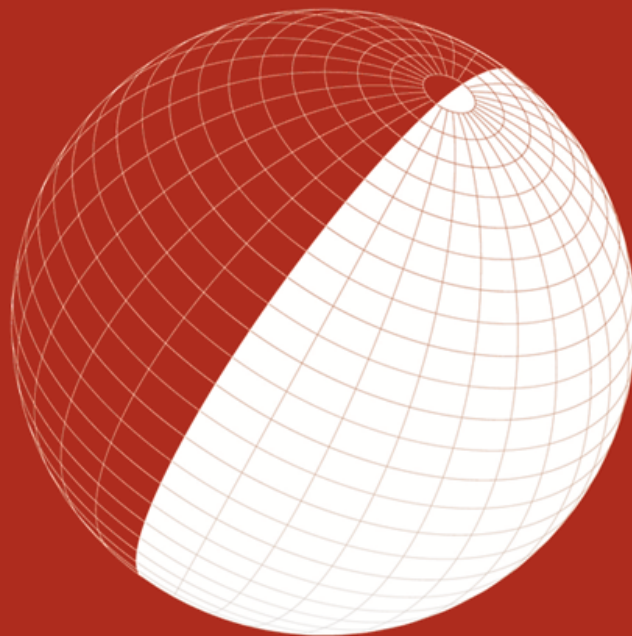


PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

IMPACTO DEL RD-LEY 12/2018,
DE SEGURIDAD DE LAS REDES Y
SISTEMAS DE INFORMACIÓN



CNPIC

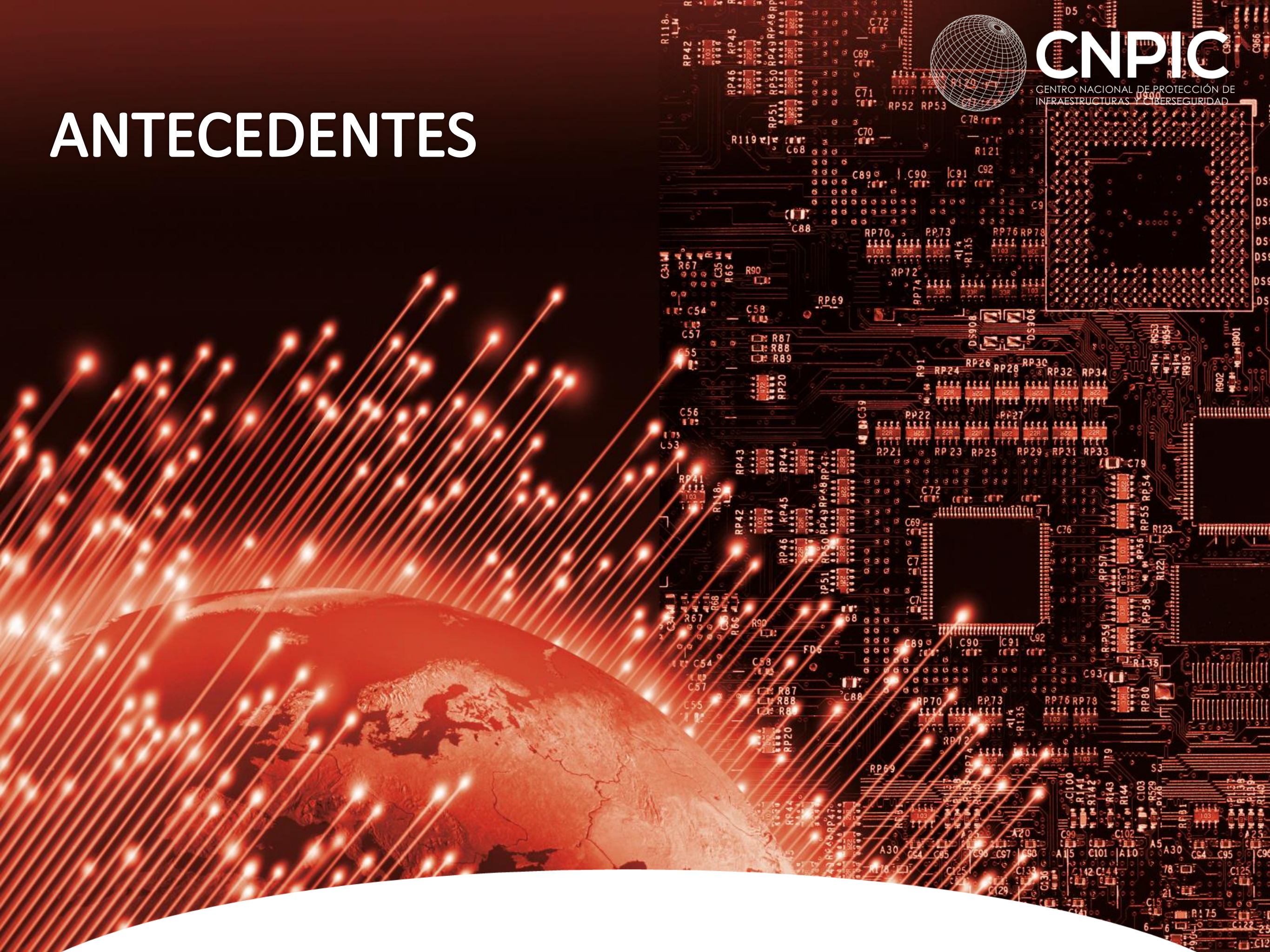
CENTRO NACIONAL DE PROTECCIÓN DE
INFRAESTRUCTURAS Y CIBERSEGURIDAD

ANTECEDENTES



CNPIC

CENTRO NACIONAL DE PROTECCIÓN DE
INFRAESTRUCTURAS Y CIBERSEGURIDAD



DIRECTIVA 2016/1148 CE (NIS)

The NIS Directive: objectives

Increased national
cybersecurity capabilities

EU level
cooperation

Risk management &
reporting

Boosting the
overall
online
security in
Europe

OBLIGATORIEDAD
OPERADORES Y
PROVEEDORES
DE REPORTAR
CIBERINCIDENTES
(AUTORIDADES, CSIRTS)

(AUTORIDADES, CSIRTS)
CIBERINCIDENTES

DIRECTIVA 2016/1148 CE (NIS)



DIRECTIVA 2016/1148 CE (NIS)

ANEXO II: Sectores y Subsectores (art. 4.4)

Á
m
b
i
t
o

ENERGY: ELECTRICITY, GAS AND OIL

TRANSPORTATION: AIR, RAILROAD, WATER AND ROAD

BANKING: CREDIT INSTITUTIONS

FINANCIAL MARKET INFRASTRUCTURE

HEALTH: HEALTHCARE PROVIDERS

WATER: DRINKING WATER SUPPLY AND DISTRIBUTION

DIGITAL INFRASTRUCTURE: INTERNET EXCHANGE POINTS,
DOMAIN NAME SYSTEM SERVICE PROVIDERS,
TOP LEVEL DOMAIN NAME REGISTERS

DIRECTIVA 2008/114 EU (PIC)

ANEXO I: Sectores y Subsectores

**Á
m
b
i
t
o**

ENERGY: ELECTRICITY, GAS AND OIL

TRANSPORTATION: AIR, RAILROAD, WATER AND ROAD

DIRECTIVA 2008/114 EU (PIC)

Sectores y Subsectores

Á
m
b
i
t
o

ENERGÍA	INDUSTRIA NUCLEAR	TIC	AGUA
			
ALIMENTACIÓN	SALUD	SISTEMA FINANCIERO	TRANSPORTE
			
INDUSTRIA QUÍMICA	ESPACIO	INVESTIGACIÓN	ADMINISTRACIÓN
			

LEY 8/2011, PIC

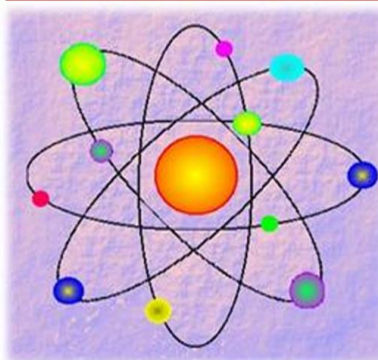
ENFOQUE INTEGRAL (FÍSICO / CIBER / PERSONAL)

ENERGÍA

INDUSTRIA NUCLEAR

TIC

AGUA



ALIMENTACIÓN

SALUD

SISTEMA FINANCIERO

TRANSPORTE



INDUSTRIA QUÍMICA

ESPACIO

INVESTIGACIÓN

ADMINISTRACIÓN



Art. 2, a): **SERVICIO ESENCIAL:** », el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Art. 2, b): **SECTOR ESTRÁTEGICO:** cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma

Art. 2, h): **CRITERIOS HORIZONTALES DE CRITICIDAD,**

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.
2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.
3. El impacto medioambiental, degradación en el lugar y sus alrededores.
4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales

COM (2009) 149 final

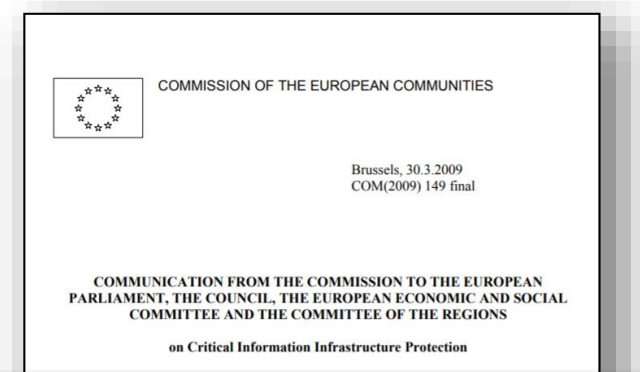
1: Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these **(b) ICT systems, services, networks and infrastructures (in short, ICT infrastructures)** form a vital part of European economy and society, either **(a) providing essential goods and services or constituting the underpinning platform of other critical infrastructures**. They are typically regarded as **critical information infrastructures (CIIs)** as their **(c) disruption or destruction would have a serious impact on vital societal functions**.

1: This Communication focuses on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the **security and resilience of CIIs**. This focus **is consistent** with the debate launched at the request of the Council and the European Parliament to addresses the challenges and priorities for **network and information security (NIS) policy** and the most appropriate instruments needed at EU level to tackle them.

Critical Information Infrastructure (CII): ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers / software, Internet, satellites, etc.).”

“CIIP should therefore be viewed as a **cross-sector phenomenon** rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective”.

(Libro Verde PEPIC COM(2005) 576 final - 2005).



Art 5.2 NIS DIRECTIVE

The criteria for the identification of the **operators of essential services**, as referred to in point (4) of Article 4, shall be as follows:

- (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;**
- (b) the provision of that service depends on network and information systems; and**
- (c) an incident would have significant disruptive effects on the provision of that service.**

COM (2009) 149 final

2: On the regulatory side, the Commission proposal to reform the Regulatory Framework for electronic communications networks and services contains new provisions on security and integrity, in particular to:

- (1) **strengthen operators' obligations to ensure that appropriate measures are taken** to meet identified risks,
- (2) **guarantee the continuity of supply of services** and
- (3) **notify security breaches**.

5.5. Criteria for European Critical Infrastructures in the ICT sector

ICT sector specific criteria. By building on the initial activity carried out in 2008, the Commission will

- continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria for identifying European critical infrastructures for the ICT sector. To this end, relevant information will be drawn from a specific study being launched.³²

Target: first half of 2010 for the Commission to define the criteria for the European critical infrastructures for the ICT sector.

Art. 14 NIS DIRECTIVE:

1. Member States shall ensure that operators of essential services **take appropriate and proportionate technical and organisational measures to manage the risks** posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the **provision of such essential services, with a view to ensuring the continuity of those services**.

3. Member States shall ensure that operators of essential services **notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact** on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

CEPS TASK FORCE REPORT 2010

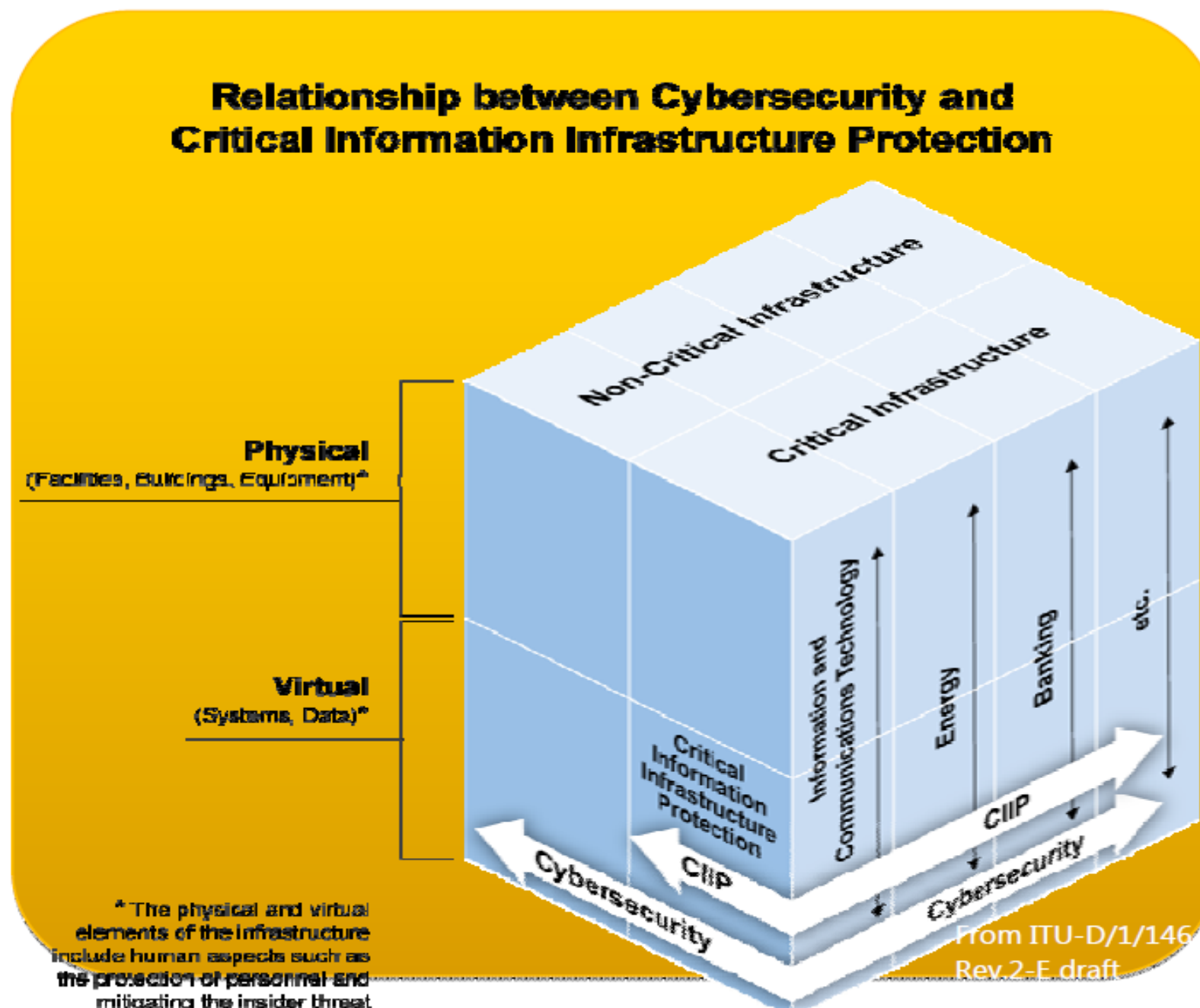
P. 24:

“Overall, it is widely acknowledged that **CIIP can be seen as a subset of CIP**, albeit essential for the purposes of infrastructure protection.

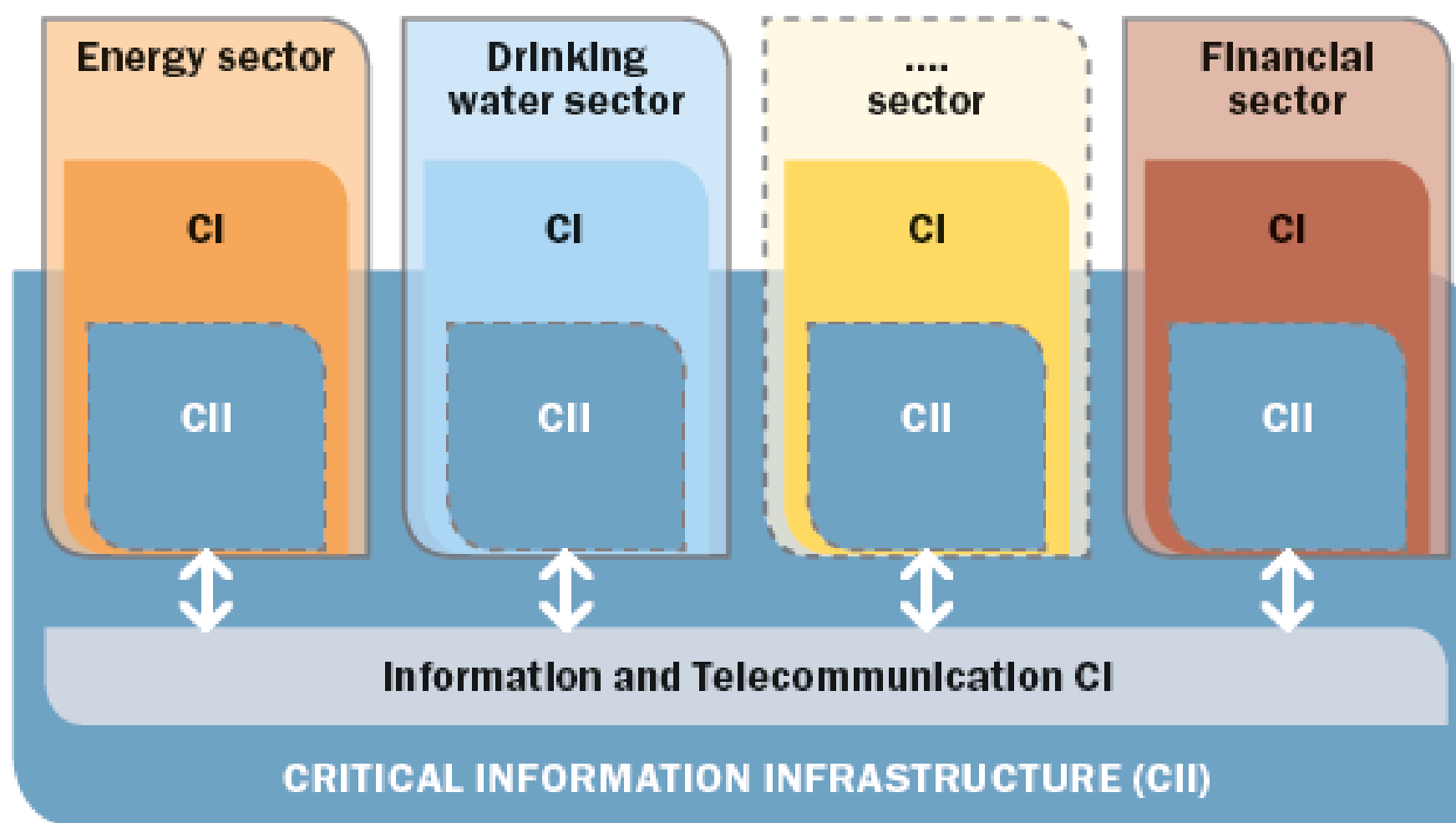
Critical Information Infrastructure (CII) generally refers to Information and Communication Technology systems that are essential to operations of national and international Critical Infrastructures. Examples include **i)** telecommunication networks, management, location-based services for emergency calls; **ii)** transportation: air traffic control, train routing and control, traffic management; **iii)** financial services: credit card transactions, settlement systems, transaction records, electronic stock/bond trading; and **iv)** control systems/SCADA (Supervisory, Control and Data Acquisition) to manage energy production and distribution, chemical manufacturing and refining processes. In a recent OECD recommendation, CII was defined as referring to: ***those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.***

CII can include **i)** information components supporting critical infrastructures; **ii)** information infrastructures supporting essential components of government business; and/or **iii)** information infrastructures essential to the national economy.

Figure 7. Cyber-security and CIIP



IMPLANTACIÓN POLÍTICAS CIP - CIIP



IMPLANTACIÓN POLÍTICAS CIP - CIIP



- ✓ UK
- ✓ FRANCIA
- ✓ ALEMANIA
- ✓ HOLANDA
- ✓ USA
- ✓ **ESPAÑA**

UNIÓN
EUROPEA



- ✓ JAPÓN
- ✓ COREA
- ✓ AUSTRALIA
- ✓ BÉLGICA
- ✓ CROACIA

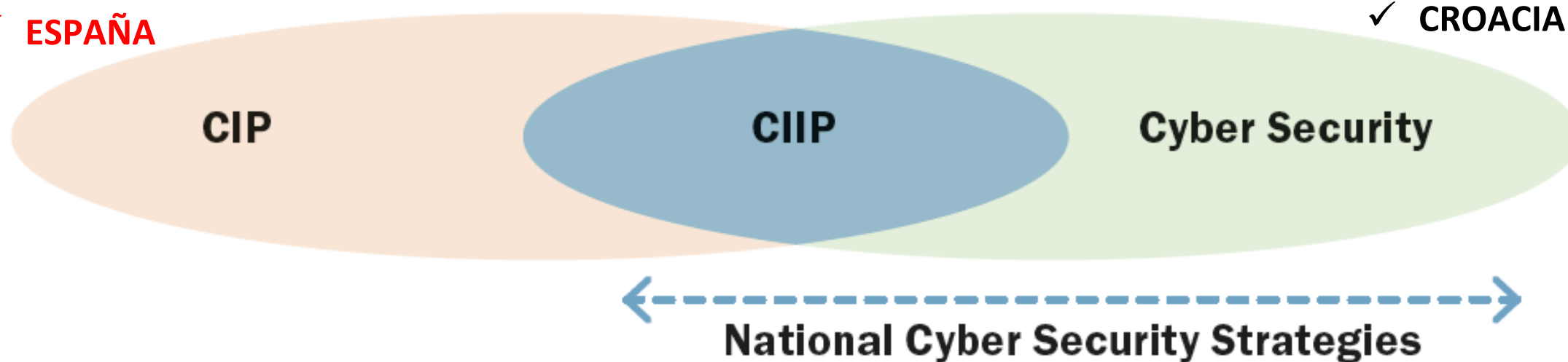


Figure 2. Relationship and coverage between CIP, CIIP, and cyber security.

PARTE I – CONCLUSIONES

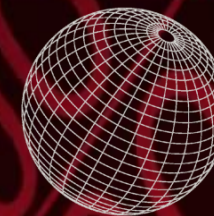
LA TRANSPOSICIÓN DE LA DIRECTIVA NIS A LA LEGISLACIÓN NACIONAL DEBE CONSIDERAR, EN LA PARTE RELATIVA A LAS MEDIDAS DE PROTECCIÓN SOBRE LOS SERVICIOS ESENCIALES, LA LEY 8/2011 PIC:

- La base conceptual del **art. 5 de la Directiva NIS** (identificación operadores servicios esenciales) coincide con el término **CII**.
- El **concepto de servicio esencial** (al que no se refiere la Directiva NIS) se puede integrar en la definición del art. 2 a) de la Ley 8/2011, PIC.
No existen servicios esenciales PIC y servicios esenciales NIS, SÓLO EXISTEN SERVICIOS ESENCIALES
- La **aproximación sectorial** de la Directiva NIS se debe integrar en la sectorización existente en la Ley 8/2011, PIC.
- **Procedimientos** para llevar a cabo la identificación de los servicios esenciales, la dependencia (o no) de las redes y sistemas de información, y la designación de operadores esenciales: **PES**.

PARTE I – CONCLUSIONES

LA TRANSPOSICIÓN DE LA DIRECTIVA NIS A LA LEGISLACIÓN NACIONAL DEBE CONSIDERAR, EN LA PARTE RELATIVA A LAS MEDIDAS DE PROTECCIÓN SOBRE LOS SERVICIOS ESENCIALES, LA LEY 8/2011 PIC:

- Al afectar de forma muy importante a la **seguridad nacional** (un bien jurídico a proteger es la **prestación y continuidad de los servicios esenciales**). «*considerandos 19, 20, 49, 57*»; «*arts. 5.2., 6.1., 14.3*».
- Por el principio de **eficiencia jurídica**.
- Al estar ya **establecidos mecanismos operativos** que cubren la mayoría de necesidades previstas por la Directiva, y al contar con la **aceptación de los operadores** de los sectores estratégicos afectados.
- Para **impedir la inseguridad jurídica y obligaciones duplicadas** de las entidades dentro del ámbito de aplicación de la nueva norma.
- Por razones de **eficiencia económica**.



CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE
INFRAESTRUCTURAS Y CIBERSEGURIDAD

ANÁLISIS RDL 12/2018 (LSRSI): IMPACTO SOBRE LEY 8/2011 (LPIC)

RASGOS PRINCIPALES RD-LEY 12/2018, SRSI



Ámbito de
aplicación



Autoridad
competente



CSIRTS
de
referencia



Obligaciones
de
seguridad



Régimen
sancionador



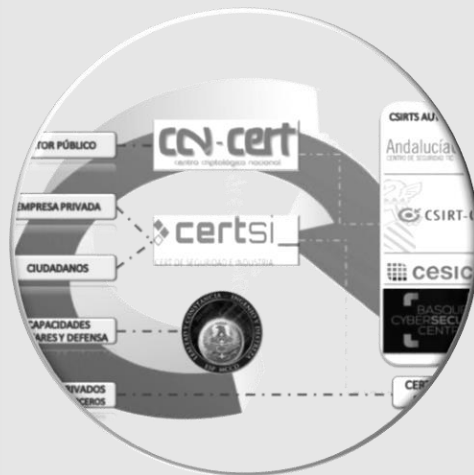
RASGOS PRINCIPALES LEY SRSI



**ÁMBITO DE
APLICACIÓN**



**Autoridad
competente**



**CSIRTS
de
referencia**



**Obligaciones
de
seguridad**



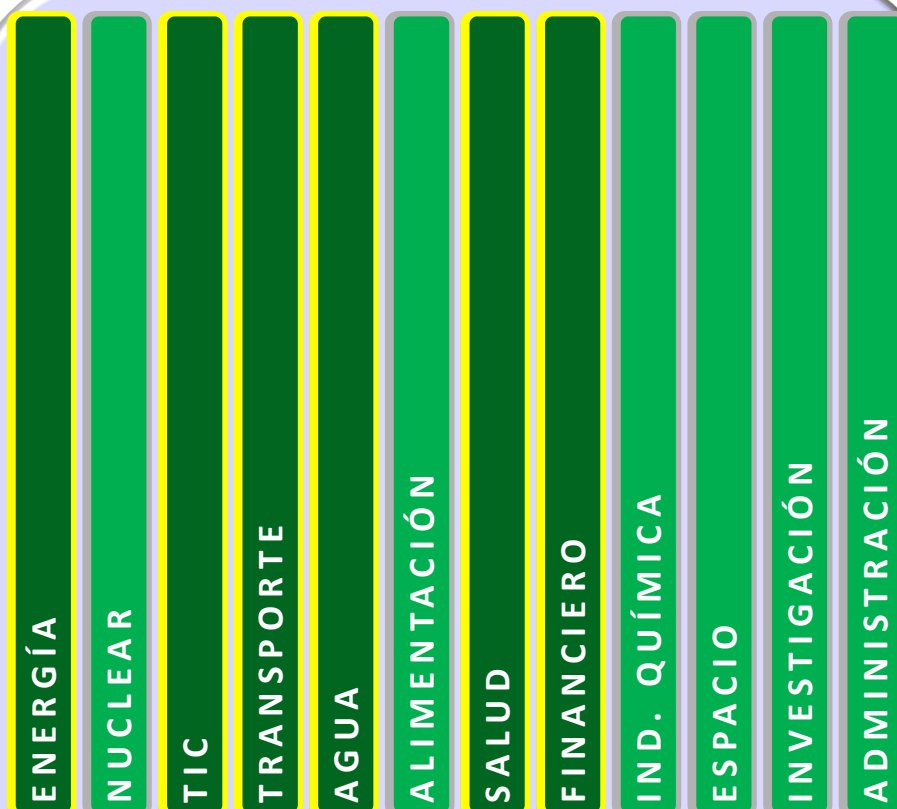
**Régimen
sancionador**

SERVICIOS ESENCIALES Y SECTORES DE APLICACIÓN

SERVICIO ESENCIAL: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas [art. 2.a) LPIC]

que dependa para su provisión de las redes y sistemas de información [art. 3.c) RD-LSRSI]

SERVICIOS DIGITALES



SERVICIOS ESENCIALES



IDENTIFICACIÓN SERVICIOS ESENCIALES

La identificación de los servicios esenciales y de los operadores que los prestan se efectuará por los órganos y procedimientos previstos por la Ley 8/2011 y su normativa de desarrollo [art. 6.1. RD-LSRSI]



SECTOR FINANCIERO

SUBSECTOR	ÁMBITO	SERVICIO ESENCIAL	DESCRIPCIÓN // JUSTIFICACIÓN ESENCIALIDAD	DEPENDENCIA DE LAS REDES Y SISTEMAS DE INFORMACIÓN
SISTEMAS Y SERVICIOS DE PAGO	PAGOS ELECTRÓNICOS MINORISTAS	Intercambio, compensación y liquidación de instrumentos de pago de pequeños importes	Canaliza, mediante procedimientos de naturaleza electrónica, una parte sustancial de operaciones minoristas, de incidencia muy directa en la economía real (pago de nóminas, pensiones, o devoluciones de impuestos, entre otras).	SÍ El servicio se realiza a través de los sistemas y procedimientos electrónicos del SNCE y de redes de comunicación financiera.
	PAGOS ELECTRÓNICOS MAYORISTAS	Liquidación de grandes pagos entre entidades financieras de la zona euro	Es el sistema donde se liquidan los sistemas vinculados, el mercado interbancario y las operaciones de política monetaria de la zona euro. Procesa elevados importes y está directamente vinculado con el conjunto del sistema de pagos español.	SÍ El intercambio con la plataforma TARGET2 se realiza mediante procedimientos electrónicos y a través de la red de comunicación financiera de SWIFT.
	PAGOS CON TARJETA DE CRÉDITO O DÉBITO	Pagos de particulares con tarjeta de crédito y de débito	Este servicio se utiliza por particulares mediante tarjetas emitidas por entidades de crédito, permitiendo el procesamiento de pagos que se liquida en las cuentas de las entidades. El sistema electrónico de pago principal en el comercio minorista es el que se realiza mediante tarjeta de crédito o débito y TPV, y constituye más del 40% del volumen de ventas.	SÍ Todos los procesos se llevan a cabo por medios electrónicos.
	PAGOS Y COBROS EN EFECTIVO	Pagos y cobros en efectivo	Este servicio de pago utiliza billetes emitidos por el banco central europeo y se distribuyen por el Banco de España. El efectivo es el medio de pago más utilizado por número de transacciones y constituye un medio esencial de pago.	NO
	PAGOS MINORISTAS POR CUENTA DE LAS ADMINISTRACIONES PÚBLICAS	Pagos minoristas por cuenta de las Administraciones Públicas	Es el servicio de pago del Estado y la Seguridad Social a sus beneficiarios, a través de las entidades financieras. Dentro de estos pagos se incluyen: las nóminas de funcionarios, las pensiones, o la participación de las comunidades autónomas en los ingresos del Estado.	SÍ Las órdenes se dan a través de sistemas electrónicos.

SERVICIOS ESENCIALES IDENTIFICADOS

ENERGÍA: 14 SERVICIOS ESENCIALES

TRANSPORTE: 19 SERVICIOS ESENCIALES

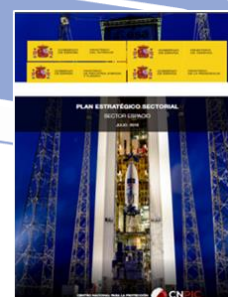
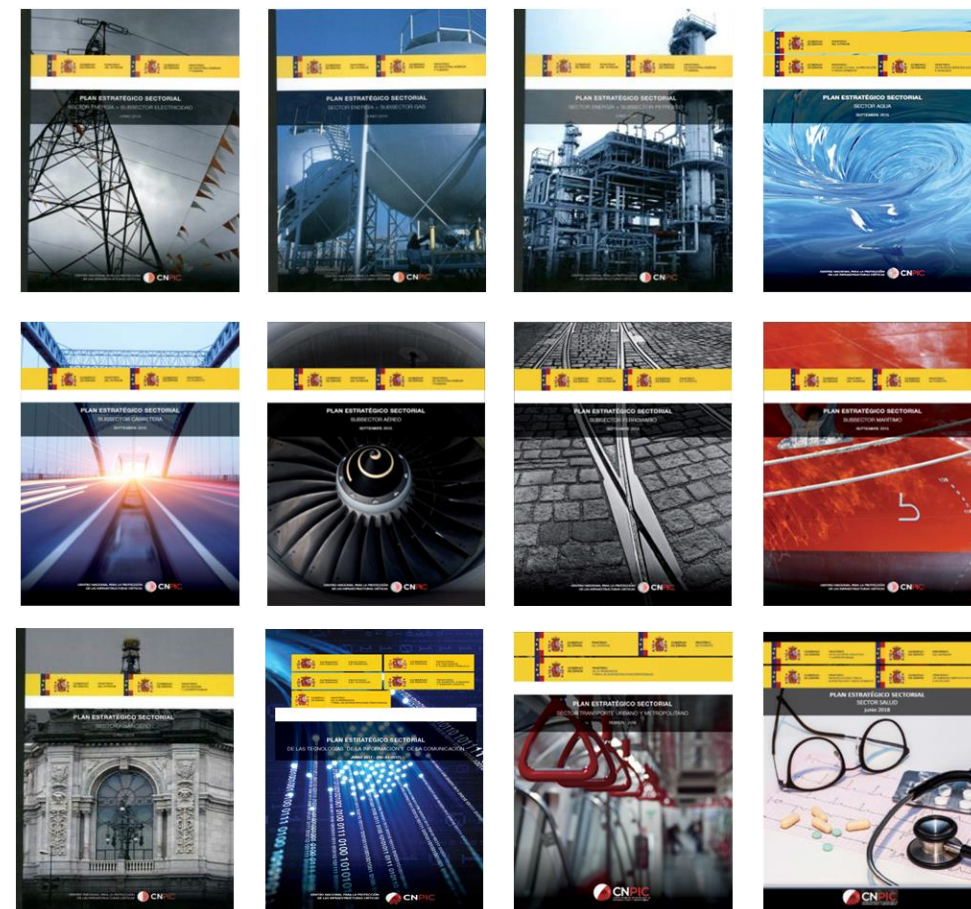
SALUD: 10 SERVICIOS ESENCIALES

SERVICIOS FINANCIEROS: 15 SERVICIOS ESENCIALES

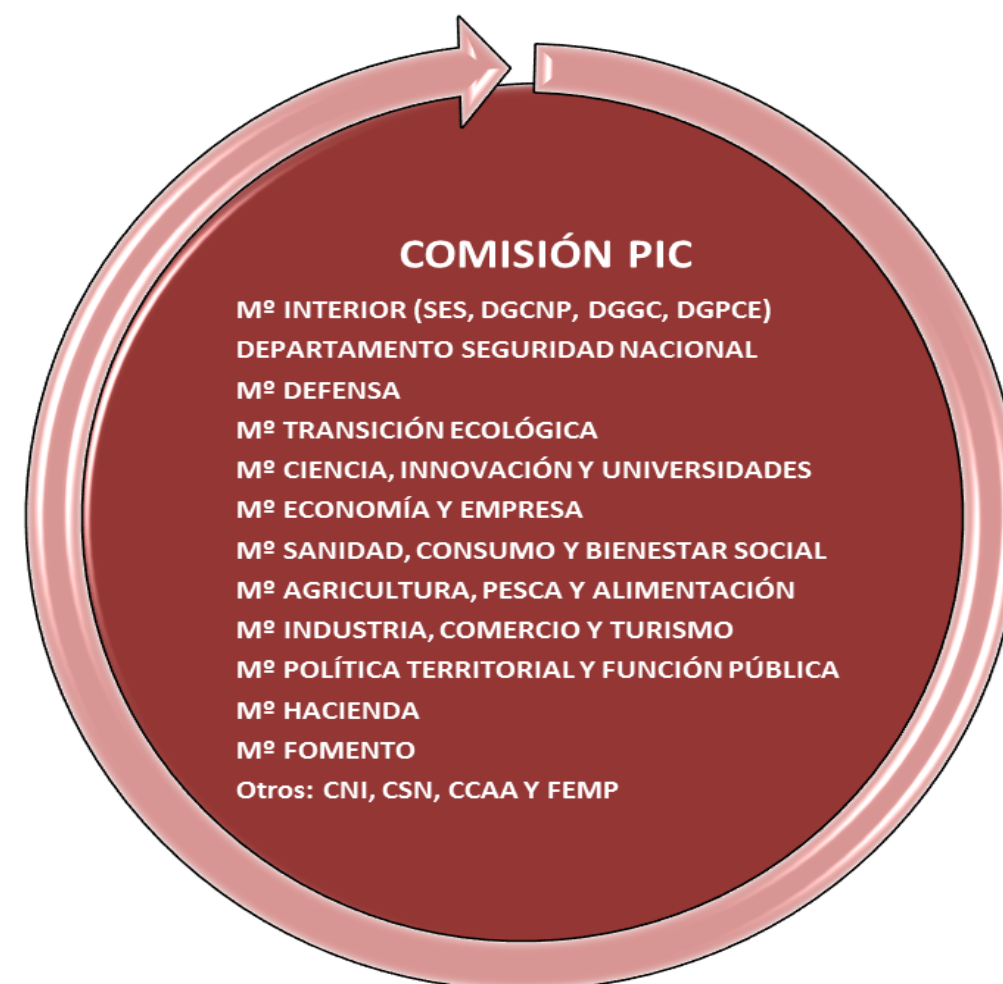
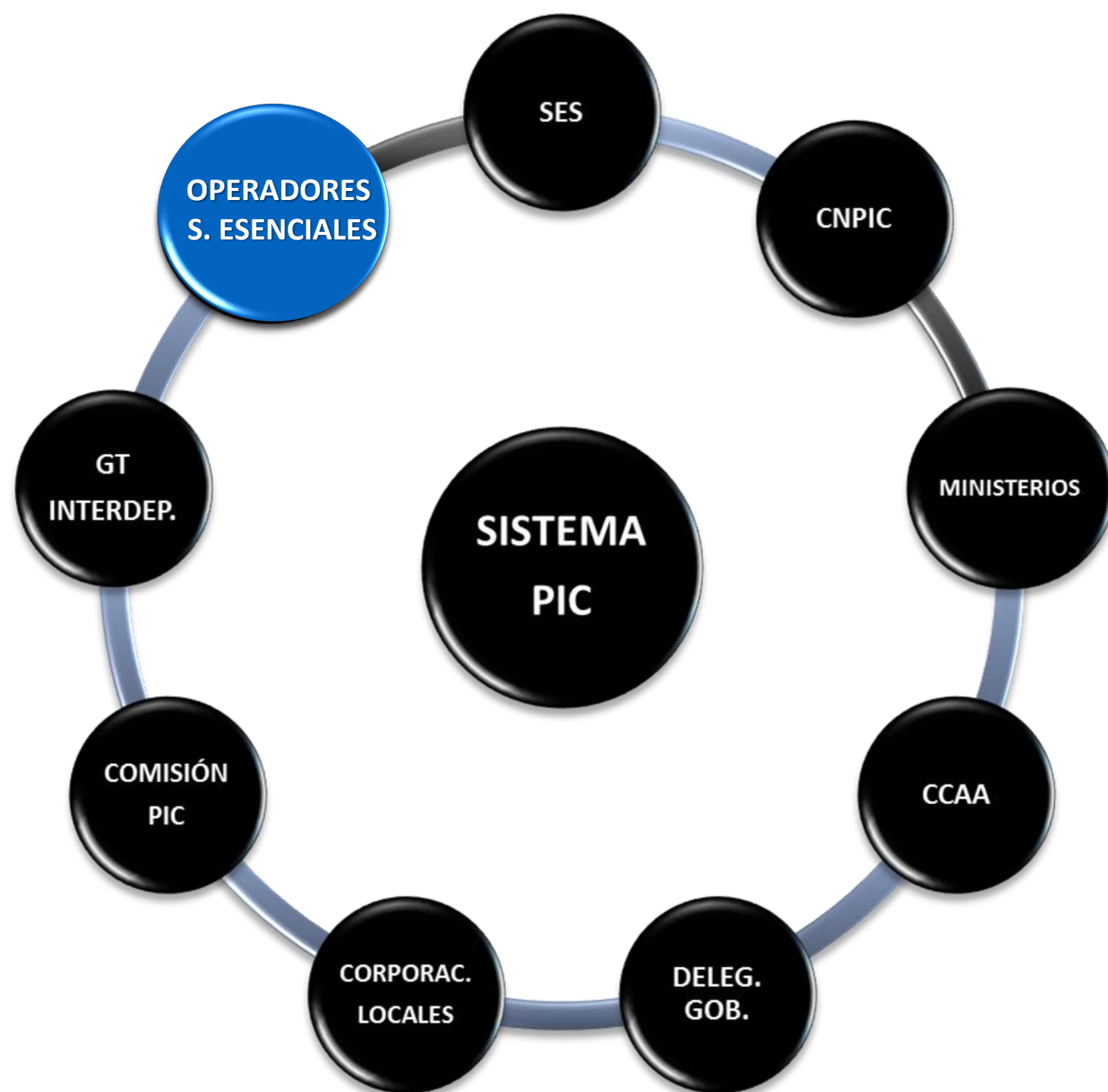
AGUA: 5 SERVICIOS ESENCIALES

TIC / SERVICIOS DIGITALES : 8 SERVICIOS ESENCIALES

ANTES DE 2019/11/09



IDENTIFICACIÓN OPERADORES CRÍTICOS Y ESENCIALES



SERVICIOS ESENCIALES Y SECTORES DE APLICACIÓN

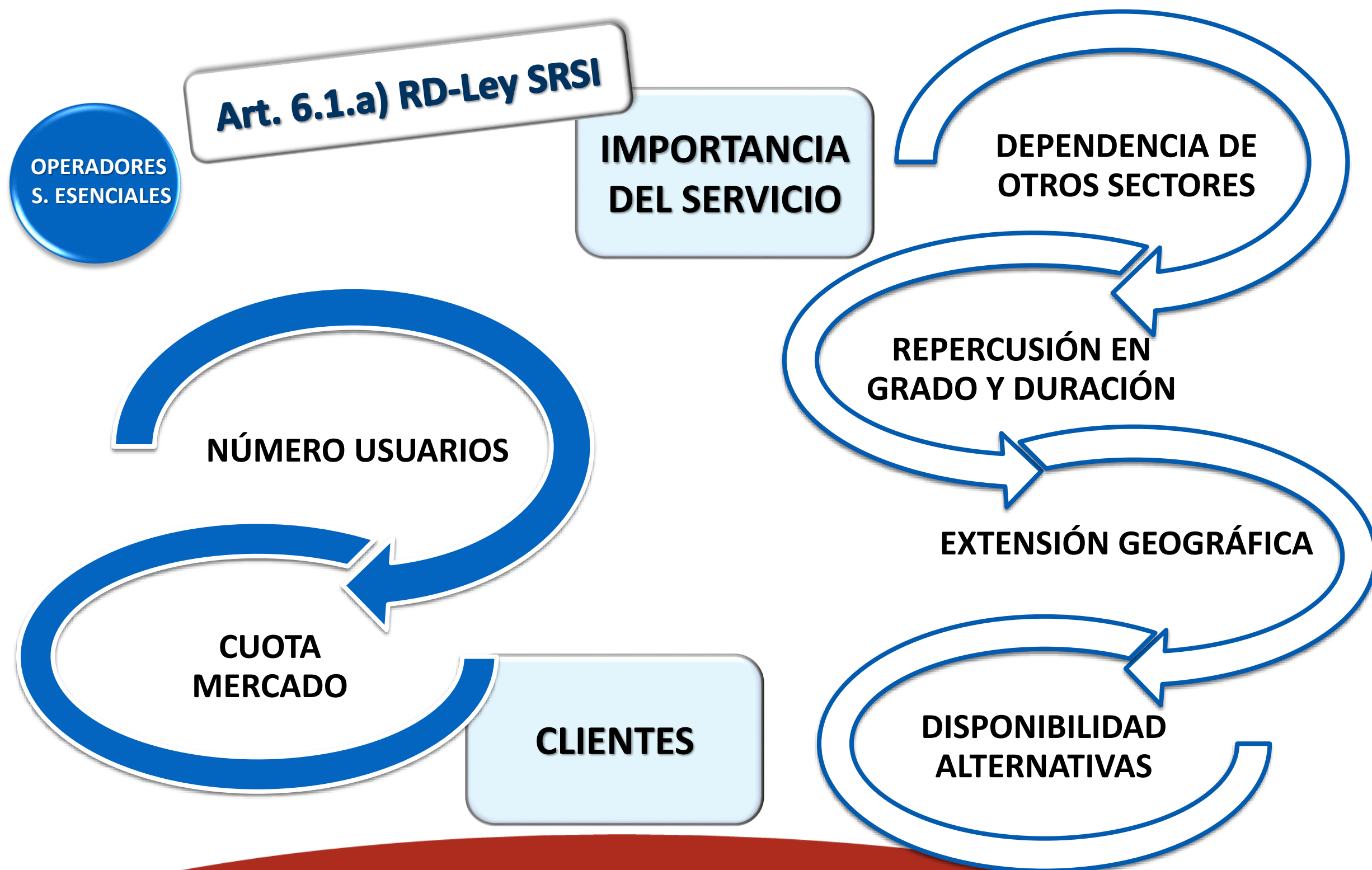
SERVICIO ESENCIAL: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas [art. 2.a) LPIC]

que dependa para su provisión de las redes y sistemas de información [art. 3.c) RD-LSRSI]

OPERADOR DE SERVICIOS ESENCIALES: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril [art. 3.d) RD-LSRSI]



IDENTIFICACIÓN OPERADORES CRÍTICOS Y ESENCIALES



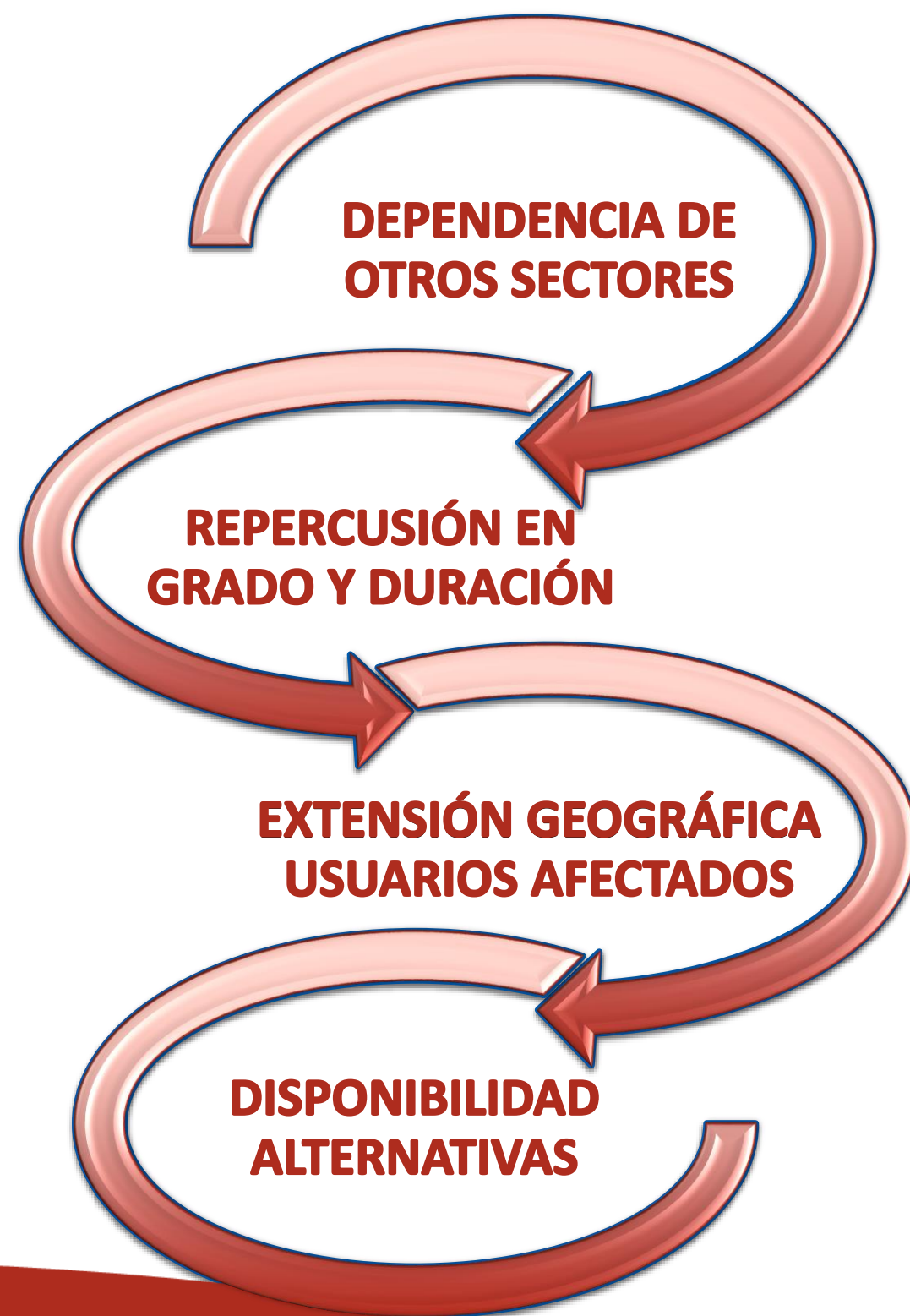
IDENTIFICACIÓN OPERADORES CRÍTICOS Y ESENCIALES

**OPERADORES
CRÍTICOS**

**Encaje con art. 6.1.a)
RD-Ley SRSI**



IDENTIFICACIÓN OPERADORES CRÍTICOS Y ESENCIALES



IDENTIFICACIÓN OPERADORES CRÍTICOS Y ESENCIALES

ART. 6.2. RD-LEY SRSI

**EN EL CASO DE TRATARSE DE UN
OPERADOR CRÍTICO DESIGNADO
EN CUMPLIMIENTO DE LA LEY
8/2011, DE 28 DE ABRIL, BASTARÁ
CON QUE SE CONSTATE SU
DEPENDENCIA DE LAS REDES Y
SISTEMAS DE INFORMACIÓN PARA
LA PROVISIÓN DEL SERVICIO
ESENCIAL DE QUE SE TRATE**



OPERADORES S. ESENCIALES IDENTIFICADOS

ENERGÍA: 18 OPERADORES CRÍTICOS // SERVICIOS ESENCIALES

TRANSPORTE: 43 OPERADORES CRÍTICOS // SERVICIOS ESENCIALES

SALUD: 11 OPERADORES CRÍTICOS // SERVICIOS ESENCIALES

S. FINANCIEROS: 14 OPERADORES CRÍTICOS // SERVICIOS ESENCIALES

AGUA: 37 OPERADORES CRÍTICOS // SERVICIOS ESENCIALES

TIC : 8 OPERADORES CRÍTICOS // SERVICIOS ESENCIALES

132

**DEPENDENCIA DE
OTROS SECTORES**

**REPERCUSIÓN EN
GRADO Y DURACIÓN**

**EXTENSIÓN GEOGRÁFICA
USUARIOS AFECTADOS**

**DISPONIBILIDAD
ALTERNATIVAS**

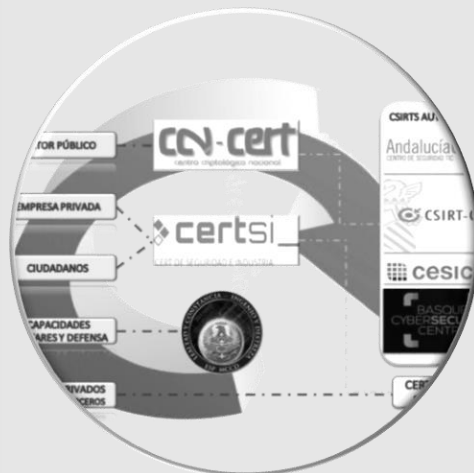
RASGOS PRINCIPALES LEY SRSI



Ámbito de
aplicación



**AUTORIDAD
COMPETENTE**



CSIRTS
de
referencia



Obligaciones
de
seguridad



Régimen
sancionador

AUTORIDAD COMPETENTE

ART. 9 RD-LEY SRSI

**AUTORIDAD
NACIONAL: SES**

- Supervisar cumplimiento obligaciones: gestión riesgos/impacto mínimo
- Requerir información para evaluar seguridad de redes y sistemas de información
- Requerir pruebas de aplicación efectiva de políticas de seguridad (auditorías)
- Dictar instrucciones vinculantes para subsanar deficiencias
- Cooperar con otras autoridades nacionales e internacionales
- Recibir notificación incidentes (a través CSIRTS)
- Ejercer la potestad sancionadora

**OPERADORES
CRÍTICOS**

SERVICIOS ESENCIALES

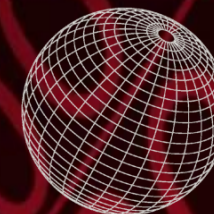
SERVICIOS DIGITALES



**RD
SRSI**

AUTORIDAD COMPETENTE





RASGOS PRINCIPALES LEY SRSI



Ámbito de
aplicación



Autoridad
competente



CSIRTS
DE
REFERENCIA

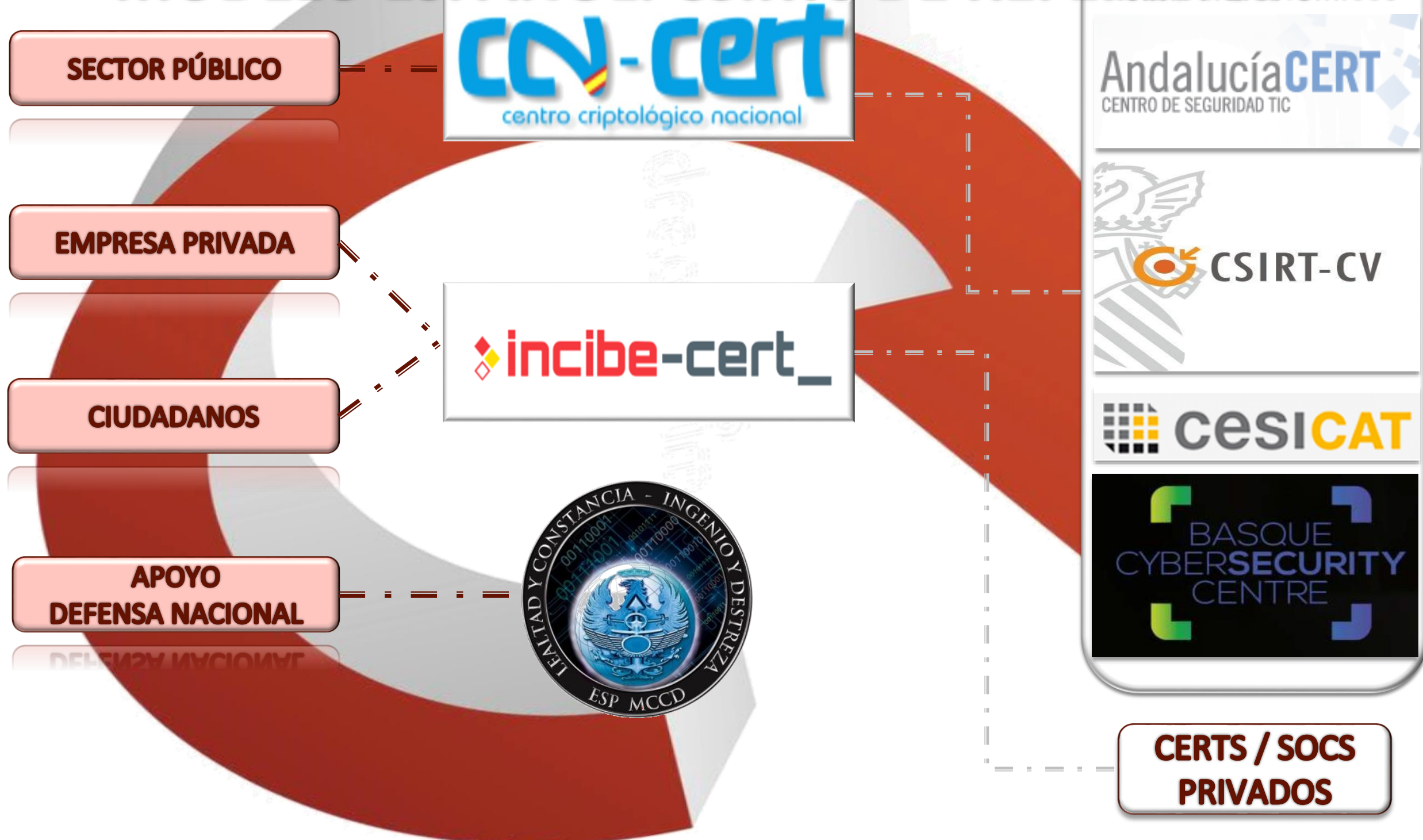


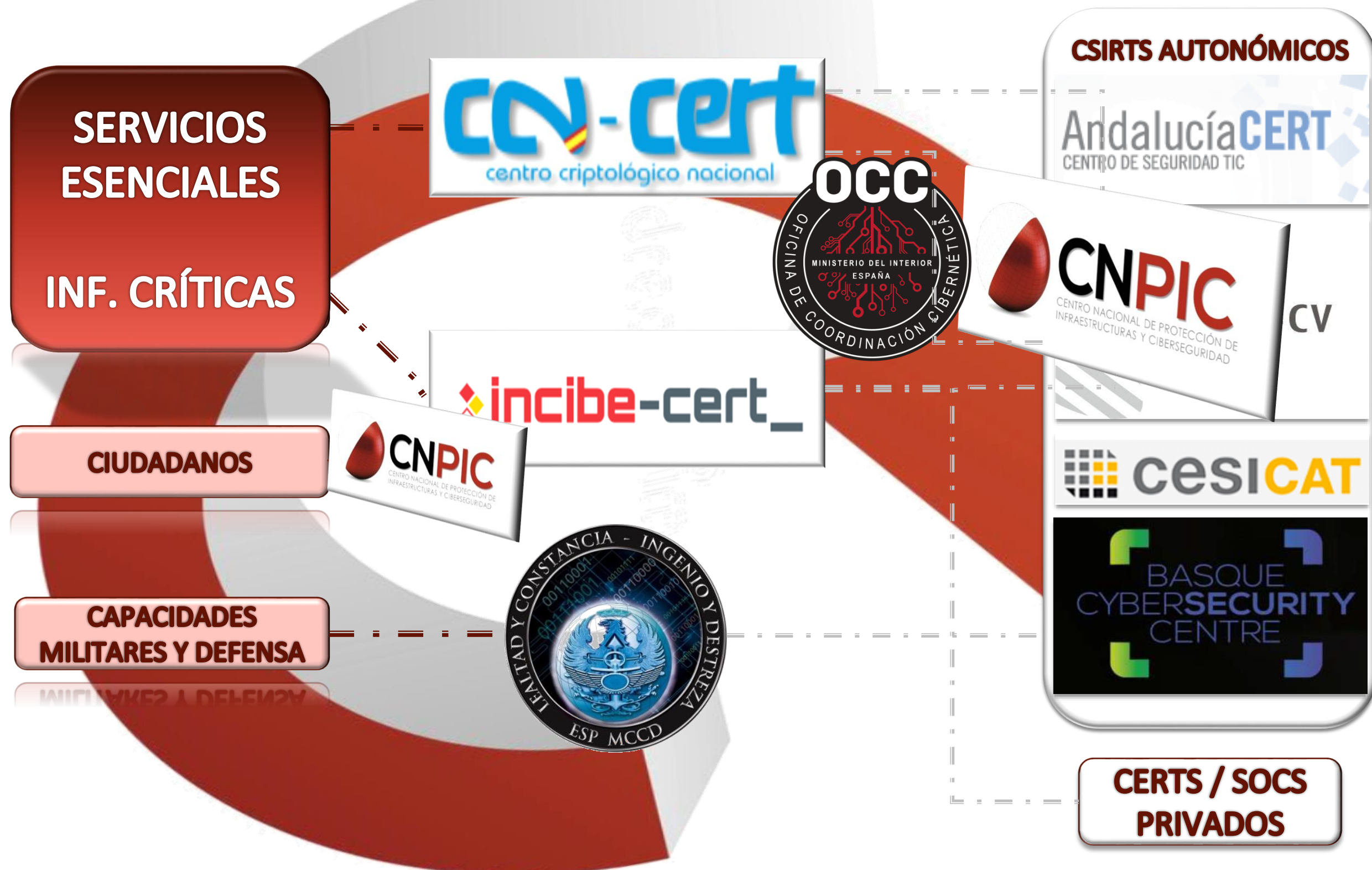
Obligaciones
de
seguridad



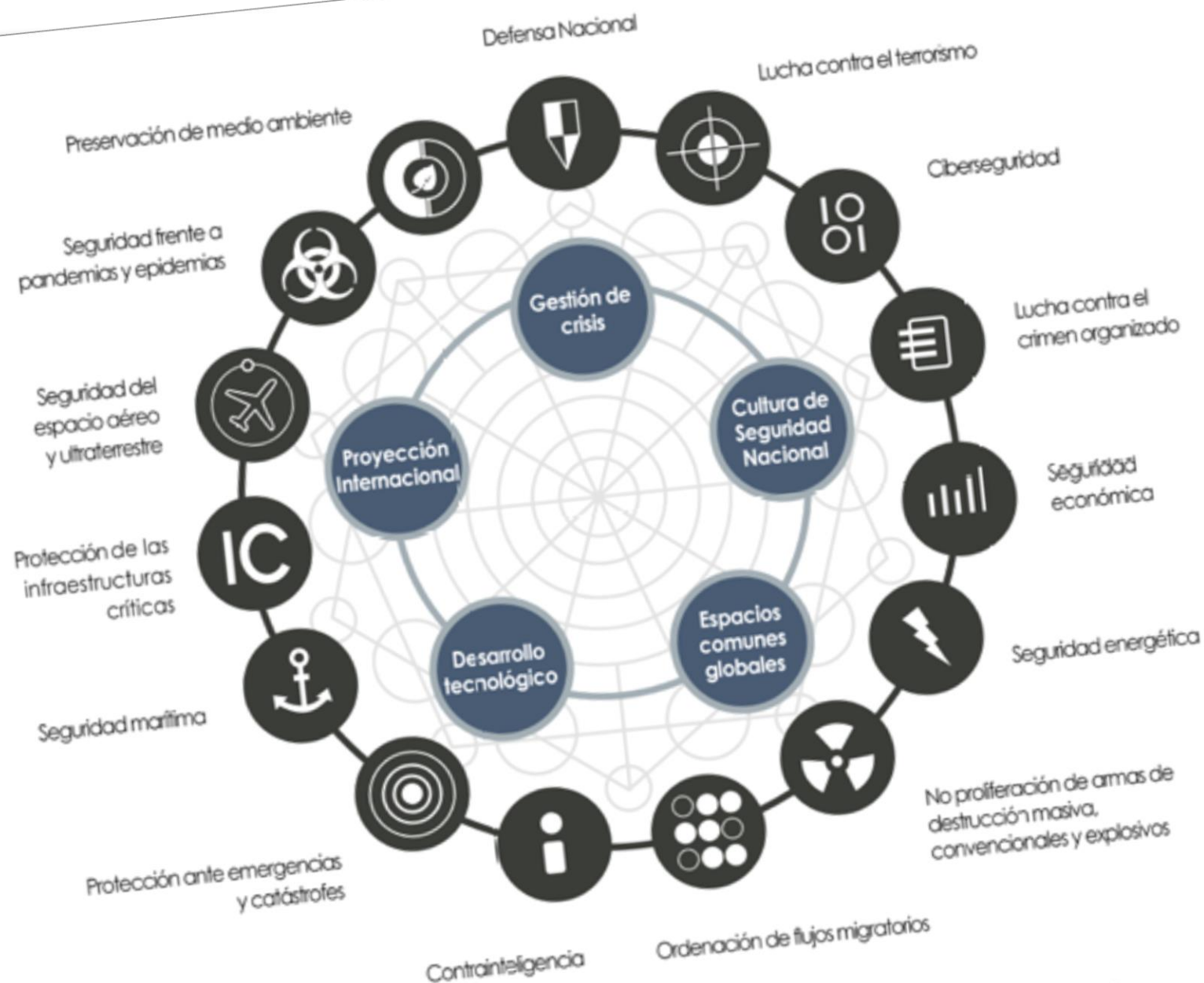
Régimen
sancionador

MODELO ESPAÑOL: CSIRTS DE REFERENCIA





PUNTO DE CONTACTO ÚNICO



OBJETIVOS GENERALES Y ÁMBITOS DE LA **SEGURIDAD NACIONAL**



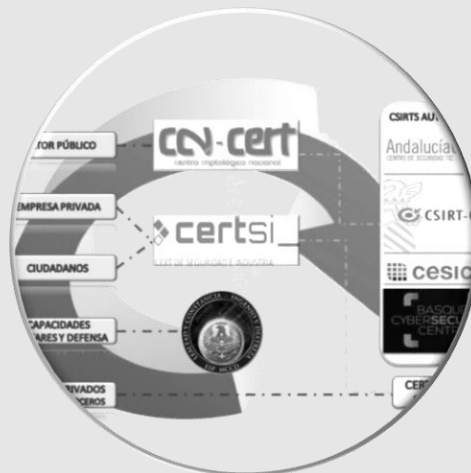
RASGOS PRINCIPALES LEY SRSI



Ámbito de
aplicación



Autoridad
competente



CSIRTS
de
referencia



OBLIGACIONES
DE
SEGURIDAD



Régimen
sancionador

OBLIGACIONES DE SEGURIDAD



OBLIGACIONES DE SEGURIDAD

CRITERIOS A SEGUIR POR OCs

	ACTIVOS	
	FÍSICOS	SIST. INFORMACIÓN
ORGANIZATIVOS / GESTIÓN	ORGANIZATIVAS O DE GESTIÓN	
	Análisis de Riesgos	Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo
	Planificación	Identificación de objetivos y programación de las actividades para conseguirlos
	Definición de roles y responsabilidades	Asignación de responsabilidades en materia de seguridad
	Cuerpo normativo	Elaboración de políticas, estándares y procedimientos de seguridad
	Cumplimiento normativo	Identificación de normativa aplicable y cumplimiento con las mismas
	Certificación, acreditación y evaluación de seguridad	Revisiones periódicas de los sistemas para evaluar su nivel de seguridad
OPERATIVOS / PROCEDIMIENTOS	OPERACIONALES O PROCEDIMENTALES	
	Gestión de activos y de la configuración	Identificación de activos, control de inventario
	Formación y concienciación	Planes de formación y concienciación en seguridad
	Planes de Contingencias	Planes de Contingencias informáticas y físicas
	Supervisión continua	Evaluación / auditoría continua de los sistemas
	Seguridad del personal	Procesos de selección, régimen interno, procedimientos de cese
	Gestión de acceso - Gestión de usuarios	Altas, bajas y modificaciones
	Gestión de acceso - Control de accesos temporales	De personas, vehículos, etc. Identificadores de usuario temporales de los sistemas (mantenimiento...)
	Gestión de acceso - Control de entradas y salidas	Paquetería, correspondencia... Soportes, equipos... e información (DLP, DRM...)
	Procedimientos operacionales del personal de seguridad	Control de rondas de seguridad N/A
	Evacuación	Plan de evacuación N/A
PROTECCIÓN / TÉCNICOS	DE PROTECCIÓN O TÉCNICAS	
Medidas detección y prevención	Medidas de prevención y detección	
	Anti-intrusión	Seguridad física y electrónica perimetral, sistemas de detección perimetral Firewalls, DMZs, IPSs, segmentación de redes, protección del puesto de trabajo, cifrado, VPNs
	Control de accesos (incluye autenticación)	De personas, vehículos, paquetería y mercancías (medios humanos, tarjetas activas, lectores de tarjetas, lectores de matrículas, tornos, scanner, etc.) Registro de usuarios, gestión de privilegios, gestión de claves secretas, revisión de derechos de acceso..., identificadores de usuario acceso a SSII
	Instalación y configuración segura	Configuración segura de los equipos y sistemas con carácter previo a su entrada en operación, mantenimiento de los equipos y control de los cambios. Aseguramiento de las condiciones ambientales para su operación (temperatura, humedad...)
	Protección frente a malware	N/A* Instalación de sistemas anti-virus, antispyware, etc.
	Desarrollo seguro de aplicaciones	N/A* Desarrollo basado en mejores prácticas, auditorías preproducción
Medidas coordinación y monitorizac.	Medidas de coordinación y monitorización	
	Monitorización	Sistemas CCTV (cámaras, video vigilancia) IDSs, sistemas de integridad de software y sistemas de monitorización y gestión de logs
	Coordinación (gestión de incidencias)	Centro de Control, central de alarmas propia, sistemas de comunicación... Creación de equipos de respuesta a incidentes (CSIRT), infraestructuras SOC

IMPLANTACIÓN PSO / PPE



NOTIFICACIÓN DE CIBERINCIDENTES



TIPOLOGÍA	NIVEL REPORTE	VENTANA DE REPORTE
0-day	3, 4 y 5	NOTIFICACIÓN INMEDIATA + INFORME TRAS RESOLUCIÓN
APT	3, 4 y 5	NOTIFICACIÓN INMEDIATA + INFORME TRAS RESOLUCIÓN
Denegación de Servicio (DoS/DDoS)	3, 4 y 5	NOTIFICACIÓN INMEDIATA + INFORME TRAS RESOLUCIÓN
Distribución de malware	3, 4 y 5	NOTIFICACIÓN INMEDIATA + INFORME TRAS RESOLUCIÓN
Acceso a cuentas privilegiadas o de usuarios de alto nivel	4 y 5	EN PROCESO DE RESOLUCIÓN 4H + INFORME TRAS RESOLUCIÓN
Ransomware	4 y 5	NOTIFICACIÓN INMEDIATA
Modificación no autorizada de información	4 y 5	PROCESO DE RESOLUCIÓN 4H
Robo y/o filtración de datos	4 y 5	NOTIFICACIÓN INMEDIATA
Defacement	4 y 5	NOTIFICACIÓN INMEDIATA + INFORME TRAS RESOLUCIÓN
Infección con malware	5	NOTIFICACIÓN 24H + INFORME TRAS RESOLUCIÓN
Escaneo de puertos/red interno	5	NOTIFICACIÓN 24H + INFORME TRAS RESOLUCIÓN
Explotación de vulnerabilidades/compromiso de aplicaciones	5	NOTIFICACIÓN 24H + INFORME TRAS RESOLUCIÓN
Ingeniería social	5	NOTIFICACIÓN 24H + INFORME TRAS RESOLUCIÓN

SEGURIDAD Y NIVELES DE ACTIVACIÓN

Definición

Contexto

Ventana de reporte

Nivel Amenaza PNPIC

Incident notification

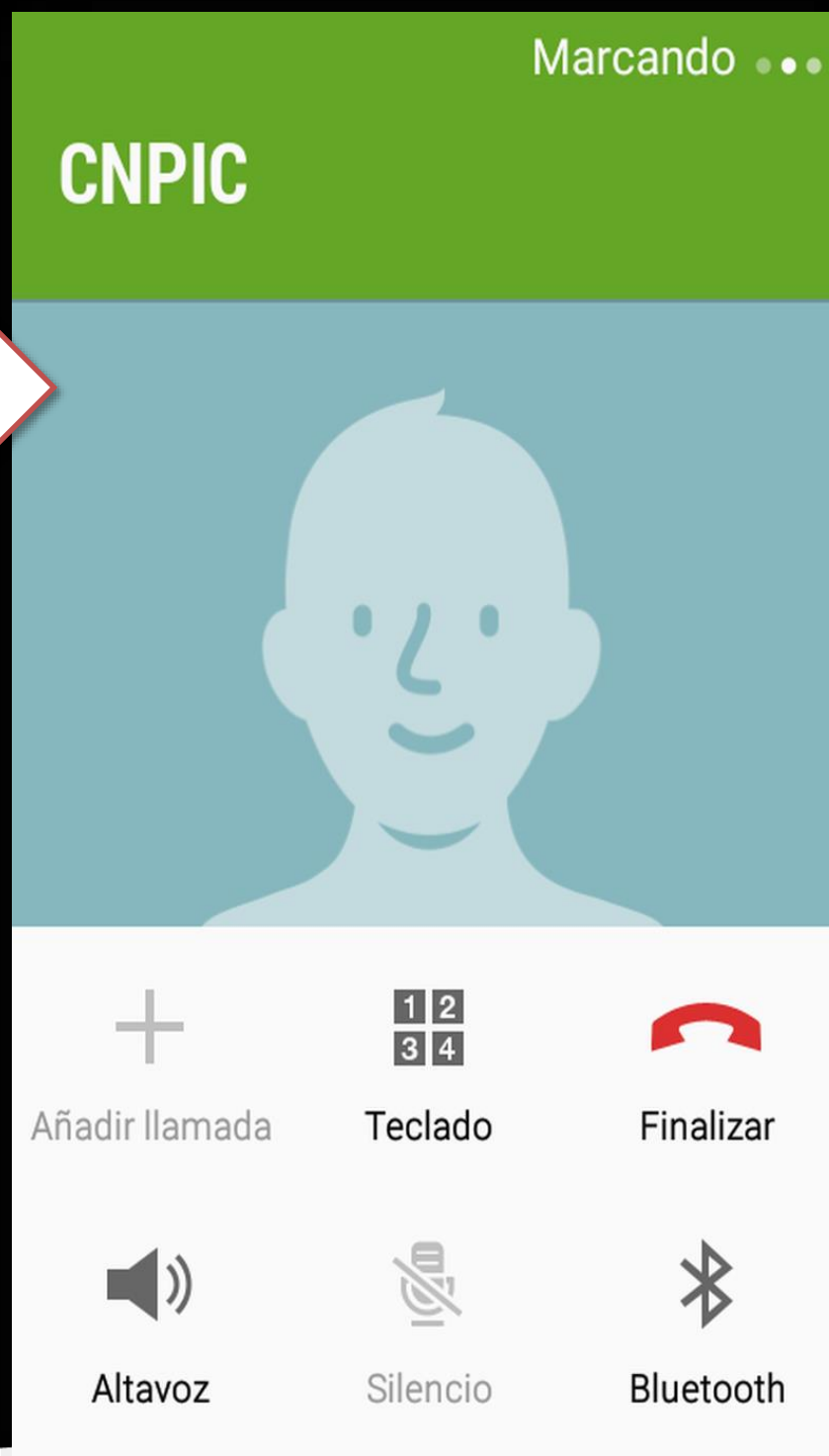


- Most countries are developing:
 - Thresholds
 - Templates and forms
 - Reporting tools and platforms
- Difficult issues:
 - Awareness and culture about reporting
 - Trends and patterns
- Mandatory notification is one small part of the puzzle
 - Voluntary information sharing about threats and near-misses
 - Response by operational teams, CSIRTs etc
 - Drive improvements in the sector

INCIDENTES CON CARACTERES DE DELITO



HERRAMIENTA ALERTPIC



- **LLAMADA DIRECTA**
 - Efectúa una llamada desde el terminal al número pre-establecido de atención de CNPIC
 - Este número se proporciona desde el sistema, por lo que se puede asignar de forma dinámica



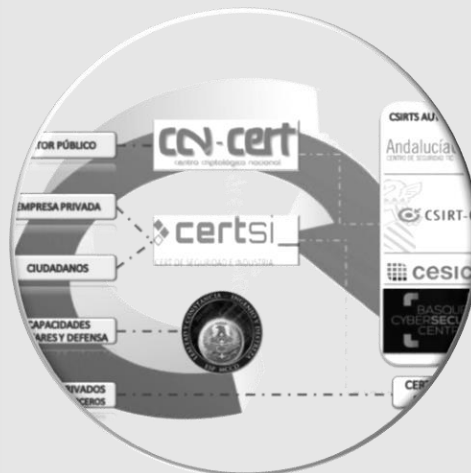
RASGOS PRINCIPALES LEY SRSI



Ámbito de
aplicación



Autoridad
competente



CSIRTs de
referencia



Obligaciones
de
seguridad



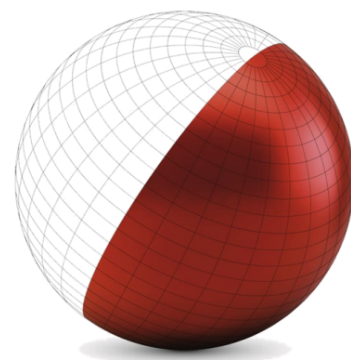
RÉGIMEN
SANCIONADOR

RÉGIMEN SANCIONADOR

**Régimen
sancionador**



**OPERADORES
CRÍTICOS**



CNPIC

CENTRO NACIONAL DE PROTECCIÓN DE
INFRAESTRUCTURAS Y CIBERSEGURIDAD

Centro Tecnológico de Seguridad del Ministerio del Interior
C/ Cabo López Martínez, s/n
28048 El Pardo (Madrid)

WWW.CNPIC.ES