MEMORIA
2016

CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN
DE LAS INFRAESTRUCTURAS CRÍTICAS

MEMORIA CNPIC 2016

INTRODUCCIÓN

El CNPIC es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas ubicadas en territorio nacional. Siendo el Secretario de Estado de Seguridad, del Ministerio del Interior, el máximo responsable del sistema de Protección de las Infraestructuras Críticas nacionales.

Es el Centro pionero en España en el concepto de seguridad integral, llevando a cabo importantes avances en el campo de la protección de las infraestructuras críticas en distintos ámbitos como el normativo, con la implantación de instrumentos de planificación o de planes de seguridad, y también en materia de ciberseguridad, etc...

Durante el año 2016, el CNPIC ha seguido progresando en la mejora del Sistema de Protección de Infraestructuras Críticas, para garantizar la adecuada prestación de los servicios esenciales. Destacándose entre sus actividades:

- Inauguración por el Ministro del Interior, de las nuevas instalaciones del CNPIC, en el Centro Tecnológico de Seguridad (CETSE), con sede en El Pardo.
- Haber conseguido un marco normativo que contribuya a despejar y definir las incógnitas que plantea la comunidad de la seguridad española.
- Mantener y actualizar el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) como instrumento de programación del Estado, elaborado por la Secretaría de Estado de Seguridad.
- Cumplir y supervisar el mandato de la Ley 8/2011, de 28 de abril y del Real Decreto 704/2011 de protección de las infraestructuras críticas, contribuyendo para mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad y con ello garantizar el bienestar de todos los ciudadanos, coordinando y promoviendo el correcto funcionamiento del Sistema PIC.
- Disponer de la Oficina de Coordinación Cibernética (OCC) como punto de contacto nacional de información con la Comisión Europea y los Estados miembros en lo relativo a los ataques contra los sistemas de información, permitiendo promover y garantizar la ciberseguridad, por su transversalidad como nexo de unión que comunica todos los entornos de la vida moderna.
- Fortalecer las capacidades humanas y tecnológicas de las Unidades de las Fuerzas y Cuerpos de Seguridad del Estado dedicadas al ciberterrorismo y a la ciberdelincuencia.
- Disponer del CERT de Seguridad e Industria para el servicio de los operadores estratégicos y del sector privado.
- El CNPIC es el Punto de Contacto del Estado Español designado en el ámbito de protección de las Infraestructuras Críticas, por ello se ha reforzado la idea de colaboración y cooperación internacional con el objetivo, entre otros, de establecer alianzas en el ámbito de la ciberseguridad.

- Promover la cooperación público-privada, la confianza mútua entre el sector público y privado y la responsabilidad compartida en el ámbito de la seguridad.
- Convertir al Sistema PIC español en un modelo de referencia a nivel mundial, habiendo sido sus instalaciones objeto de visita de las delegaciones lationamericanas de Argentina, México, Brasil y Chile interesados en conocer en profundidad el modelo PIC instaurado en España.

ÍNDICE

1 ¿QUÉ ES EL CNPIC?

El **CNPIC** fue creado el 2 de noviembre de 2007 mediante Acuerdo de Consejo de Ministros, 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 la Infraestructuras Críticas.

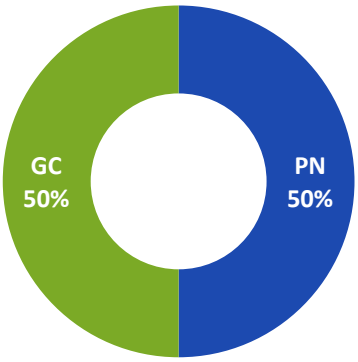
La legislación española sobre protección de infraestructuras críticas establece la necesidad de garantizar la adecuada prestación de los servicios esenciales a través de mecanismos que posibiliten la **seguridad integral** de este tipo de infraestructuras. Esta tarea está encomendada al **CNPIC**, que asiste al Secretario de Estado de Seguridad, responsable máximo del Sistema de Protección de las Infraestructuras Críticas (en adelante **Sistema PIC**), en sus funciones. En este Sistema, del cual el **CNPIC** es pieza central, se integran tanto otros departamentos de la Administración Pública española, como operadores y compañías que prestan servicios esenciales, habiéndose consagrado en pocos años un modelo de **cooperación público-privada** inédito hasta hoy en la seguridad española, que ha convertido a **España en una referencia a nivel internacional**.

1.1 ORGANIGRAMA

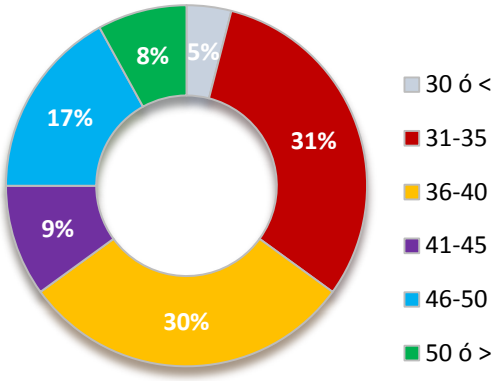
1.2 PLANTILLA

El **CNPIC** lo integran funcionarios procedentes de las Fuerzas y Cuerpos de Seguridad del Estado, con la siguiente distribución:

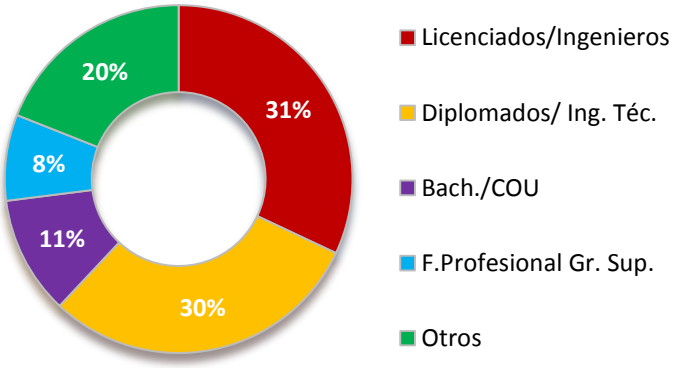
COMPOSICIÓN CNPIC



DISTRIBUCIÓN POR EDAD



FORMACIÓN DEL PERSONAL



1.3 NUEVA SEDE

En el mes de abril, fueron inauguradas por el Ministro del Interior, las nuevas instalaciones del Centro Tecnológico de Seguridad (CETSE), que alojan tanto al Centro Nacional de Protección de Infraestructuras y Ciberseguridad (**CNPIC**) como a la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), ambos órganos de la Secretaría de Estado de Seguridad (SES), y que concentra las unidades tecnológicas de seguridad del Ministerio del Interior, dependientes de la Secretaría de Estado de Seguridad.

El Centro es un edificio moderno que dispone de las últimas innovaciones en sistemas de información y comunicación. Cuenta con tres plantas, 63 zonas de oficina, 4 dependencias en la zona recepción, 72 puestos en la zona común, una sala con 6 puestos, salas de formación y reuniones, salón de actos, cafetería, salas de espera, vestuarios, almacenes mantenimiento y un helipuerto, que facilitarán el desarrollo de las tareas encomendadas a los componentes de las Fuerzas y Cuerpos de Seguridad del Estado, que desempeñan allí sus funciones. Además cuenta con dos salas ZAR (Zona de Acceso Restringido) para asegurar la protección de la información clasificada.

2 ACTIVIDADES DEL CNPIC

2.1. DESARROLLO NORMATIVO

Durante 2016 se han emitido las siguientes instrucciones:

➢ La **INSTRUCCIÓN 1/2016** de la Secretaría de Estado de Seguridad del 10 de febrero de 2016, por el que se actualiza el **PLAN NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (PNPIC).** Dicha instrucción está íntimamente ligada a la Instrucción 3/2015 dictada por la Secretaría de Estado de Seguridad, por la que se actualiza el **Plan de Prevención y Protección Antiterrorista (PPPA)**.

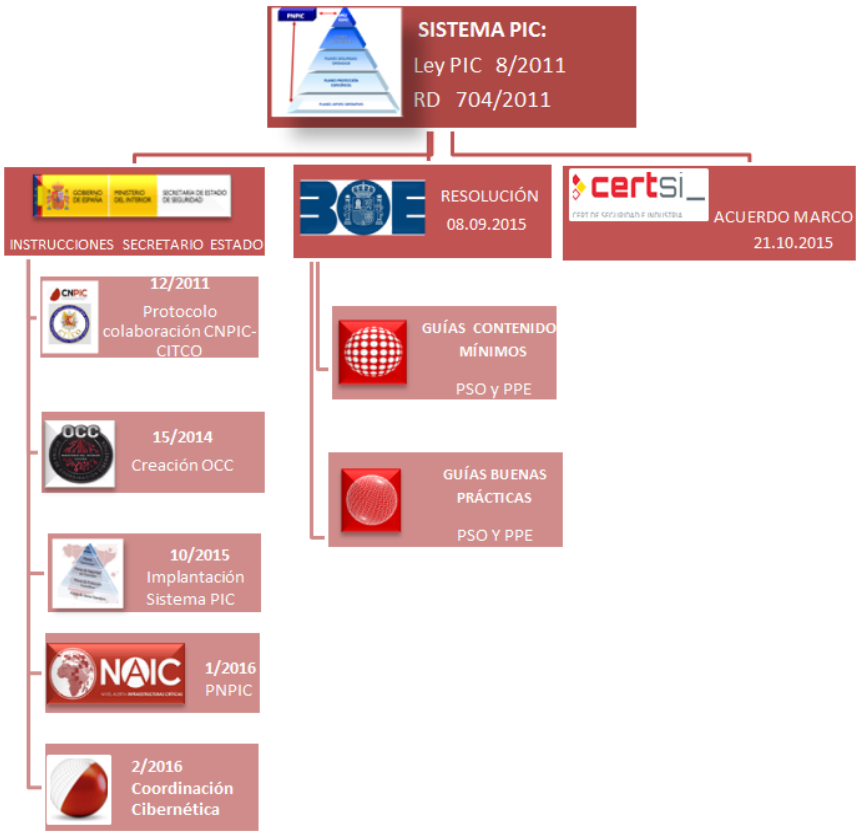
El **PNPIC** supone la culminación del Sistema de Protección de Infraestructuras Críticas emanado de la Ley 8/2011, PIC, y la implantación de todas las herramientas de planificación previstas en dicha norma. Significa la puesta en marcha de medidas operativas concretas sobre dos presupuestos fundamentales:

- La inclusión de la figura del operador crítico como partícipe del sistema de seguridad nacional.
- La inclusión de medidas de ciberseguridad, dando contenido al concepto de seguridad integral.

Los principales actores participantes en el **PNPIC** son:

- Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).
- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO)
- Fuerzas y Cuerpos de Seguridad del Estado (FCSE)
- Operadores Críticos (OC)

➢ **INSTRUCCIÓN 2/2016**, de 20 de mayo, de la Secretaria de Estado de Seguridad, por la que se regula la **Coordinación en materia de Ciberseguridad**, designando a la **Oficina de Coordinación Cibernética (OCC)** del **CNPIC** como **Punto de Contacto Nacional** de Coordinación operativa para el intercambio de Información con la Comisión Europea y los Estados miembros, en el marco de lo establecido en el artículo 13 de la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, y sin perjuicio de lo establecido en la Instrucción 15/2014 de creación de la OCC. Con la publicación de esta instrucción se amplía el ámbito de actuación de la OCC, constituyéndose en el **punto de contacto las 24 horas al día**, dando respuesta dentro de los plazos estipulados en la Directiva y con enlace permanente con las Fuerzas y Cuerpos de Seguridad del Estado. Asimismo, la OCC será responsable del intercambio de información sobre ciberdelitos con terceros países, y órganos internacionales y de la Unión Europea, cuando así lo requieran las autoridades competentes.



2.2 PLANES ESTRATÉGICOS SECTORIALES (PES)

El desarrollo de los **Planes Estratégicos Sectoriales**, nos permite conocer las infraestruccturas estratégicas, y en particular, las infraestructuras críticas nacionales sobre las que se asientan los servicios esenciales para la sociedad, así como los operadores, propietarios o gestores de las mismas, las vunerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas para su funcionamiento.

En el 2016 **se han finalizado** los PES relativos a los **Sectores de la Industria Química y del Espacio**, siendo aprobados el 14 de julio de 2016, por la Comisión Nacional para la Protección de Infraestructuras Críticas (Comisión PIC).

Los Planes Estratégicos aprobados en el 2016, han incluido una particularidad en relación a los realizados anteriormente (energía, industria nuclear, financiero, transporte y agua), que ha sido la introducción de las **medidas organizativas** propuestas con la actualización del **Plan Nacional de Protección de Infraestructuras Críticas** (**PNPIC**), en consonacia con el nuevo Plan Nacional de Prevención y Protección Antiterrorista.

PES aprobados/finalizados 2016

- SECTOR INDUSTRIA QUÍMICA
- SECTOR ESPACIO

En el proceso de implantación del Sistema PIC, se han **elaborado y aprobado, desde su inicio en 2014, 12 PES**, todos ellos con clasificación de **CONFIDENCIAL**:

FASES DE IMPLANTACIÓN DEL SISTEMA PIC

1ª FASE: 5

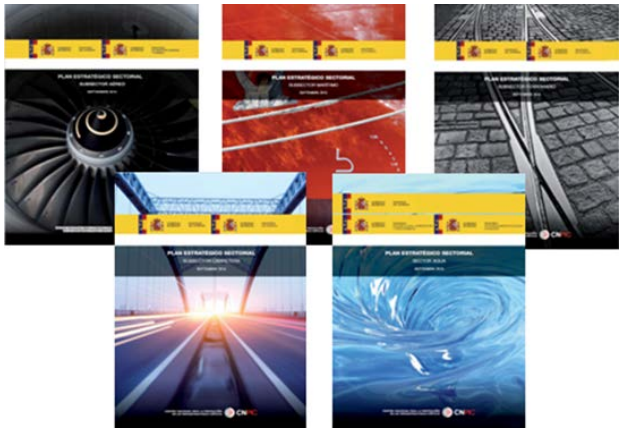
SECTOR ENERGÍA: electricidad, gas y petróleo

SECTOR INDUSTRIA NUCLEAR

SECTOR FINANCIERO

Aprobados por la COMISIÓN PIC

14 julio 2014



2ª FASE: 5

SECTOR TRANSPORTE: aéreo, marítimo, ferroviario y carreteras.

SECTOR AGUA

Aprobados por la COMISIÓN PIC

10 septiembre 2015

3ª FASE: 2

SECTOR INDUSTRIA QUÍMICA

SECTOR ESPACIO

Aprobados por la COMISIÓN PIC

14 julio 2016

Además en el **Catálogo Nacional de Infraestructuras Estratégicas** se almacena, entre otra información, toda la relacionada con los operadores y las infraestructuras críticas. Dicho Catálogo tiene el carácter de SECRETO, siendo custodiado, gestionado y mantenido por el **CNPIC**.

Hasta el momento se ha realizado el nombramiento de **106 operadores críticos** y la identificación de varios cientos de infraestructuras críticas, de los sectores de la Energía (electricidad, gas y petróleo), Industria Nuclear, Sistema Financiero, Transporte (aéreo, marítimo, carretera y ferrocarril), Agua, Industria Química y Espacio.

2.3 PLANES DE SEGURIDAD DEL OPERADOR (PSO)

Para? Concentrar las **políticas generales en el ámbito de la seguridad** que los **operadores** de infraestructuras críticas tienen a la hora de garantizar la **protección y la seguridad del conjunto de infraestructuras** que son de su propiedad o gestión.

Cuáles? En 2016 se han iniciado los **Planes de Seguridad del Operador (PSO),** correspondientes a la 2ª Fase de implantación del Sistema PIC.

2.4 PLANES DE PROTECCIÓN ESPECÍFICOS (PPE)

Para? Documento operativo donde se definen **las medidas de protección concretas que garantizan la seguridad integral (física y lógica)** de aquellas infraestructuras identificadas como críticas.

Cuáles? Durante 2016 se aprobaron los planes correspondientes a los sectores de la Energía (electricidad, gas y petróleo) y Sistema Financiero.

Quiénes? En el desarrollo del sistema de planificación e implantación territorial de los PPE han intervenido las **19 Delegaciones de Gobierno, así como los cuerpos policiales** del territorio donde se encuentran enclavadas las diferentes infraestructuras críticas de los sectores mencionados.

2.5 CENTRO DE COORDINACIÓN Y ALERTA (CECOA)

Departamento ubicado en el CNPIC que trabaja con la información remitida por operadores y FCS, relativos a las infraestructuras y personal que lo gestiona. Durante 2016 el CECOA ha realizado las siguientes actuaciones:

CECOA - 2016

Nº llamadas recibidas de consultas PI3	250
Número de correos enviados y recibidos 24H	+1.200
Número y tipo de incidentes gestionados	Operativa PI3 y Simulacro de REE
Nº de infraestructuras incorporadas a PI3	+ de 1.500

2.6 GRUPOS DE TRABAJO ESTABLECIDOS Y REUNIONES MANTENIDAS

2.6.1 GRUPO DE TRABAJO PES

Para la elaboración de los PES se han formado grupos de trabajo y se han realizado numerosas reuniones. Colaborando en la confección de los documentos: ministerios y otros organismos públicos o privados, como: empresas/operadores, asociaciones profesionales, etc. Desgranándose de la siguiente manera:

SECTOR INDUSTRIA QUÍMICA

Grupos de trabajo	1
Nº de reuniones	8
Nº Asistentes	11
ORGANISMOS COLABORADORES	
Públicos	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
	DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL
Privados	FEIQUE

SECTOR ESPACIO

Grupos de trabajo	1
Nº de reuniones	9
Nº Asistentes	10
ORGANISMOS COLABORADORES	
Públicos	MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
	MINISTERIO DE DEFENSA
	INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS
	CNI
Privados	INTA

2.6.2 GRUPO DE TRABAJO INTERDEPARTAMENTAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS (GTIPIC)

El **Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (GTIPIC)**, se ha reunido en cuatro ocasiones durante el 2016, en las siguientes fechas:

- 01/06/2016 – Aprobar los borradores de los Planes Estratégicos del Sector de la Industria Química y del Espacio, para su presentación a la Comisión Nacional PIC.
- 16/06/2016 – Proponer la designación de los operadores críticos de los sectores mencionados a la Comisión Nacional.
- 28/06/2016 – Elaborar y aprobar los borradores de los Capítulos I y II del Plan Estratégico del Sector de las Tecnoclogías de la Información y de la Comunicación (TIC).

- 15/12/2016 – Presentar y aprobar el borrador de la Memoria Anual de Actividades 2015-2016 de la Comisión Nacional PIC, así como la preparación de la reunión de la Comisión.

En estas reuniones han participado diferentes departamentos ministeriales involucrados en el ámbito de las infraestructuras críticas, las CCAA con competencias delegadas en materia de seguridad (Cataluña, Navarra y País Vasco) y la Federación Española de Municipios y Provincias (FEMP).

2.6.3 COMISIÓN NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS – (COMISIÓN PIC)

La Comisión Nacional para la Protección de las Infraestructuras Críticas (Comisión PIC), presidida por el por el Secretario de Estado de Seguridad, se reunió el **14 de julio de 2016**, con las actuaciones específicas:

- Aprobación de los Planes Estratégicos Sectoriales (PES) de la Industria Química y del Espacio
- Designación de los Operadores Críticos (OC) de los sectores afectados
- Aprobación de la Memoria Anual de Actividades 2015-2016 de la Comisión PIC

2.6.4 MESA DE COORDINACIÓN PIC

Constituida el **15 de junio de 2016,** fecha en la que tuvo lugar la primera reunión que fue presidida por el Director del Gabinete de Coordinación y Estudios de la Secretaria de Estado de Seguridad. Se creó en el marco de la Instrucción nº 1/2016, de la Secretaría de Estado de Seguridad, por la que se actualizaba el **Plan Nacional de Protección de las Infraestructuras Críticas** conforme al apartado quinto de la citada Instrucción en su punto segundo.

Su objetivo fundamental es **acercar a la Administración y a los operadores de servicios esenciales en la coordinación de medidas operativas de seguridad**. En este sentido, se prevé su funcionamiento como órgano permanente de apoyo para el seguimiento y coordinación de las medidas de protección activadas, por los operadores críticos, así como para el establecimiento de procedimientos de colaboración y comunicación entre los distintos agentes del Sistema de Protección de Infraestructuras Críticas.

Además de la reunión de constitución se han celebrado otras dos reuniones (15/09/2016 y 15/11/2016), asistiendo el Director del CNPIC, como presidente de la Mesa, los representantes de los operadores críticos (OC) uno por cada sector estratégico que cuenta con Plan Estratégico Sectorial (PES) elaborado y diferentes miembros del CNPIC.

2.6.5 MESA DE COORDINACIÓN CIBERSEGURIDAD PIC

El objetivo de esta mesa, cuya reunión constitutiva tuvo lugar el **29 de septiembre de 2016**, es **dar soporte a la Mesa de Coordinación PIC**, a la que está subordinada, en aquellos asuntos relacionados con la ciberseguridad, con objeto de que ésta pueda coordinar las acciones que se requieran en cada momento.

Está compuesta por un representante de cada uno de los 12 sectores/subsectores estratégicos con PES elaborado (Electricidad, Gas, Petróleo, Industria Nuclear, Financiero, T. Aéreo, T. Ferroviario, T. Marítimo, T. Carretera, Agua, Espacio e Industria Química).

A parte de la reunión constitutiva se celebró otra reunión el 30/11/2016 por lo que se han mantenido un total de **dos reuniones** en el año 2016.

2.6.6 GRUPO DE TRABAJO ELABORACIÓN PES TIC

Creado en el año 2015, este grupo formado por personal del CNPIC y tres consultoras. Desde su creación ha venido realizando trabajos para la **elaboración del estudio del Plan Estratégico Sectorial (PES) del sector de las Tecnologías de la información y la Comunicación (TIC)**, estando prevista su finalización al ser aprobado el PES de las TIC.

En el año 2016 se han celebrado un total de **10 reuniones** con las consultoras, manteniéndose la última reunión el pasado 26/10/2016, no estando previstas más reuniones de este grupo.

2.6.7 GRUPO DE TRABAJO INTERDEPARTAMENTAL ELABORACIÓN PES TIC

Creado en el año 2015, este grupo formado por personal del CNPIC y de los Ministerios/organismos competentes (Energía, Turismo y Agenda Digital, Economía y Competitividad, Defensa - MCCD y CESTIC-, Hacienda y Función Pública y CNI) en el ámbito del sector TIC. Tiene como objeto, al igual que el anterior grupo, la elaboración del estudio del Plan Estratégico Sectorial (PES) del sector de las Tecnologías de la información y la Comunicación (TIC).

La primera reunión de este GT se mantuvo en el año 2015, habiéndose celebrado en el año 2016 **cuatro reuniones**. La documentación de partida fue la elaborada en el grupo que

contaba con la participación de las tres consultoras, de modo que este grupo continuó con la realización de los trabajos necesarios para la elaboración del estudio del Plan Estratégico Sectorial (PES) del sector de las Tecnologías de la Información y la Comunicación (TIC). Está previsto que este grupo acometa el desarrollo final del PES TIC en el presente año 2017.

2.6.8 GRUPO DE TRABAJO DIRECTIVA 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 6 DE JUNIO DE 2016 (Directiva NIS)

El Director del **CNPIC**, en reunión celebrada el 4/10/2016, formó parte de la Comisión Técnica para la transposición a la legislación nacional de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Constituyéndose el grupo de trabajo el **11 de octubre de 2016**, con el objetivo de realizar la **transposición de la Directiva NIS.**

En este grupo participan 10 representantes del Ministerio de la Presidencia del Gobierno, CCN-CNI, Ministerio de Energía, Turismo y Agenda Digital, Ministerio del Interior: CNPIC y Secretaría General Técnica. Ha celebrado seis reuniones, en las siguientes fechas: 11/10/2016, 26/10/2016, 08/11/2016, 23/11/2016, 01/12/16 y 16/12/2016.

2.6.9 GRUPO DE TRABAJO GIRIS

El Grupo de "**Información Clasificada Nuclear**" fue constituido el **26 de febrero de 2016,** en la sede de Consejo de Seguridad Nuclear, su objetivo es la creación de las red de puntos de control o servicios "oficiales" en el ámbito de la protección de la información clasificada dentro del ámbito de la industria nuclear. En el mismo participa, como representante designado por el Ministerio del Interior, el Jefe del Servicio de Planes y Seguridad del **CNPIC**. Durante 2016, se ha reunido en una ocasión.

2.6.10 GRUPO DE TRABAJO LANDSEC

Constituido el **14 de diciembre de 2016,** en el Ministerio del Interior, es de un grupo de trabajo de la **Comisión Europea** que trata de analizar las mejores prácticas para la Protección y Seguridad de Zonas Públicas de las **Infraestructuras dentro del sector del Transporte**, en todos sus subsectores. En el mismo participa como representante del **CNPIC** el Jefe del Servicio de Planes y Seguridad, celebrándose una reunón.

2.6.11 GRUPO DE TRABAJO SOBRE EL SISTEMA DE INSPECCIONES EN MATERIA DE SEGURIDAD PORTUARIA

Se creó el **25 de enero de 2016**, teniendo como objetivo **diseñar la organización y el contenido del sistema de inspecciones** para el control de la **normativa sobre protección marítima**.

La Sección de Planificación Estratégica del Servicio de Planes y Seguridad del **CNPIC**, participó junto a 17 integrantes de diferentes organismos (Puertos del Estado, Secretaría General de Transporte, Dirección General de la Marina Mercante, Área de Seguridad Ciudadana del Gabinete de Coordinación y Estudios de la SES, Guardia Civil, Policía Nacional, etc..). En total, durante 2016, se han celebrado cuatro reuniones.

2.6.12 GRUPO DE TRABAJO "REMOTEDLY PILOTED AIRCRAFT"

Se creó en abril de 2015 y está formado por miembros de la SES (Gabinete Coordinación y Estudios y la SGSICS), Policía Nacional, Guardia Civil, CNI, Ministerio de Defensa, Presidencia de Gobierno y Casa Real.

RPA
REMOTELY PILOTED AIRCRAFT

Tiene un doble objetivo: elaborar el **Proyecto de Real Decreto** por el que se regula la utilización civil de aeronaves pilotadas por control remoto (DRONES) y analizar un **sistema de seguridad** capaz de neutralizar este tipo de amenaza.

Durante el 2016 el **Grupo de trabajo de Drones se reunió un total de seis veces**. El **CNPIC** presta asesoramiento técnico al Grupo, en materia de detección y neutralización ante un ataque de DRON a infraestructuras críticas.

2.6.13 COMITÉ DE PARTES "ALTER TECHNOLOGY"

El **CNPIC** colabora con Alter Technology, como **Entidad de Certificación** de productos y sistemas de seguridad. El **CNPIC**, desde el 11 de noviembre de 2015, **ha pasado a formar parte del Comité de Partes de la Entidad de Certificación**, dada la importancia y obligatoriedad de que los sistemas de seguridad de las Infraestructuras Críticas sean de GRADO 4.

ALTER TECHNOLOGY

Se reúnen una vez al año.

2.6.14 CIP CONTACT GROUP

En el **Programa Europeo para la Protección de Infraestructuras Críticas** (PEPIC), existen una serie de iniciativas asociadas en las que el **CNPIC** está participando de manera asidua, como punto de contacto del Estado español para la coordinación de temas PIC con otros Estados miembros, el Consejo y la Comisión.

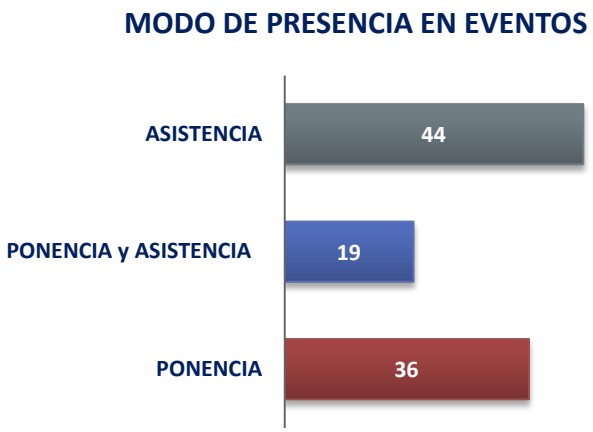
En lo que respecta al punto de contacto, anualmente, se celebran **2 reuniones en Bruselas**. En la última reunión, uno de los puntos de la Agenda era la **transposición de la Directiva NIS** a las legislaciones Nacionales.

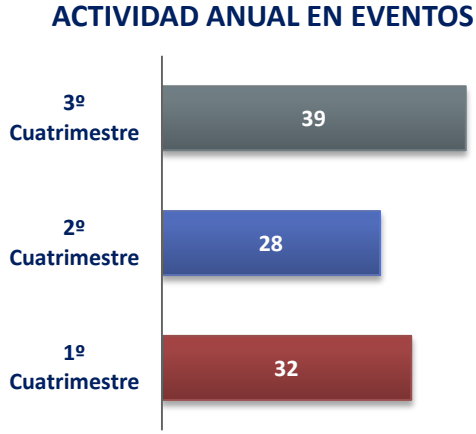
EN TOTAL: ***14 GRUPOS DE TRABAJO*** **(nacionales e internacionales)**

65 REUNIONES

2.7 INTERVENCIONES EN CONFERENCIAS, CURSOS, FOROS, SEMINARIOS, JORNADAS, ETC

El **CNPIC**, a lo largo del año 2016, ha participado en ***99 eventos.*** A continuación se muestran, en gráficos, los detalles de los mismos:

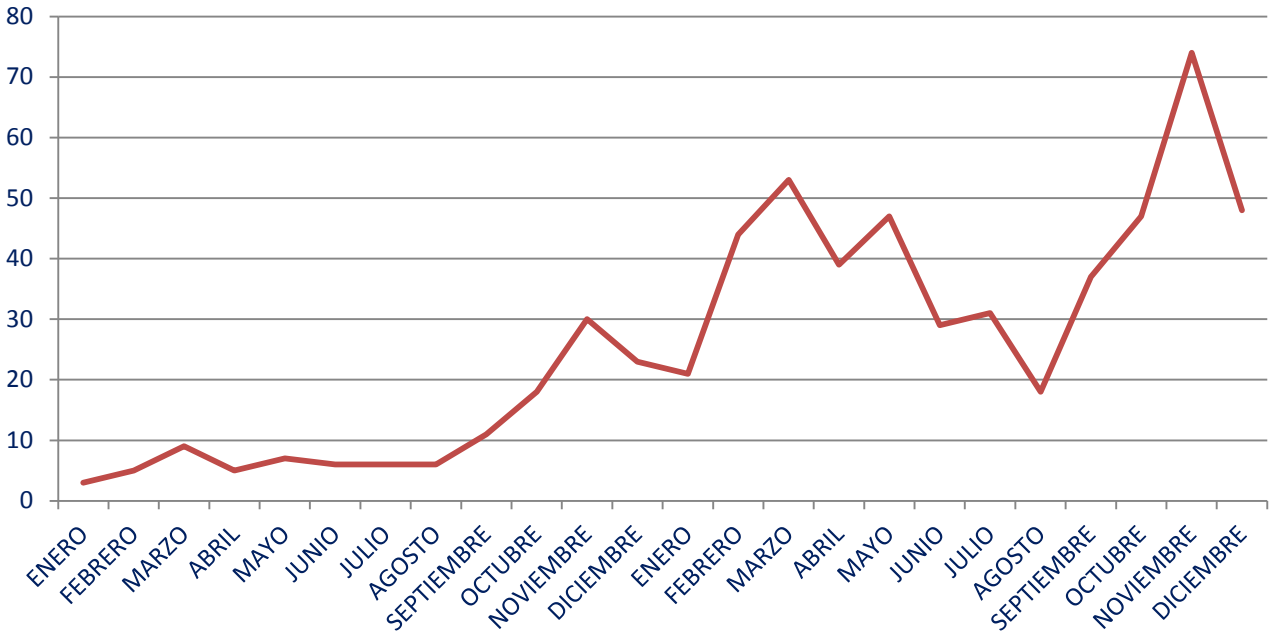




2.8 ACTUACIONES DEL CNPIC EN MATERIA DE CIBERSEGURIDAD

En el año 2016, el CERTSI, con la colaboración de la OCC, ha gestionado un total de **479 incidentes** que afectan a operadores críticos y estratégicos, representando un **incremento del 357%** sobre el total de incidentes gestionados en 2015, que fueron 134.

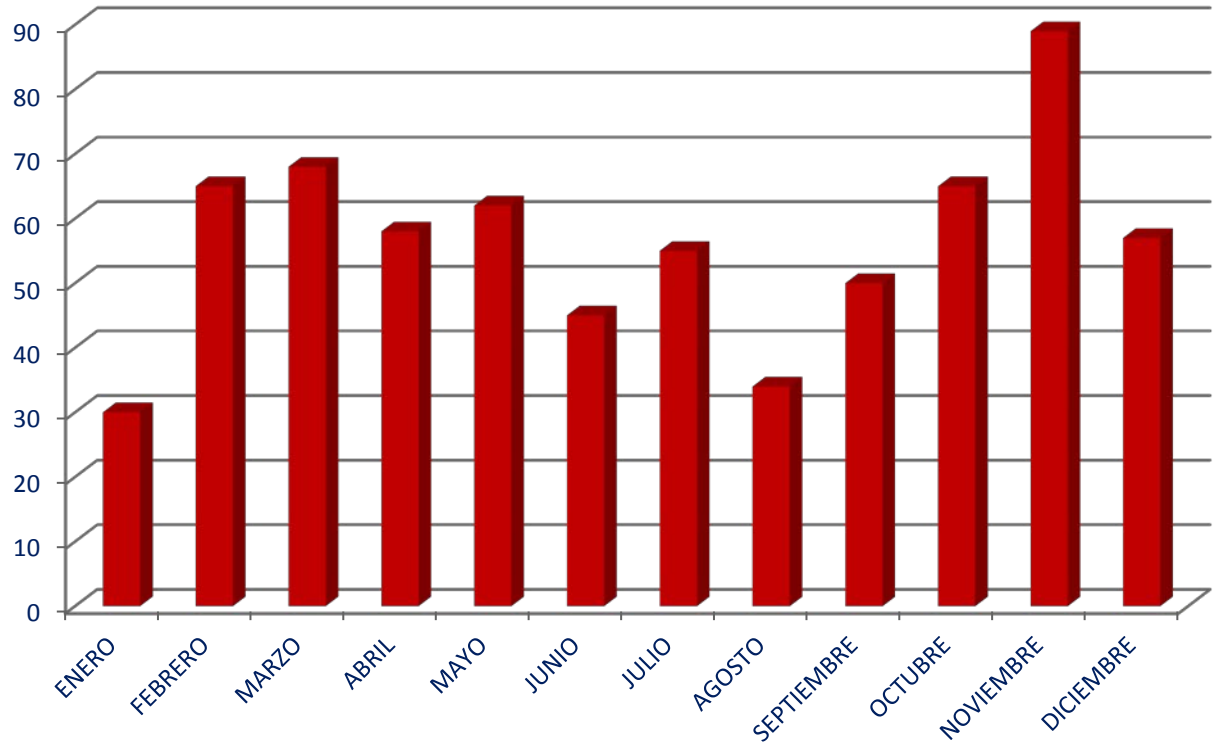
INCIDENTES GESTIONADOS EN LOS ÚLTIMOS 24 MESES



Se han llevado a cabo **678 actuaciones**, en relación a:

- **Intercambio de Información** en materia de ciberdelincuencia y ciberterrorismo.
- **Coordinación** de acciones de respuesta ante ciberincidentes llevadas a cabo por el CNPIC, el CERTSI y las unidades tecnológicas de las FCSE.
- **Emisión de alerta temprana** ante ciberamenazas.

En el siguiente gráfico se muestra la distribución mensual, durante 2016, en la gestión de actuaciones:



La OCC ha establecido **dispositivos extraordinarios de seguridad (DEC)** con ocasión de los siguientes eventos y/o situaciones:

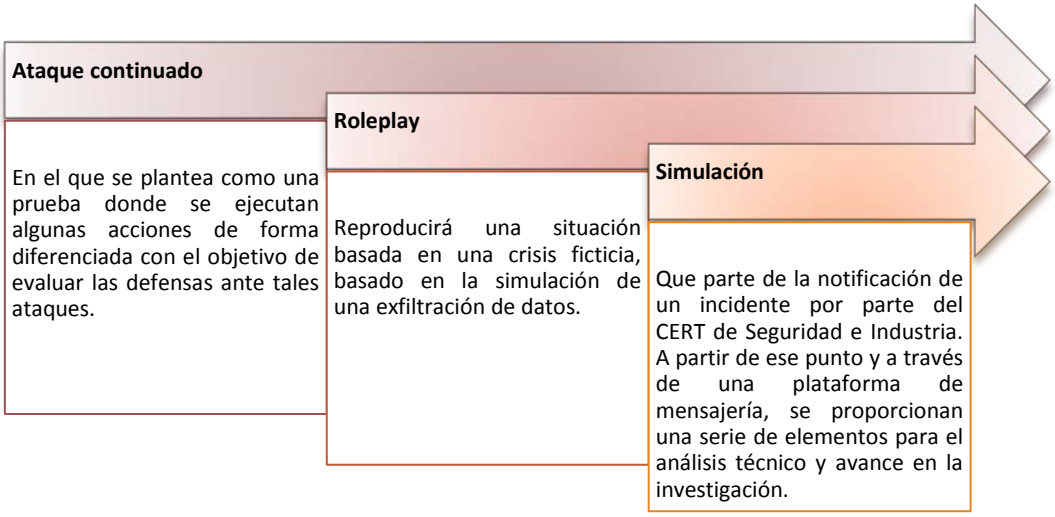
- ENERO–DICIEMBRE. Nivel 4 (ALTO) de **Alerta Antiterrorista** (aún vigente).
- JUNIO. **Elecciones Generales** día 26.

2.9 PARTICIPACIÓN DEL CNPIC EN CIBEREJERCICIOS

2.9.1 CyBerEx 2016

El **CNPIC** organizó esta edición, que contó con la asistencia de más de **20 participantes** procedentes de los operadores estratégicos nacionales, con el objetivo principal de mejorar su adiestramiento, evaluar el nivel de respuesta y potenciar los mecanismos de coordinación internos y externos de la organización.

Este año el ejercicio se desarrolló afrontando la evaluación y mejora de la resiliencia en las situaciones de ataque a entidades del Sector de la Energía, Financiero, Agua, Transporte y TIC. El escenario de CyberEx es mixto, y está compuesto por tres formatos de pruebas que pretenden evaluar capacidades distintas. Así, los tres escenarios que se abordaron en la iniciativa son:



Resultado: Con gran éxito de convocatoria, los resultados del Ciberejercicio han permitido a las organizaciones participantes **medir** sus **niveles de protección y capacidad técnica**.

2.9.2 International CiberEx2016

El **CERTSI** y la Organización de Estados Americanos **(OEA)** organizaron la segunda edición de los ciberejercicios International CyberEx, donde intervinieron más de 50 participantes de los 34 países de la OEA, Operadores, CERTs y entidades con equipos de ciberseguridad del entorno de la OEA.

La apertura oficial de los Ejercicios International Cyberex se realiza el **21 de julio de 2016,** en INCIBE (León), interviniendo en ella el Director del CNPIC. En esta ocasión, el ciberejercicio se desarrolló sobre la base de la **realización de desafíos en formato CTF** (capture de flag). Este formato se basa en el modelo de competición de seguridad cibernética y está diseñado para servir como un ejercicio de entrenamiento que permita otorgar a los participantes experiencia en el seguimiento de una intrusión, así como trabajar en las capacidades de reacción ante ciberataques análogos a los que suceden en el mundo real.

Resultado: Tanto el ciber ejercicio como la **gran afluencia de participantes**, fue valorado muy positivamente por los operadores.

2.9.3 Locked Sields 2016

Es el ejercicio anual de defensa en red en tiempo real basado en escenarios, organizado por el **Centro de Excelencia Cooperativa de Ciberseguridad de la OTAN**, con la misión de mejorar la capacidad, la cooperación y el intercambio de información entre la OTAN, los aliados y los asociados en la defensa cibernética. Locked Shields 2016 se organizó en cooperación con las Fuerzas de Defensa de Estonia, las Fuerzas de Defensa de Finlandia, el Colegio de Defensa de Suecia, el Ejército Británico, el Comando Europeo de los Estados Unidos. Esta edición, dirigida a los países integrantes de la OTAN, estuvo centrada en capacitar a los expertos en seguridad que protegen los sistemas nacionales de TI diariamente.

Resultado: En este ciberejercicio, basado en la protección frente a vulnerabilidades de PLCs, **se probaron destrezas técnicas y capacidad de trabajo en equipo**. Contó con una gran participación de entidades públicas, quedando de manifiesto la gran utilidad de la ejecución de ejercicios técnicos con alta carga real.

2.9.4 CyBer Europe 2016

Organizado por la **Comisión Europea (ENISA)**, y coordinado a nivel nacional por el DSN, el escenario de Cyber Europe 2016 se desarrolló alrededor de las industrias de TI, telecomunicaciones y ciberseguridad. El ejercicio está organizado para los equipos de seguridad informática, continuidad empresarial y gestión de crisis procedentes únicamente de los Estados miembros de la UE y de la Asociación Europea de Libe Comercio (AELC). Una de las fases del ejercicio y de mayor participación se centró en los **retos técnicos**, con lo que se pretendía **entrenar las capacidades técnicas** de los jugadores de forma individual y como equipo.

Resultado: Los diferentes escenarios: Ddos entidad financiera española, ciberataques a entidades españolas, defacement, simulación ataque físico con drones, incidente con malware, suponen **escenarios complejos y realistas resultando una muy buena experiencia de entrenamiento**.

2.9.5 CMX-16

Organizado por el **Estado Mayor de la Defensa (EMAD)**, se celebró la vigésima edición de gestión de crisis de la OTAN, en el que ensayaron y comprobaron los **procedimientos de consulta y toma de decisiones** en el nivel estratégico tanto político como militar. En el ejercicio, estuvieron involucradas autoridades civiles y militares de diversos Ministerios de los países aliados, del Cuartel General de la OTAN y de sus dos mandos estratégicos. Se desarrolló un escenario de crisis, ficticio pero verosímil, centrado en la defensa colectiva, con desafíos planteados por amenazas de guerra híbrida en la que se emplea una amplia gama de medidas tanto militares como civiles en el marco de un diseño altamente integrado. El principal **objetivo era poner a prueba procedimientos existentes, mejorar la resiliencia y establecer nuevas necesidades procedimentales**.

Resultados: El CNPIC, participó más como planificador que como jugador, ya que el rol del CNPIC se simuló desde la SES.

2.10 PARTICIPACIÓN DEL CNPIC EN PROYECTOS I+D+I

2.10.1 Red Nacional de Laboratorios Industriales (RNLI)

Proyecto dirigido a disponer de una **red de laboratorios** con capacidad para la experimentación e investigación de soluciones que **aumenten los niveles de seguridad de las infraestructuras** nacionales, además de apoyar el fomento de la colaboración y cooperación entre los actores involucrados en la seguridad de estos entornos, facilitando el intercambio de conocimiento dentro de la comunidad.

2.10.2 Proyecto HELIOS

Plataforma web para uso de servicios y herramientas dirigidas a **Fuerzas y Cuerpos de Seguridad del Estado**. Entre sus herramientas, destacan: inteligencia, análisis de amenazas, vigilancia de dominios, análisis avanzados, chequeo de claves, monitorización de redes anónimas, análisis de ciberataques, servicios de información sobre vulnerabilidades y panel de botnets.

2.10.3 Proyecto ENSI

El **Esquema Nacional de Seguridad Industrial (ENSI)** es un instrumento con vocación global para la **mejora de la seguridad** de las empresas del sector industrial, especialmente **particularizado a Operadores Críticos**. El objetivo es mejorar sus capacidades, minimizar los riesgos a los que se ven sometidos los servicios esenciales, y establecer metodologías y medidas para su mitigación, siendo aplicable en sistemas de control industrial de cualquier organización.

2.10.4 Proyecto ICARO

Servicio de compartición de información sobre ciberamenazas, basado en el proyecto MISP (Malware Information Sharing Platform), a través de indicadores de compromiso (IOC). De forma que la utilización de dichos

IOC permita **ampliar las capacidades de protección** en el perímetro de las entidades que forman parte del servicio.

2.10.5 Detector de Incidentes

Es una **Plataforma Tecnológica de Alerta Temprana y Servicios de Vigilancia Tecnológica,** enmarcada en la Estrategia de Ciberseguridad Nacional. Consiste en la puesta en marcha de un dispositivo encargado de **trasladar la inteligencia en ciberseguridad del CERTSI a la salida a internet de determinados operadores críticos**. El objeto es proporcionar una capa de detección que acompañe a las capacidades de protección de la entidad, encargándose el detector de identificar determinados casos en los que una máquina de la entidad haya sido comprometida.

2.10.6 Consorcios en Proyectos de H2020

Este año el **CNPIC** forma parte de dos Consorcios en **Proyectos de H2020,** ambos del Topic CIP-01- 2016-2017, "***Prevención, detección, respuesta y mitigación, de las amenazas contra IC, tanto físicas como cyber***", junto a "EVERIS" (enfocado en el sector del Gas Natural) y "AIRBUS" (sobre el sector Nuclear).

Además, dentro de la temática "Lucha contra el crimen y el terrorismo", SEC 12 FCT-2016-2017, Subtopic 2 "***Detención y neutralización de drones en áreas restringidas",*** con objeto de desarrollar un sistema ANTIDRON, se participa en:

- El Proyecto **INTRUDER.** Liderado por la Agencia de Investigación y Defensa sueca, el Ministerio del Interior participa aglutinando a: Policía Nacional, Guardia Civil y SES. Además, la Pyme "AEORUM" participa en el paquete de trabajo que desarrolla la implementación de los sensores. AEORUM, en dos de sus proyectos (en el año 2015 "DRONECAPTOR", y en el 2016 "DRONES4CIP"), que fueron respaldados por el **CNPIC** ha conseguido financiación de los fondos europeos FEDER INNTERCONECTA.

2.11 PRESENCIA DEL CNPIC EN LOS MEDIOS DE COMUNICACIÓN

2.11.1 Artículos y reportajes

➢ **Revista CUADERNOS DE SEGURIDAD**

- Febrero 2016
  - Artículo: "*Retos de la inteligencia artificial en el ámbito de la seguridad*"

    Autor: Jefe del Servicio de Ciberseguridad y OCC del CNPIC.

    https://issuu.com/peldano/docs/cuadernos-de-seguridad_307/54?mode=window

➢ **Revista RED SEGURIDAD**

- 4 ª trimestre 2016 – nº 72
  - Artículo : *"Evolución de la Ciberseguridad en el ámbito PIC".*

    Autor: Jefe de Sección de Análisis del Servicio de Ciberseguridad.

    http://www.redseguridad.com/revistas/red/075/index.html#20
- 4º trimestre 2016 – nº 75
  - Reportaje: *"OCC - el engranaje contra los ciberataques".*

    Autor: Jefe del Servicio de Ciberseguridad y OCC del CNPIC.

    http://www.redseguridad.com/revistas/red/075/index.html#20

➢ **Revista SEGURITECNIA**

- Septiembre 2016
  - Artículo: *"Guía de reporte de incidentes para operadores críticos".*

    Autor: Jefe de Sección de OCC del Servicio de Ciberseguridad del CNPIC.

    http://www.seguritecnia.es/seguridad-publica/administraciones-publicas/guia-de-reporte-de-incidentes-para-operadores-criticos
  - Artículo: *"Planes Estratégicos de la Industria Química y el Espacio"*

    Autor: Jefe del Servicio de Planes y Seguridad del CNPIC.

    http://www.seguritecnia.es/revistas/seg/436/index.html#20
  - Artículo: "Nuevo Plan Nacional para la Protección de las Infraestructuras Críticas: un reto en contínua evolución".

Autor: Jefe del Servicio de Normativa y Coordinación

http://www.seguritecnia.es/revistas/seg/436/index.html#24

2.11.2 Entrevistas

➢ **Revista SEGURILATAM**

- Febrero 2016
  - Entrevista al Director del CNPIC

    http://www.segurilatam.com/entrevistas/entrevistas/los-representantes-de-los-gobiernos-latinoamericanos-saben-que-el-cnpic-es-su-socio-y-aliado-en-la-proteccion-de-infraestructuras-criticas

➢ **ABC digital**

- 1 de abril de 2016
  - Entrevista al Director del CNPIC

    http://www.abc.es/sociedad/abci-fernando-sanchez-estamos-entrenando-equipos-para-repeler-ataques-fisicos-201604010759_noticia.html

➢ **Revista CUADERNOS DE SEGURIDAD**

- Octubre 2016, nº 315
  - Entrevista al Director y al Jefe del Servicio de Ciberseguridad del CNPIC

    https://www.puntoseguridad.com/cuadernos-de-seguridad/revista/315

➢ **Revista SEGURITECNIA**

- Noviembre 2016 – nº 436
  - Entrevista al Director del CNPIC

    http://www.seguritecnia.es/seguridad-aplicada/infraestructuras-criticas/el-modelo-pic-espanol-es-una-referencia-para-muchos-paises-que-estan-iniciandose-en-esta-materia

➢ **Revista RED SEGURIDAD**

- 4º trimestre 2016
  - Entrevista al Jefe del Servicio de Ciberseguridad y OCC del CNPIC.

    http://www.redseguridad.com/especialidades-tic/ciberseguridad/capacidades-de-ciberseguridad-en-infraestructuras-criticas

➢ **Diario "EL CONFIDENCIAL"**

- 2 de diciembre de 2016, en El Pardo (Madrid)
  - Entrevista al Director del CNPIC

    http://www.elconfidencial.com/espana/2016-12-24/terrorismo-ciberataques-tormenta-solar-viaje-a-las-tripas-de-la-seguridad-del-estado_1298909/

2.11.3 Otras publicaciones

➢ **EDITORIAL BORREDÁ (FUNDACIÓN BORRMART)**

- 22 de febrero de 2016
  - **Prólogo del libro** *"Modelo de Protección de Infraestructuras Críticas en España: Guía PIC"* (2ª edición en noviembre de 2016)

    Autor: Fernando J. Sánchez Gómez, Director del CNPIC
  - **Artículo** sobre la *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 – Guía PIC*, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la unión.

    Autor: Sección de Legislación y Estudios

2.11.4 Boletines informativos CNPIC

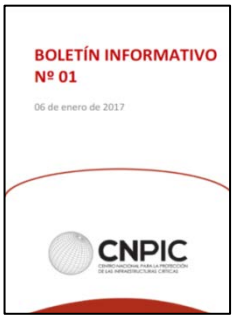
Durante el **2016** se han publicado **102 boletines informativos** donde se han incluido las principales noticias relacionadas con los doce sectores estratégicos, así como otras noticias vinculadas con infraestructuras críticas, terrorismo, distintos eventos de interés para el **CNPIC** y las actividades de la OCC.

Se han generado dos tipos de Boletines Informativos:

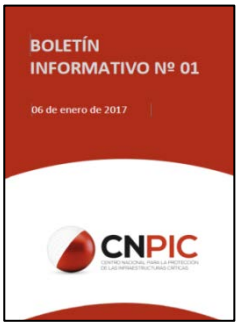
➢ **INTERNO.** Su difusión se realiza a las siguientes Áreas de la SES.

➢ **EXTERNO.** Destinado a **operadores** y otros **organismo públicos**, tanto nacionales como internacionales.

BOLETÍN INTERNO



BOLETÍN EXTERNO



2.12 ELABORACIÓN DE INFORMES, CONVENIOS, CONSULTAS, ACUERDOS, ETC…

- **INFORMES.** Se han emitido **56** informes.
- **CONVENIOS.** El **CNPIC**, ha participado en la redacción del:
  - Convenio Marco de colaboración en materia de Ciberseguridad, de 25 de febrero de 2016, entre la Secretaría de Estado de Seguridad y Legalitas. Firmado el pasado año, aunque su elaboración y redacción fue en el 2015.

- **CONSULTAS.** Se han respondido a **30** consultas.
- **ACUERDOS DE CONFIDENCIALIDAD.** Se han realizado **77** acuerdos de confidencialidad.
- **RESOLUCIONES.** Se han elaborado **189 resoluciones**.
- **APORTACIONES A DOCUMENTOS.** Se han modificado o realizado observaciones y/o aportaciones a los siguientes 3 documentos:
  - Observaciones a la **Resolución 1540** sobre armas nucleares, químicas y biológicas.
  - **Proyecto Real Decreto Transporte de mercancías peligrosas**.
  - **IS-41**, de 26 de julio 2016, del Consejo de Seguridad Nuclear por la que se aprueban los requisitos de protección física de fuentes radiactivas.

C / Cabo López Martínez, s/n
CP 28048 El Pardo (Madrid)
Tf. +34 918 398 203.

www.cnpic.es