Nota de prensa

# El secretario de Estado de Seguridad, Francisco Martínez, presenta el nuevo Plan de Protección de las Infraestructuras Críticas

- **Francisco Martínez ha destacado, ante los operadores críticos, que el nuevo Plan "va a servir para fortalecer el sistema de seguridad nacional de manera alineada con el Plan Nacional de Prevención Antiterrorista"**

- **Además, ha señalado que por primera vez, el Plan Nacional de Protección de las Infraestructuras Criticas contempla la seguridad de forma integral, gestionando los posibles incidentes en las propias infraestructuras o los que se cometan desde el mundo virtual**

**8 de marzo de 2016.-** El secretario de Estado de Seguridad, Francisco Martínez, ha presentado esta mañana en la sede de Gas Natural Fenosa, el nuevo Plan Nacional de Protección de las Infraestructuras Críticas ante 200 operadores públicos y privados de infraestructuras críticas de los sectores de la energía, la industria nuclear, el sistema financiero, el transporte y el agua.

Durante su intervención, Francisco Martínez ha ido desgranando las novedades de este plan, aprobado el pasado mes de febrero por la Secretaría de Estado de Seguridad, y que ha asegurado "va a servir para fortalecer el sistema de seguridad nacional de manera alineada con el Plan Nacional de Prevención Antiterrorista". De tal manera que la activación de los niveles de alerta de ambos planes, tanto en materia antiterrorista como en la protección de las infraestructuras –que ahora también se fija en 5 niveles- se hará conjuntamente, ha señalado.

En este sentido, ha recordado que desde enero de 2015, la Oficina de Coordinación Cibernética puso en marcha un Dispositivo Extraordinario de Ciberseguridad (DEC) correspondiente al nivel de alerta antiterrorista 4 (alto); un dispositivo particularmente enfocado al seguimiento de acciones relacionadas con la difusión de material y propaganda yihadista. Ya que, según Martínez, "las principales amenazas para nuestro país –incluidas el terrorismo y los riesgos para la ciberseguridad e infraestructuras críticas-,

se contemplan de manera global, integral y coherente en la Estrategia de Seguridad Nacional".

Siguiendo con las novedades, Francisco Martínez ha señalado que por primera vez, el Plan contempla la gestión integral de la seguridad, abarcando la doble dimensión –física y virtual- de la realidad del funcionamiento de estos servicios esenciales. Aspecto en el que ha hecho hincapié, ya que a su juicio, "el ciberataque supone un riesgo con una probabilidad mucho más alta que el asalto físico a una instalación y que, además, ofrece un riesgo menor para quien lo comete".

En este contexto, ha destacado que durante 2015, el CNPIC, a través del Centro de Respuesta a Incidentes de Seguridad TIC de Seguridad e Industria (CERTSI), resolvió alrededor de 50.000 incidentes de ciberseguridad, de los que, 134 estaban dirigidos contra infraestructuras críticas. Además, ha asegurado que está previsto que a lo largo de 2016 los ciberataques asciendan a 100.000, de los cuales, 300 serían contra infraestructuras críticas.

El secretario de Estado de Seguridad ha señalado que, en base a los datos, el balance de los últimos cuatro años en materia de seguridad de infraestructuras públicas es muy positivo. Por una parte, ha destacado que se han nombrado 93 operadores críticos y se han identificado a más de 300 infraestructuras críticas de sectores como la energía, la industria nuclear, el sistema financiero, el transporte y el agua. Asimismo, ha puesto de relieve la multiplicación de los instrumentos de planificación con la puesta en marcha de 10 planes estratégicos sectoriales.

En esta materia, también se ha referido al impulso que se ha dado a nivel internacional, destacando los acuerdos de colaboración suscritos con Europol, el FBI o la Organización de los Estados Americanos (OEA), además de la activa participación de España en la Unión Europea.