MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+I
- Ciberseguridad
- Prensa y Eventos
- Documentación
- Contacto

CNPIC - Inicio

El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (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 y con la ciberseguridad en el seno del Ministerio del Interior**. El CNPIC depende del **Secretario de Estado de Seguridad**, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

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.

Nivel de Alerta en Infraestructuras Críticas (NAIC)

MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+i
- Ciberseguridad
- Prensa y Eventos
- Documentacion
- Contacto

Inicio ‣ Centro

EL CENTRO - Origen

El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, en el seno de la Secretaría de Estado de Seguridad, teniendo como objetivo principal la creación de un catálogo de infraestructuras conjunto para Policía Nacional y Guardia Civil.

Este primer objetivo marcado, se amplió posteriormente, ya que si el fin último era mejorar significativamente el nivel de seguridad, se necesitaba de la colaboración de múltiples actores, sobretodo, de aquellos que gestionan las infraestructuras y proporcionar los servicios esenciales para la sociedad.

SITUACIÓN EN NUESTRO PAÍS

En España, las actuaciones necesarias para optimizar la seguridad de las infraestructuras críticas se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

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 en sus funciones.

Las competencias del CNPIC están 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, que desarrolla la anterior, y por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

¿DÓNDE ESTAMOS?

En la localidad madrileña de El Pardo, ocupando las 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 SES. Desde abril de 2016 este edificio concentra ambas unidades tecnológicas de seguridad del Ministerio del Interior

PILARES DEL CNPIC

SISTEMA PIC (Sistema de Protección de Infraestructuras Críticas). Según se determina en el artículo 5 de la Ley 8/2011, se compone de aquellas "instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos" y se configura, de esta forma, como una de las piezas esenciales en la que descansa la propia seguridad nacional.

SEGURIDAD INTEGRAL. El CNPIC fue pionero en España en la aplicación de este concepto, entendiendo que la seguridad debe ser sistémica (también lo son las amenazas), no singular ni aislada. La protección de infraestructuras críticas se contempla desde un ángulo integral y comprensivo, no de manera fraccionada y, por tanto, aúna la seguridad física, cibernética y de personal.

Asociación público-privada. Es la clave sobre la que se basa la respuesta a los distintos ataques que puedan sufrir las infraestructuras críticas y los propios operadores de servicios esenciales. El principio de cooperación público – privada preside la legislación sobre materia PIC y la normativa sobre seguridad en nuestro país, y se basa en una distribución de responsabilidades, con el objeto de poder garantizar la protección y seguridad de los servicios esenciales. Por tanto, se puede decir que la colaboración y la coordinación público-privada son la piedra angular sobre la que se sustenta este Sistema. Por eso, el fundamento de la relación CNPIC-operador crítico no es otro que la confianza mutua, construida sobre la base de muchos años de trabajo común, las relaciones personales y la existencia de canales seguros, fiables y permanentes entre las dos partes.

ORGANIGRAMA

Actualmente, el CNPIC se compone de tres áreas en las que se estructura la unidad:

ORGANIGRAMA

Actualmente, el CNPIC se compone de tres áreas en las que se estructura la unidad:

- **Servicio de Planes y Seguridad**

  Cuya misión es la de coordinar las actividades necesarias para la implantación del Esquema de Planificación *PIC*. Además es, a través del Centro de Coordinación y Alerta (CECOA), el órgano encargado de la custodia, mantenimiento, gestión y explotación del Catálogo Nacional de Infraestructuras Estratégicas y de la alimentación y actualización de las bases de datos.

- **Servicio de Ciberseguridad - Oficina de Coordinación Cibernética**

  Encargado de coordinar todos los aspectos relativos a la seguridad cibernética dentro de la Secretaría de Estado de Seguridad y, especialmente, aquellos asuntos relacionados con la ciberseguridad de las infraestructuras y servicios esenciales a nivel nacional e internacional.

- **Servicio de Normativa y Coordinación**

  Cuyas misiones principales son de apoyo a las dos secciones anteriores: las referidas al ámbito normativo y legal; la obtención, tratamiento y difusión de información; las relativas a la I+D+i; y las relaciones y coordinación con otros agentes, nacionales e internacionales. Es, así, el punto focal de contacto del CNPIC con la Unión Europea y terceros países.

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+i
- Ciberseguridad
- Prensa y Eventos
- Documentación
- Contacto

Inicio ▸ Preguntas Frecuentes

CNPIC - Preguntas Frecuentes

- **¿Qué es un servicio esencial?¿Qué es una Infraestructura Crítica y Estratégica?**
- **¿Qué es un Sector estratégico? ¿Cuántos existen en España?**
- **¿Qué es el Sistema PIC? y ¿Por quién está formado?**
- **¿Qué es el Esquema de Planificación PIC?**
- **¿Qué es un operador crítico? ¿Cuántos hay y quiénes son?**
- **¿Qué es y que contiene el Catálogo Nacional de Infraestructuras Estratégicas?**

Nivel de Alerta en Infraestructuras Críticas (NAIC)

¿Qué es el Plan Nacional de Protección de infraestructuras Críticas (PNPIC)?

El Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), actualización del anterior que databa de 2007, fue aprobado mediante instrucción núm. 1/2016, de la Secretaría de Estado de Seguridad.

El PNPIC contiene los criterios y las directrices precisas para movilizar las capacidades operativas de respuesta, articulando medidas par asegurar la protección permanente, actualizada y homogénea de las infraestructruras críticas, de cualquiera de los sectores estratégicos recogidos en la Ley PIC, frente a las amenazas de carácter deliberado; todo ello en la línea y de forma coordinada con lo establecido por el Plan de Prevención y Protección Antiterrorista, con el que está vinculado.

¿Qué es el Nivel de Alerta en infraestructuras críticas (NAIC)?

El Nivel de Alerta es una escala compouesta por varios niveles complementarios, cada uno de los cuales se encuentra asociado a un grado de riesgo que, por lo general, va en concordancia con los niveles de alerta del Plan de Prevención y Protección Antiterrorista, en funcón de la valoración de la amenaza terrorista que se aprecie en cada momento.

¿Pueden ser distintos el nivel de alerta antiterrorista y el nivel de activación para la protección de infraestructuras críticas?

Sí, aunque lo normal es que coincidan. Sin embargo, en circunstancias concretas, ambos pueden variar en funciónde la información de la que se disponga, de las circunstancias asociadas a la misma y de la valoración de la amenaza que realicen los intervinientes en el Sistema PIC.

¿Cuántos niveles hay?

Existen cinco niveles de activación, al igual que en la clasificación previst aen el Plan de Prevencióin y Protección Antiterrorista, asociados a un determinado nivel de riesgo: el Nivel 1 corresoponde a **riesgo bajo**, el nivel 2 a **riesgo moderado**, el nivel 3 a **riesgo medio**, el Nivel 4 a **riesgo alto** y el Nivel 5 a **riesgo muy alto**.

¿Qué implica cada uno de los niveles?

La activación de cada nivel de seguridad del PNPIC lleva aparejada la puesta en marcha gradual de un conjunto de medidas específicas adaptadas al estado y naturaleza de la amenaza.

¿Quién decide el nivel de activación de protección de infraestructuras críticas?

La activación de un nivel de seguridad del PNPIC compete al Ministerior del Interior, a través de la Secretaría de Estado de Seguridad, correspondiéndose con el grado de riesgo detectado en cada momento, en atención a la valoración de la amenaza y otras circunstancias asociadas a la misma. Pero, en el caso del presenta Plan, se considerará especialmente la intención, capacidad y probabilidad de comisión de un ataque deliberado contra infraestructuras críticas que proporcionan servicios esenciales a la ciudadanía.

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

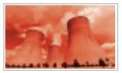
MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+i
- Ciberseguridad
- Prensa y Eventos
- Documentación
- Contacto

Inicio ‣ Legislación Aplicable

CNPIC - Legislación Aplicable

Genérico



Industria Nuclear

Industria Química

Espacio

Agua

Energía

Tecnología de la Información y de la Comunicación

Transporte

Alimentación

Salud

Instalaciones de Investigación

Financiero

Administración

CNPIC - Enlaces Nacionales

	MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN		GUARDIA CIVIL
	MINISTERIO DE DEFENSA		POLICÍA
	MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD		DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL Y EMERGENCIAS
	MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA		CONSEJO DE SEGURIDAD NUCLEAR
	MINISTERIO DEL INTERIOR		FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVICIAS
	MINISTERIO DE FOMENTO		INSTITUTO NACIONAL DE CIBERSEGURIDAD
	MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD		CERT DE SEGURIDAD E INDUSTRIA

MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+i
- Ciberseguridad
- Prensa y Eventos
- Documentación
- Contacto

Inicio ▸ Relaciones Internacionales y apoyo a la I+D+i

CNPIC - CNPIC-Internacional

- **ENLACES INTERNACIONALES**
- **ORGANISMOS EUROPEOS**
- **ORGANIZACIONES INTERNACIONALES**

Volver

MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+i
- Ciberseguridad
- Prensa y Eventos
- Documentación
- Contacto

Inicio ▸ Relaciones Internacionales y apoyo a la I+D+i

CNPIC - CNPIC-I+D+i

- **APOYO A LA INNOVACION TECNOLOGICA**
- **ENLACES DE INTERÉS EN INNOVACION TECNOLÓGICA**

Volver

CNPIC - Ciberseguridad

- **Introducción**
- **Respuesta a Incidentes de seguridad de la información en Infraestructuras Críticas**
- **Preguntas Frecuentes**
- **CERT DE SEGURIDAD E INDUSTRIA, CERTSI**
- **CERT del Centro Criptológico Nacional, CCN-CERT**
- **Guías SCADA**
- **Informes de Cibercriminalidad**
- **Grupos de Trabajo sobre ciberseguridad**
- **Ciberejercicios**
- **Cifrado y claves públicas del CERTSI Y CCN-CERT**

CNPIC - Archivo

INFORMES

- **INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD 2016**
- **INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD 2015**
- **INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD 2014**

CNPIC - MEMORIAS

- **MEMORIA 2016**
- **MEMORIA 2015**
- **MEMORIA 2014**

MENÚ

- Inicio
- El Centro
- Preguntas Frecuentes
- NAIC
- Legislación Aplicable
- Enlaces Nacionales
- Relaciones Internacionales y apoyo a la I+D+i
- Ciberseguridad
- Prensa y Eventos
- Documentación
- Contacto

Inicio ‣ Contacto

CNPIC - Contacto

Clave pública del CNPIC:

Si necesita más información o tiene alguna duda, puede contactar con nosotros a través del correo Punto de Contacto Único:

ses.cnpic-buzon@interior.es

Puede descargar la Clave pública del CNPIC en el siguiente enlace: CLAVE PÚBLICA

Operadores de Infraestructuras críticas:

En caso de que una Infraestructura Crítica sufra un problema de seguridad cibernético, el operador responsable de la misma podrá beneficiarse de los servicios de nuestro Equipo de Respuesta, informando de la incidencia a través del Punto de Contacto único habilitado para esta finalidad:

pic@incibe-cert.es

La clave pública del CCN-CERT para Gestión de Incidentes TIC en Infraestructuras Críticas de las administraciones públicas puede ser descargada en el siguiente enlace: CLAVE PÚBLICA

El mensaje cifrado debe ser remitido a:

incidentes@ccn-cert.cni.es