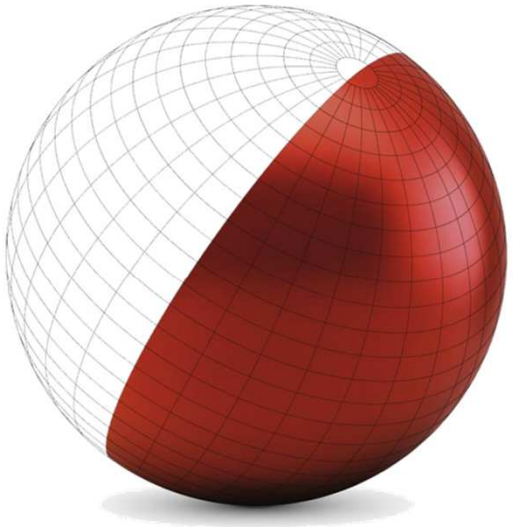
SERVICIO CIBERSEGURIDAD y OCC
(Oficina de Coordinación Cibernética)

SECCIÓN DE PROYECTOS



CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN
DE LAS INFRAESTRUCTURAS CRÍTICAS

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas. El CNPIC depende del Secretario de Estado de Seguridad del Ministerio del Interior, es máximo responsable del Sistema de Protección de las Infraestructuras Críticas nacionales.

El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

certsi_
CERT DE SEGURIDAD E INDUSTRIA

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

El **CERT de Seguridad e Industria (CERTSI_),** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Industria, Energía y Turismo y del Ministerio del Interior. Por **Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015**, el CERTSI_ es el **CERT Nacional** competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las **empresas**, los **ciudadanos** y los **operadores de infraestructuras críticas**.

Operado técnicamente por INCIBE, y bajo la coordinación del CNPIC e INCIBE, el CERTSI_ se constituyó en el año 2012 a través de un **Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información**. Actualmente es regulado mediante **Acuerdo de 21 de octubre de 2015**, suscrito por ambas Secretarías de Estado.

Los operadores de infraestructuras críticas, públicos o privados, designados en virtud de la aplicación de la Ley 8/2011, tienen en el CERTSI_ su punto de referencia para la resolución técnica de incidentes de ciberseguridad que puedan afectar a la prestación de los servicios esenciales, según establece la **Resolución de 8 de septiembre de 2015 (publicada en el BOE de 19 de septiembre), de la Secretaría de Estado de Seguridad**, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.

La Oficina de Coordinación Cibernética (OCC) es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, creado mediante Instrucción del Secretario de Estado de Seguridad 15/2014, de 19 de noviembre. Depende funcionalmente de la Secretaría de Estado de Seguridad y orgánicamente del CNPIC.

La OCC proporciona las capacidades de coordinación técnica entre el CERTSI_ y los órganos subordinados de la Secretaría de Estado de Seguridad y las Fuerzas y Cuerpos de Seguridad del Estado en lo que respecta a las competencias propias del Ministerio del Interior en el campo de la ciberseguridad. La OCC mantiene personal técnico permanentemente integrado en la estructura del CERTSI_.

¿Qué son las Infraestructuras críticas?

En el marco de la Unión Europea son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros.

SECTORES ESTRATÉGICOS:

12 SECTORES ESTRATÉGICOS

Energía

Financiero

Salud

Alimentación

Industria Química

TIC

Industria Nuclear

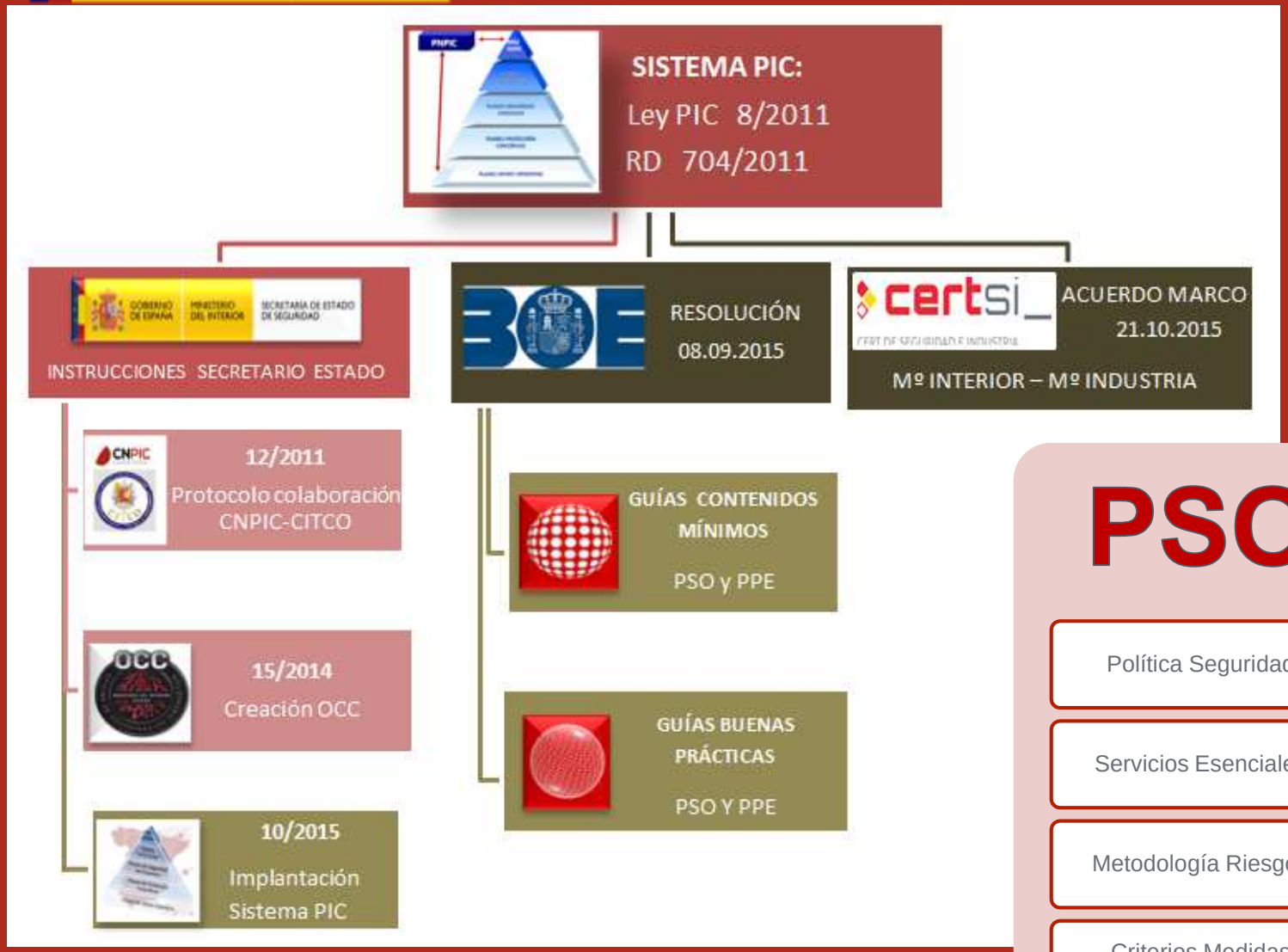
Agua

Transporte

Administración

Espacio

Instalaciones de Investigación



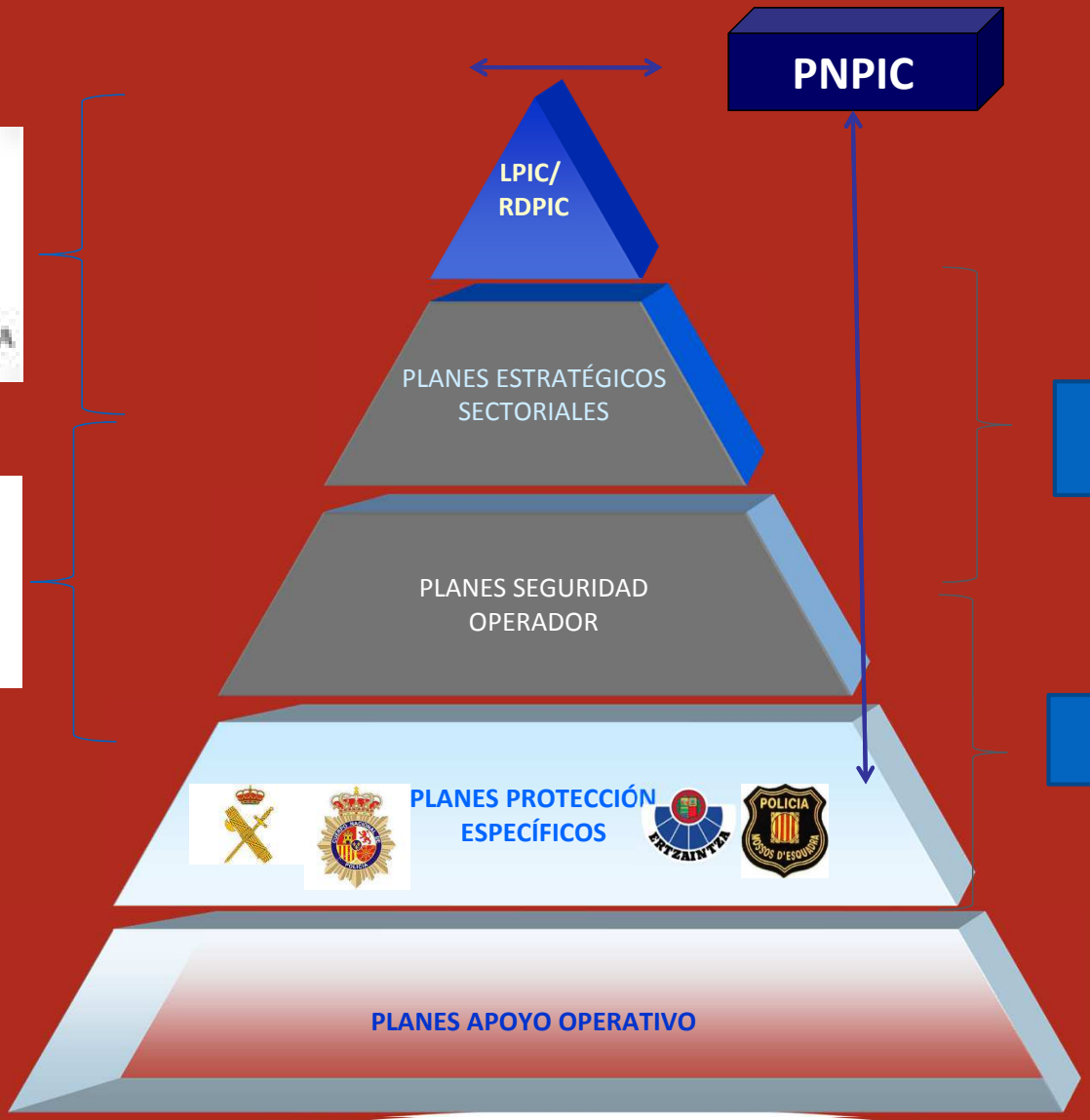
PSO

- Política Seguridad
- Servicios Esenciales
- Metodología Riesgos
- Criterios Medidas Seguridad

PPE

- Descripción infraestructura
- Resultados análisis Riesgos
  - Amenazas
  - Medidas Seguridad
- Plan Acción

ELEMENTOS DE PLANIFICACIÓN

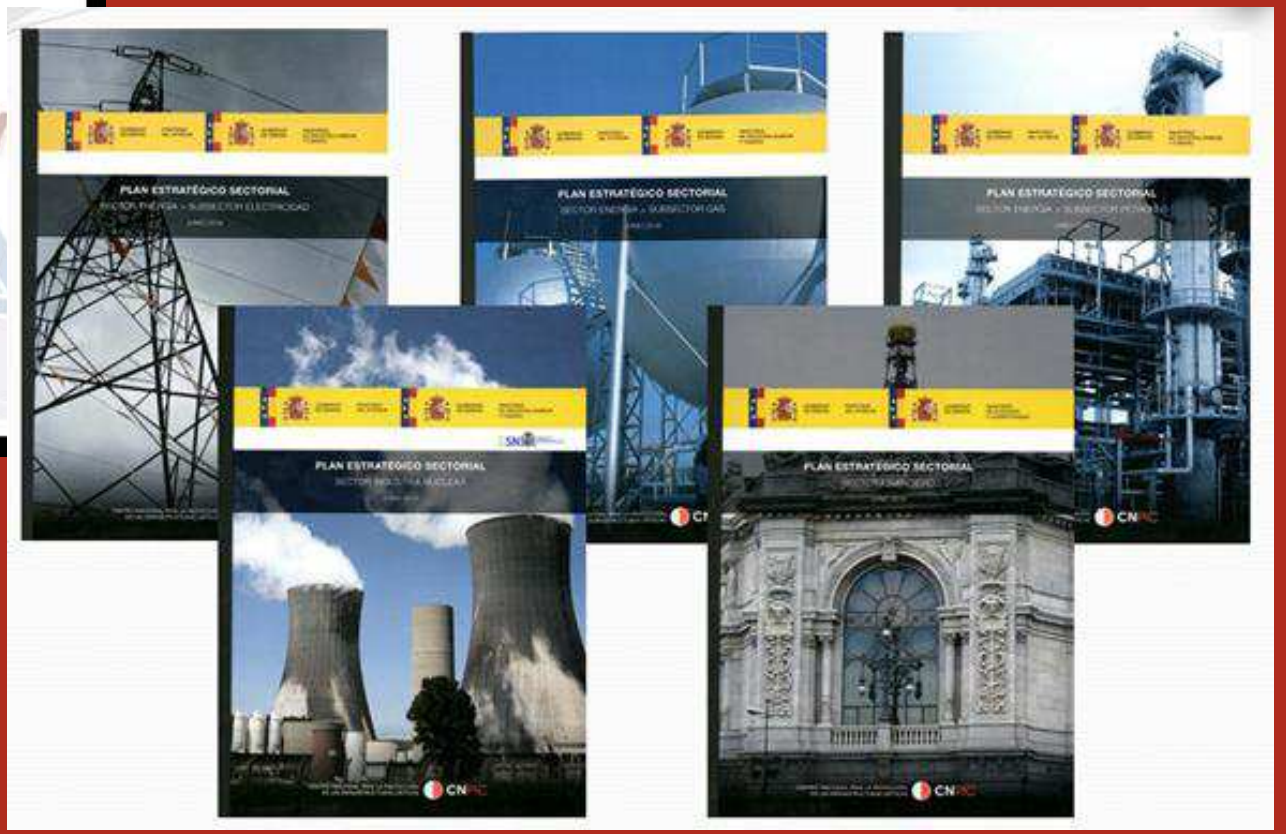


ESTRATÉGICO

OPERATIVO

Organigrama: La estructura del CNPIC tiene el objetivo de conseguir una mayor eficiencia en la gestión

ACTIVIDADES DEL CNPIC



ACTIVIDADES

Nivel de Alerta Antiterrorista: una escala compuesta por varios niveles complementarios, cada uno de los cuales se encuentra asociado a un grado de riesgo, en función de la valoración de la amenaza terrorista que se aprecie en cada momento.

Ciberamenaza emergente: Hackers iraníes atacan infraestructura crítica a nivel mundial

España activará por primera vez un dispositivo de ciberseguridad

19 junio 2014 - ACTUALIDAD - Etiquetas: CIBERDEFENSA, CORONACION, DISPOSITIVO, ESPAÑA - sin comentarios

El primer dispositivo de ciberseguridad y control de la red en España funcionará durante la proclamación de este jueves de Felipe VI como nuevo Rey. El objetivo es garantizar la coordinación operativa de todos los órganos implicados en relación a la seguridad cibernética para, en mayor medida, garantizar el correcto desarrollo de los actos y la seguridad de los participantes y asistentes al mismo.

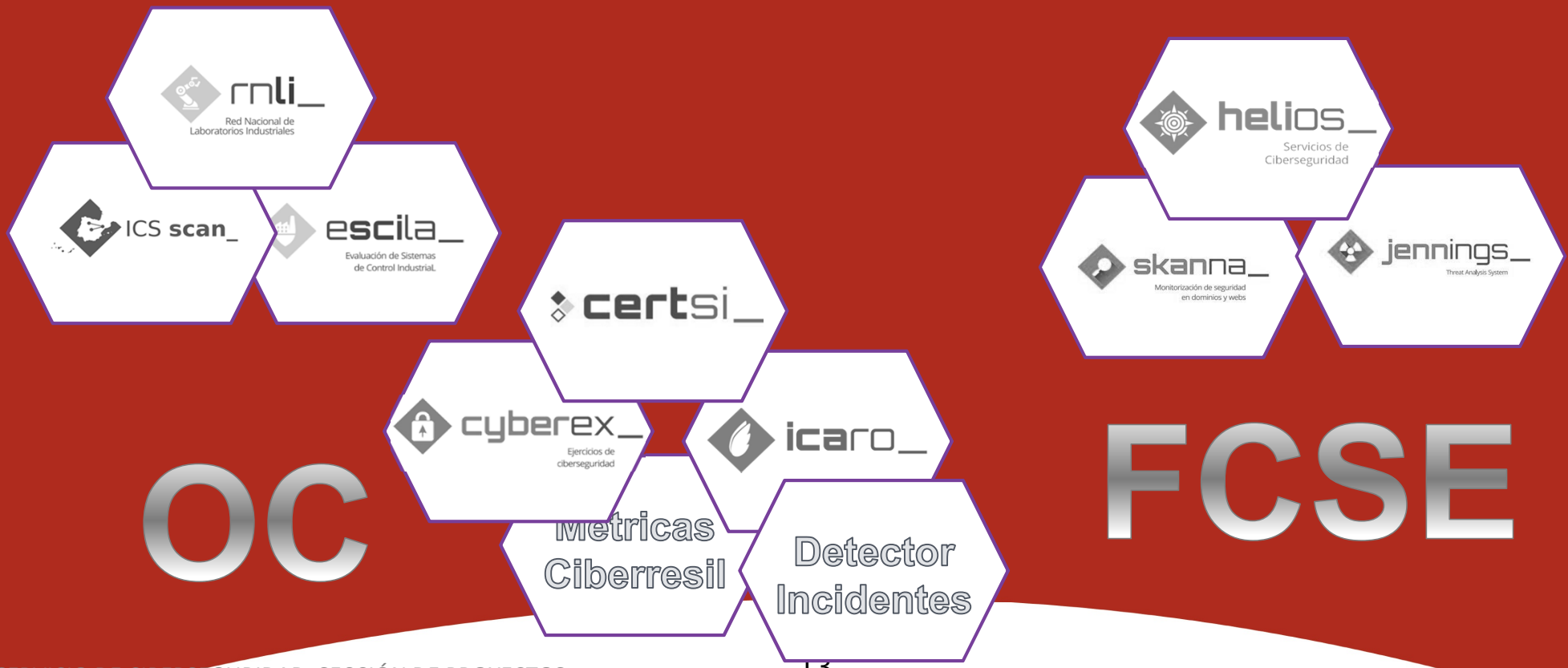
...de "reforzar la protección de

El primer ciberataque de la historia contra una eléctrica pone en alerta a todo el sector

Stuxnet: El virus capaz de crear "el caos absoluto"

PROYECTOS

Iniciativas de INCIBE y CNPIC para mejorar el nivel de seguridad de las infraestructuras críticas y las FFCCSE en España.



Métricas Ciberresil

Ciberresiliencia: Consulta de métricas e indicadores

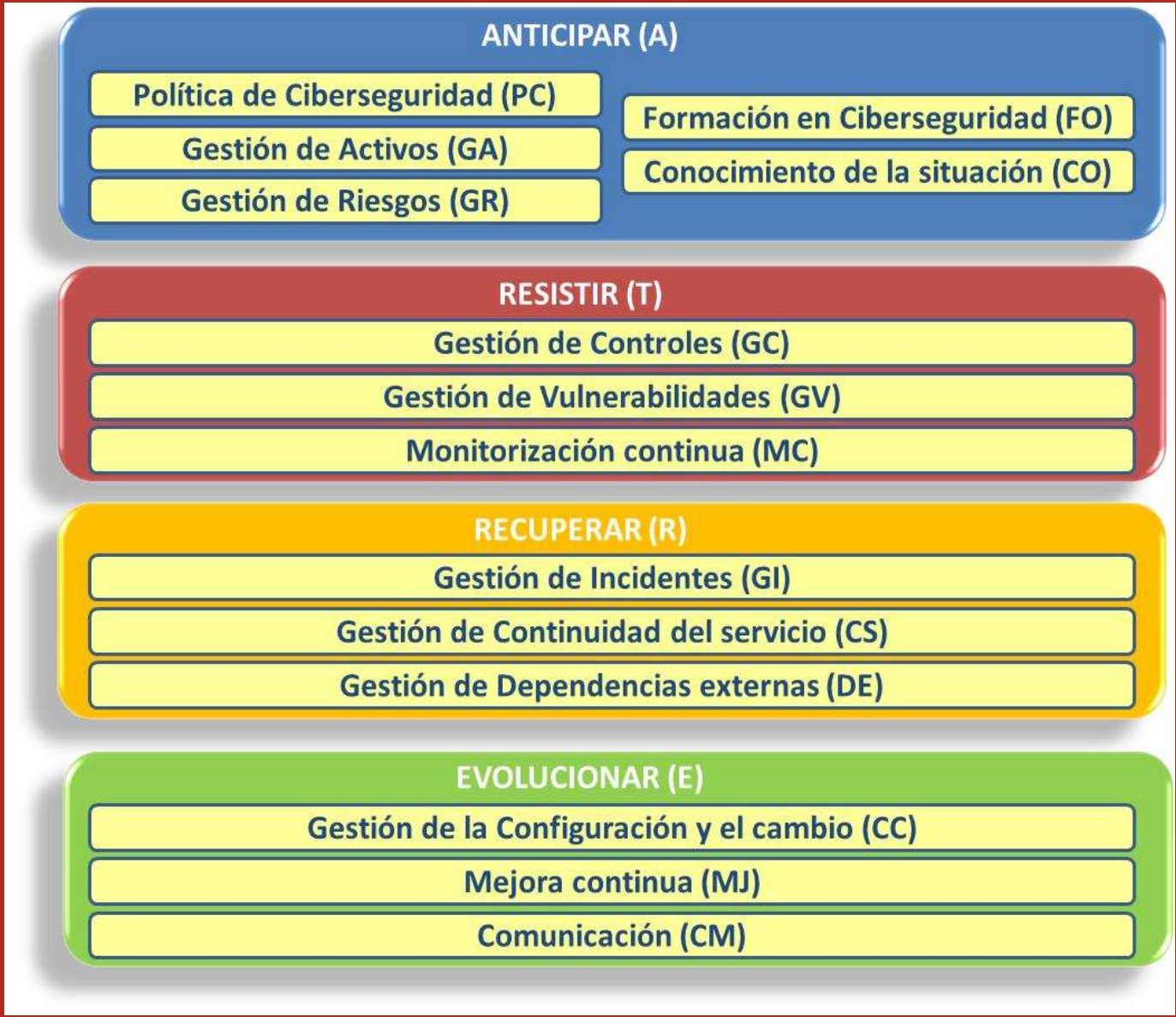
- Una de las actuaciones encomendadas al CERTSI, es la elaboración de un conjunto de métricas e indicadores. Pretendemos medir la capacidad de ciberresiliencia de los distintos operadores estratégicos, de manera agregada, ante distintos ataques, amenazas o incidentes que puedan sufrir.

- Ciberresiliencia, es la capacidad de un proceso, negocio, organización o nación para anticipar, resistir, recuperarse y evolucionar, para mejorar sus capacidades frente a condiciones adversas, estrés frente a ciberataques a los recursos necesarios para funcionar.

PROYECTOS

Métricas Ciberresil

Marco de trabajo de ciberresiliencia



PROYECTOS

- Ciberejercicios: Alcance, metodología y el rol de CERTSI.

CYBEX 2012

- Heterogéneo, multisectorial
- Simulación de ataque técnico a servicios perimetrales
- Evaluación de la capacidades técnicas y organizativas

CyberEx 2013

- Heterogéneo, multisectorial
- Simulación y ataque técnico al perímetro y WiFi
- Evaluación de la capacidades técnicas y organizativas
- Simulación de análisis técnico de un incidente

CyberEx 2014

- Orientado a operadores estratégicos.
- Simulaciones generalistas.

CyberEx 2015

- Ciberejercicio centrado en operadores estratégicos y críticos.
- Aproximación hacia un ejercicio sectorial enfocado en el negocio.

PROYECTOS

icaro_

ICARO: Compartir los IOC del malware conocido para facilitar la detección

icaro_

- Anonimización de la información compartida.
- Nodos de entrada para alimentación.
- Nodos de salida para obtención de información.
- Análisis de la información por parte de CERTSI

MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

PROYECTOS EUROPEOS

CIISC-T2 Critical Infrastructure: Improvement of Security Control against the Terrorist Threat

II Jornadas PSCIC

III Jornadas PSCIC

PROYECTOS EUROPEOS

Final Conference SCADA LAB

SCADA Laboratory and test bed as a service for Critical Infrastructure protection
Brussels (Belgium), 9th July 2014

Summary

- Must focus on education, training and awareness aspects of our current and future cyber security area
- Collaboration is essential. No single government is going to solve this problem
- Defence in depth and security by design
- Implementing this project

PROYECTOS

RNLI

- Potenciar la oferta y la demanda de la ciberseguridad en los entornos industriales a nivel nacional
- Promoción de capacidades de los laboratorios
- Fomento de la colaboración y cooperación entre los actores involucrados: nuevos servicios
- Elevar el nivel de seguridad de las infraestructuras soportadas por Sistemas de Control Industrial.

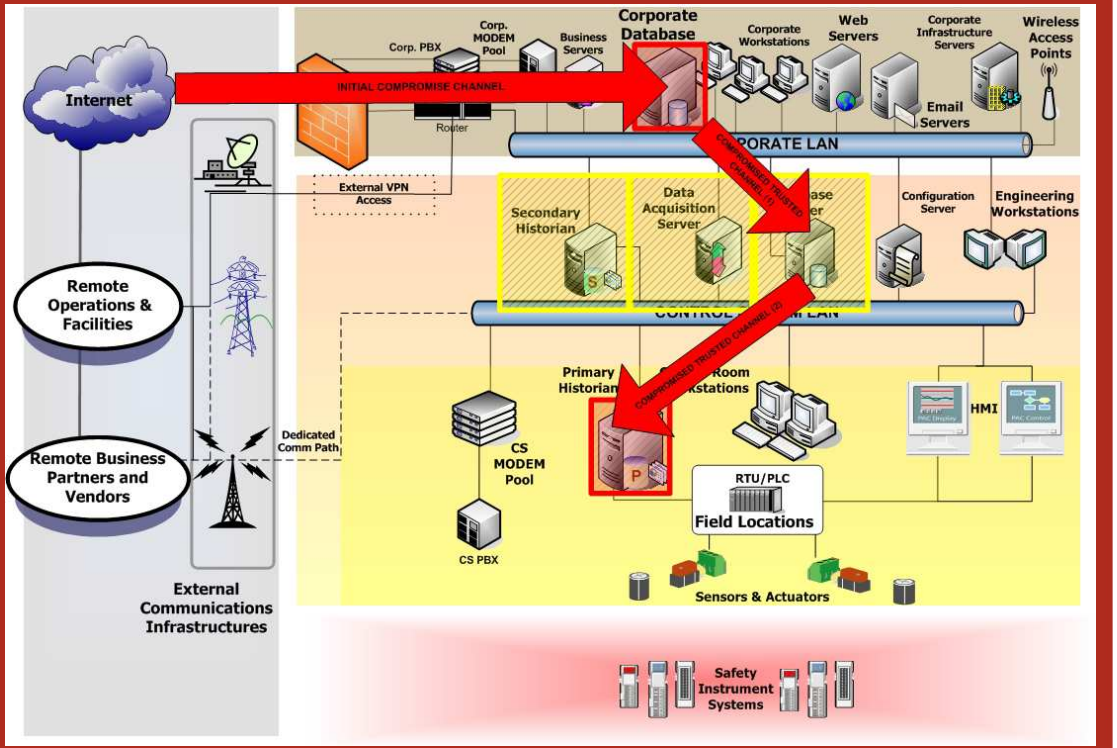
PROYECTOS

RNLI

rnli_
Red Nacional de Laboratorios Industriales

Objetivos:

- Elevar el nivel de seguridad de las infraestructuras soportadas por sistemas de control industrial.
- Potenciar un punto de unión entre la oferta y la demanda de la seguridad en los entornos industriales a nivel nacional.
- Poner a disposición de la comunidad, información acerca de infraestructuras nacionales.

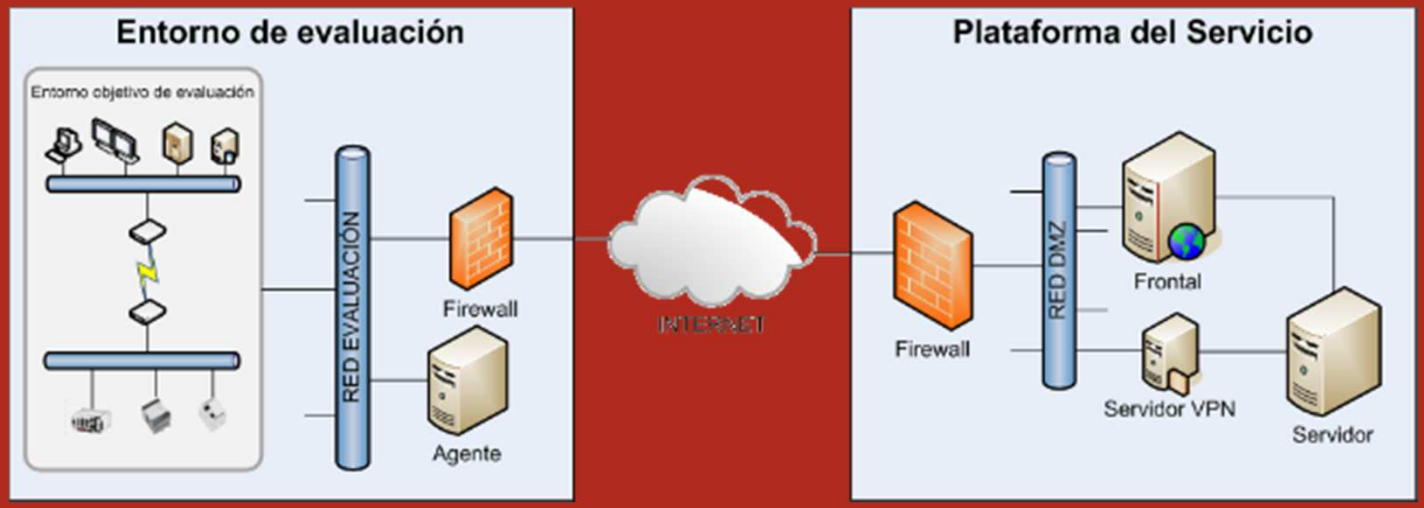


Fuente: DHS Department of Homeland Security

escila_
Evaluación de Sistemas de Control Industrial

ESCILA: Evaluación de sistemas de control industrial y automatización

- Proceso ágil, sencillo y repetible.



- Evaluación inicial de los riesgos de seguridad más importantes de un componente industrial.
- Posibilidades de un análisis técnico más profundo.

PROYECTOS

ICS_SCAN: Escaneo, monitorización y recopilación datos de servicios ICS/SCADA

- Identificación de vulnerabilidades y configuraciones incorrectas en servicios ics /scada. Notificaciones

- Repositorio de información (inteligencia):

  - Fabricantes, servicios, protocolos más utilizados
  - Útil para el desarrollo de posteriores herramientas: Honepots/Honeynets
  - Investigación vulnerabilidades en firmware/servicios comunes (PLC, RTUs, etc.)

PROYECTOS PARA FFCCSE

- ***Inteligencia.***
- ***Análisis de amenazas.***
- ***Vigilancia de dominios.***
- ***Riesgo nacional.***
- ***Análisis Avanzados.***
- ***Chequeo de claves.***
- ***Monitorización de redes anónimas.***
- ***Análisis de ciberataques.***
- ***Servicios vulnerables.***
- ***Panel de botnets.***

Gracias por su atención

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN
DE LAS INFRAESTRUCTURAS CRÍTICAS

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

WWW.CNPIC.ES