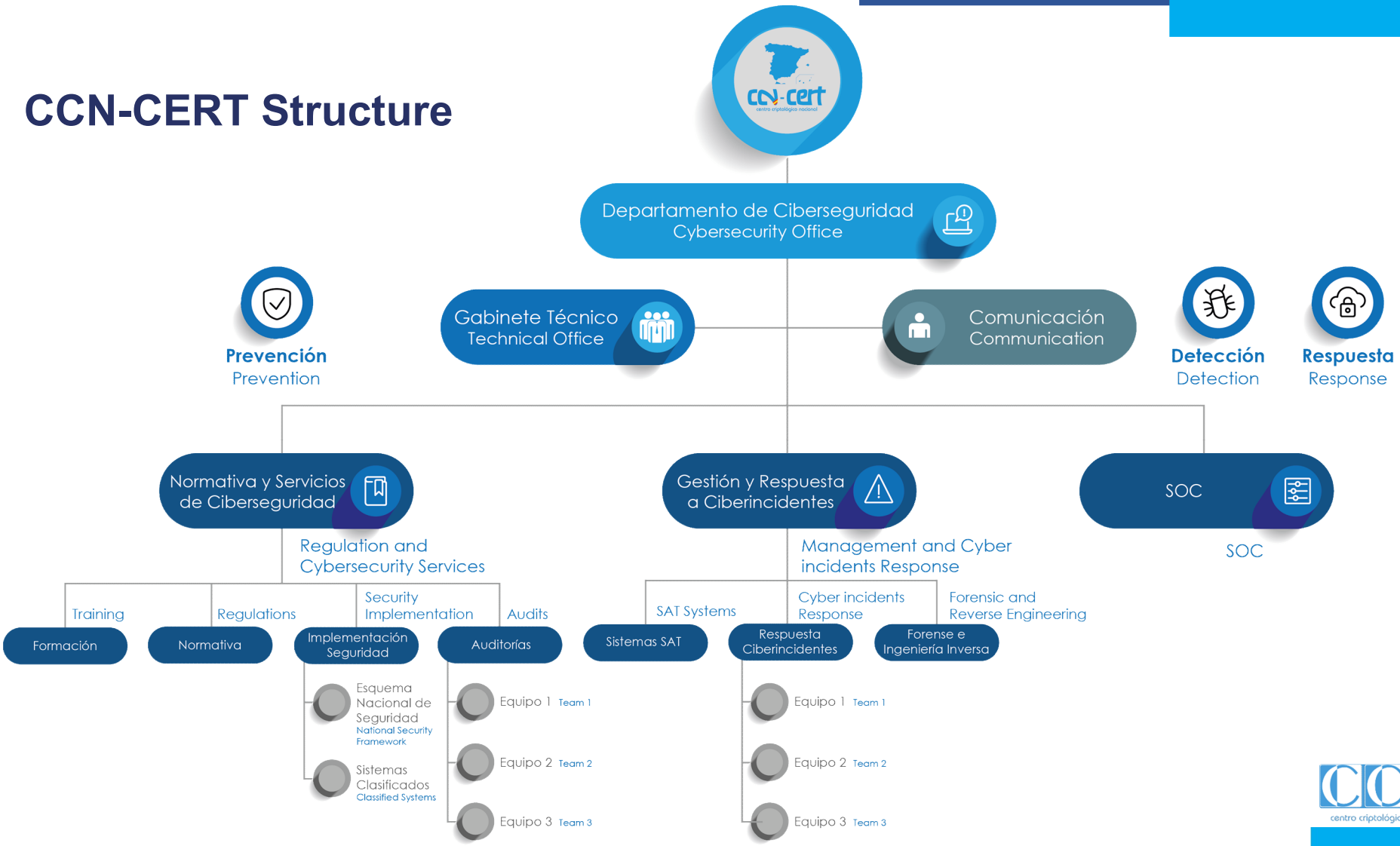
- Exchange with other Services
- Forum of Incident Response and Security Teams (FIRST),
- CSIRT Network
- Trusted Introducer
- Etc.



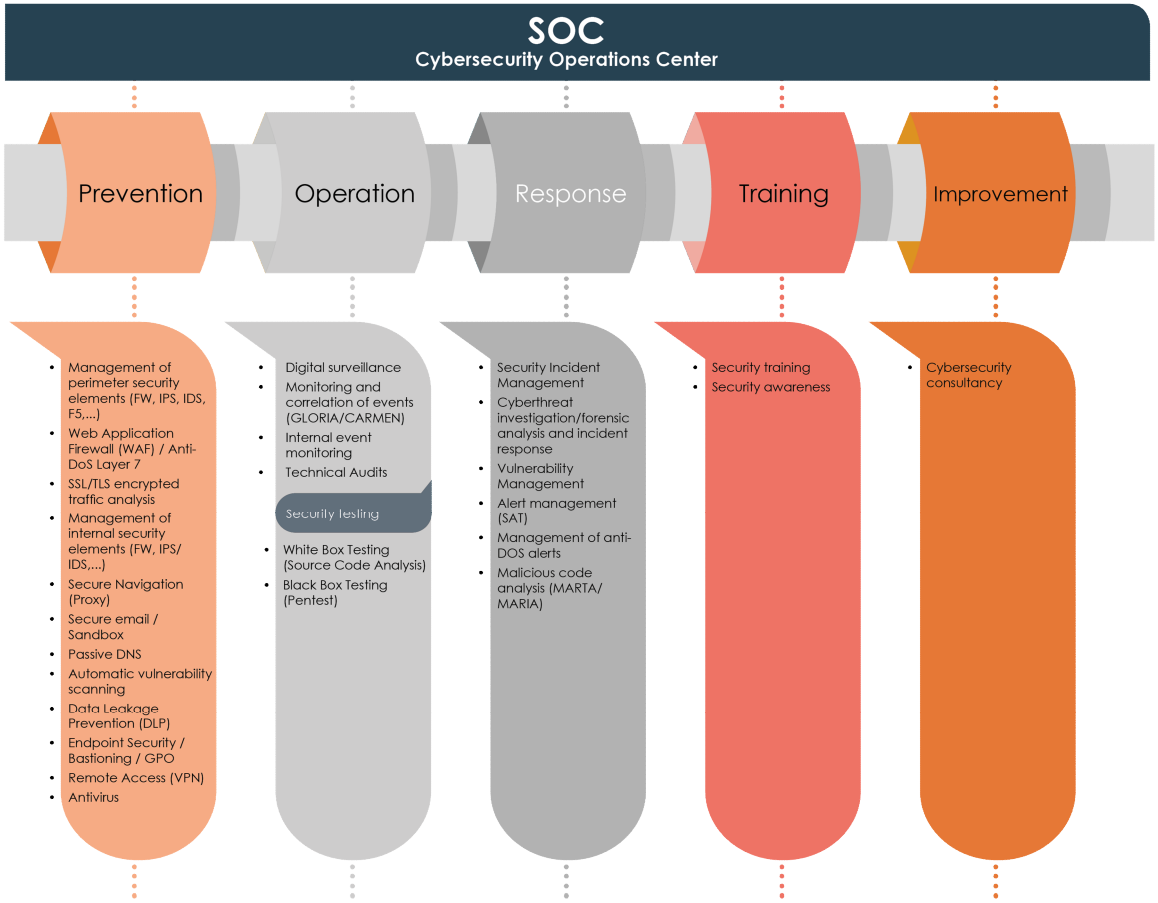
CSIRT.es

centro criptológico nacional

CCN-CERT Structure



07 Security Operation Centre



CCN
centro criptológico nacional