

El Grupo de Trabajo Informal sobre Protección de Infraestructuras Críticas, GIPIC, compuesto por el CNPIC y otras organizaciones, ha elaborado los contenidos mínimos para los Planes de Seguridad del Operador y los Planes de Protección Específicos

Los operadores de servicios esenciales deberán elaborar Planes de Seguridad integral para su organización y para cada una de sus infraestructuras críticas

- **Publicada en el BOE la Resolución, de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad, por la que se establecen los contenidos mínimos que deberán tener los Planes de Seguridad del Operador (PSO) y los Planes de Protección Específicos (PPE).**
- **Optimizar el grado de protección de las infraestructuras críticas contra ataques deliberados, tanto físicos como lógicos, que puedan afectar a la prestación de servicios esenciales para la población (energía, transporte, telecomunicaciones...) es el objetivo fundamental de toda la legislación publicada hasta la fecha y de los Planes ahora solicitados a los operadores.**

Madrid, 21 de diciembre de 2011. Aquellas organizaciones, públicas o privadas, gestoras y/o propietarias, cuyas instalaciones o sistemas sean catalogados como críticos por el Centro Nacional de Protección de Infraestructuras Críticas del Ministerio del Interior, **CNPIC**, deberán elaborar un Plan de Seguridad del Operador (**PSO**) y unos Planes de Protección Específicos (**PPE**) para cada una de sus infraestructuras críticas. Dichos planes deberán contar con unos contenidos mínimos los cuales fueron publicados el pasado 23 de noviembre en el Boletín Oficial del Estado mediante la **Resolución de 15 de noviembre de 2011**, de la Secretaría de Estado de Seguridad, del Ministerio del Interior, conforme a lo establecido en el Art 22.4 y 25.5 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas que da desarrollo reglamentario a la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Ante los numerosos riesgos y amenazas procedentes de muy diversos frentes, se hace necesario, tal y como recoge la Introducción de la citada Resolución, *el diseño de una política de seguridad homogénea e integral por parte de todas las organizaciones con infraestructuras críticas, en la cual se definan todas las medidas de seguridad que se van a implantar para la protección de las mismas (contra ataques deliberados, sean físicos o a través de Internet) con el objetivo de impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población;* es decir, aquellos servicios necesarios 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.

De este modo, en el PSO que desarrolle cada uno de los operadores críticos deberá definir la política general de su organización para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión. Este documento, como instrumento de planificación y mejora continua, contendrá además una relación de los servicios esenciales prestados, una metodología de análisis de riesgos (con identificación de las amenazas físicas y lógicas, considerando de forma especial aquellas de origen terrorista o intencionado) y unos criterios de aplicación de dichas medidas.

En cuanto a los PPE que deberán elaborar los operadores, para cada una de las Infraestructuras Críticas de las que sean propietarios o gestores, tendrán que recoger las medidas concretas para garantizar la seguridad integral (física y lógica) de dichas infraestructuras.

Plazos de presentación

Una vez que los operadores sean designados como operadores críticos tras un previo proceso de identificación y valoración de sus infraestructuras de la mano del CNPIC, el operador crítico *en el plazo de seis meses a partir de la notificación de la resolución de su designación, deberá haber elaborado un Plan de Seguridad del Operador*. Posteriormente, y de forma secuencial, *en el plazo de cuatro meses a partir de la aprobación de su PSO, el operador crítico deberá haber elaborado un Plan de Protección Específico por cada una de sus infraestructuras críticas*.

El Grupo de Trabajo Informal sobre Protección de Infraestructuras Críticas, GIPIC, ha apoyado al CNPIC en la elaboración de estos documentos, y además, está trabajando en la elaboración de una serie de guías de “buenas prácticas” que faciliten a cada operador el diseño de estos planes de seguridad.

Sobre GIPIC

El GIPIC, además de colaborar en la elaboración de los contenidos mínimos del PSO y del PPE, está trabajando en la elaboración de una serie de guías de “buenas prácticas” que faciliten a cada operador el diseño de estos planes de seguridad.

El GIPIC fue creado en octubre de 2010 para el desarrollo y elaboración de unas Guías de Contenidos Mínimos y Guías de Buenas Prácticas sobre el Plan de Seguridad del Operador y del Plan de Protección Específico, para servir de orientación y ayuda a aquellos operadores que sean designados como críticos en la elaboración de los citados planes. El objetivo fundamental de los trabajos del GIPIC, patrocinado e impulsado por el CNPIC, de la Secretaría de Estado de Seguridad del Ministerio del Interior, es la promoción de una **cultura de seguridad** en la que los sectores público y privado puedan comenzar a trabajar sobre unos **parámetros homogéneos** y claramente definidos en materia de protección de sus respectivos activos.

Colaboran en el GIPIC, además del **CNPIC**, como organismo responsable y director de los trabajos, otros organismos públicos y privados españoles (por orden alfabético): la Agrupación Empresarial Innovadora (**AEI-SRSI**) para la Seguridad de las Redes y los Sistemas de la Información, el Centro Criptológico Nacional (**CCN**), **Cuevaliente Ingenieros**, **Indra**, Ingeniería de Sistemas para la Defensa de España (**ISDEFE**), Instituto Nacional de Tecnologías de la Comunicación (**INTECO**), **PwC**, **S21sec** y **TB-Security**.

Como su nombre indica, el GIPIC es un grupo informal, sin estatutos de constitución ni de funcionamiento interno, materializando así uno de los objetivos que el CNPIC se trazó desde su constitución: la formalización de asociaciones público-privadas basadas en la confianza mutua y en el afán por conseguir un interés común.

Más información

XXXXXXX

