NOTA DE PRENSA

LOS MINISTERIOS DEL INTERIOR Y DE INDUSTRIA PARTICIPAN EN UNA JORNADA SOBRE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD EN EL SALÓN INTERNACIONAL DE SEGURIDAD (SICUR 2016)

- **La celebración del evento coincide con la reciente aprobación del Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC), que modifica el anterior Plan, datado de mayo de 2007**

- **La edición de SICUR 2016 está orientada especialmente a los nuevos operadores críticos y a aquellos países latinoamericanos que están comenzando a desarrollar sus políticas en este campo**

- **En 2015, el CERT de Seguridad e Industria (CERTSI_) se enfrentó a 134 incidentes de ciberseguridad que afectaron a infraestructuras que prestan servicios esenciales**

Madrid, 24 de febrero de 2016.- El Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) han participado en un evento en el que se ha analizado el estado de implantación de las políticas del Gobierno sobre protección de infraestructuras criticas, entre las que destaca la reciente aprobación del Plan Nacional de Protección de las Infraestructuras Críticas, que será presentado a los operadores críticos el próximo día 8 de marzo, en unas jornadas que inaugurará el Secretario de Estado de Seguridad.

Las infraestructuras críticas son las instalaciones, redes o equipos físicos y tecnológicos que prestan servicios esenciales para la sociedad, por lo que están en el 'punto de mira' de los delincuentes o grupos terroristas. Un ataque físico o cibernético a dichas infraestructuras puede tener un gran impacto en ámbitos como la salud, la seguridad, el bienestar económico de los ciudadanos, o en el funcionamiento de las instituciones del Estado y de las Administraciones Públicas.

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

PASEO DE LA CASTELLANA, 5
28071 - MADRID
TEL: 91 319 20 94
FAX: 91 308 55 66

NOTA DE PRENSA

integral de este tipo de infraestructuras. Esta tarea está encomendada al Centro Nacional para la Protección de las Infraestructuras Críticas.

En dicha labor, y con el objetivo de reforzar la seguridad cibernética idónea colabora de manera estrecha el Instituto Nacional de Ciberseguridad desde el año 2012, en virtud de un acuerdo marco de colaboración entre las Secretarías de Estado de Seguridad, y de Telecomunicaciones y Seguridad de la Información. Fruto del mismo surgió el CERT de Seguridad e Industria (CERTSI_), que es el punto de referencia y el órgano competente para la resolución técnica de aquellos incidentes de ciberseguridad que afecten a los operadores de los servicios esenciales.

La jornada, que se ha desarrollado en el Salón Internacional de Seguridad (SICUR) que se celebra estos días en Madrid, ha contado con la presencia de un centenar de personas, la mayoría de ellas operadores de los sectores de la energía, la industria nuclear, el sistema financiero, el transporte y el agua, así como con representantes de varios países latinoamericanos, procedentes fundamentalmente de los respectivos Ministerios de Interior y de Defensa.

El director del Centro Nacional para la Protección de las Infraestructuras Críticas, Fernando Sánchez, que ha intervenido en la apertura de la jornada, ha planteado brevemente la misión, los objetivos y la actividad de dicho centro y los elementos que se están presentando en la construcción del Sistema de protección de infraestructuras críticas español.

Por su parte, el director general del Instituto Nacional de Ciberseguridad, Miguel Rego, ha profundizado en la estructura del CERTSI_ y en los servicios que ofrece actualmente para la prevención, detección y respuesta ante ciberamenazas, explicando las líneas de actuación con las que va a contribuir al Plan de Infraestructuras Críticas 2016-2017.

A lo largo de la sesión, se han abordado además los retos de futuro que se plantean en este campo, en el estado de implantación de los diferentes planes y en la estructura y funcionamiento de los organismos públicos que son competentes en ello. Además, se ha podido profundizar en los aspectos de la ciberseguridad de las infraestructuras críticas y en los avances que se han producido en los últimos meses, incidiendo en la labor realizada por el CERTSI_ y la Oficina de Coordinación Cibernética del Ministerio del Interior, cuyo funcionamiento como punto de enlace entre Fuerzas y Cuerpos de Seguridad, operadores críticos y servicios tecnológicos ha sido también presentado y puesto en valor.

Según datos proporcionados por los intervinientes, en el año 2015, con respecto a 2014, se gestionaron un 180% más de incidentes de

NOTA DE PRENSA

ciberseguridad. De los cerca de 50.000 incidentes registrados, 134 correspondieron a infraestructuras críticas.

En la jornada, se ha hablado también de las líneas de colaboración para la lucha contra los ciberdelitos y el ciberterrorismo y sobre el desarrollo de tecnologías de aplicación directa en la investigación de ciberdelitos.