III JORNADA SOBRE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Tuvo lugar en Madrid el día 26 de febrero, en el Auditorio de Gas Natural Fenosa, organizada por la Fundación Borredá, y AES fue invitada a participar en la misma.

La jornada se abrió por parte de Fernando Sánchez, Director del CNPIC, que concretó el estado de situación del sistema PIC y las lecciones aprendidas, diferenciándolas en cinco fundamentales:

1) Estamos en una situación de riesgo. Hay que identificar las amenazas, analizar los riesgos, implantar contramedidas y establecer controles. Con este objetivo se crearán después del verano unos grupos de trabajo para ver cómo se están desarrollando los planes.

2) Necesidad de una metodología homogénea. Hay varios Ministerios implicados en las PIC, además del de Interior: Fomento, Sanidad y Medio Ambiente, Industria… Se deben establecer procedimientos concretos y métodos de control. Estos procedimientos deben permitir un grado de movimiento de las organizaciones.

3) La seguridad tiene que ser integral, identificando riesgos físicos, cibernéticos y de personal.

4) Tiene que ser una seguridad desde el diseño. Significa que debemos tener capacidad para que la solución se pueda integrar en el diseño. Que sea el diseño español el que evite los riesgos. Para ello es muy importante colaborar con el CERT de seguridad e industria, que ya tiene acuerdos de confidencialidad firmados con 43 empresas.

5) El intercambio de información entre organizaciones públicas y privadas es el fundamento de la PIC. La clave de ello es la confianza. Se lleva por contacto directo, por formación en grupos de trabajo sectoriales y por creación de plataformas de intercambio de información. Hay que gestionarlo por regulación de la Administración, con acceso limitado a los que forman parte del sistema PIC y su funcionamiento debe estar basado en la confianza mutua, ya que su participación es voluntaria.

El CERT de seguridad e industria tiene dos colaboradores fundamentales, que son la Guardia Civil y el Cuerpo Nacional de Policía. Para ello se ha puesto en marcha la oficina de colaboración cibernética (occ@interior.es).

Seguidamente dieron su opinión varios operadores críticos. Para José Juan Meaza, de Bahía de Bizkaia Gas, el reto más importante es la ciberseguridad.

Por su parte, José Carlos Moreno, del Banco de Santander, explicó que en general, la seguridad de nuestras IC es buena. Solamente necesitan trabajar un mayor nivel de convergencia.

Rafael Gassó, del Banco de España, dijo que, en su opinión, la Administración está ayudando a las organizaciones, impulsando con pautas que establecen lo que se requiere a los operadores críticos.

Carlos Pérez de Acciona Energía, explicó el funcionamiento de su centro de control de renovables, pionero en el mundo. La seguridad física y la lógica, dijo, han ido cada una por su lado, y es necesaria una seguridad integral.

Joaquín Álvarez, de Endesa, explicó la campaña de concienciación e información que, por su parte, han dado a todos los implicados. Tiene que existir, recalcó, un compromiso formal para trabajar la seguridad todos los días.

Rogelio Campos, de Repsol, dijo que, en su opinión, hay que mejorar la política de seguridad integral. Existe, explicó, una interdependencia entre el CNPIC, los operadores y las FCS, donde es muy importante la colaboración con implicación.

En el panel de nuevos escenarios, José Ignacio Carabias, jefe de área del CNPIC, explicó los siguientes pasos para este Centro. Se está trabajando ahora en los planes de los siguientes sectores estratégicos: transporte (aéreo, ferroviario, carretera y marítimo) y agua. A partir de verano se empezará con el plan estratégico del sector TIC.

En lo que a los planes de seguridad del operador se refiere, los operadores han hecho un gran esfuerzo, explicó.

Participaron entonces los operadores estratégicos de los sectores del transporte y del agua.

Mario Rodríguez, de AESA, indicó cómo los aeropuertos deben adecuarse constantemente a los cambios de la amenaza.

José Lóbez Cuadrado, del Ministerio del Fomento, explicó el funcionamiento de la Unidad de Emergencia y Coordinación y Gestión de Crisis de este Ministerio, que tiene la finalidad de restablecer la situación de normalidad.

Celia Tamarit, de Puertos del Estado, comentó cómo nuestros puertos son unas infraestructuras muy flexibles. Pueden dar servicio a cualquier barco en cualquier momento.

Por su parte, Margarita Palau, del Ministerio de Sanidad, explicó que el agua de consumo, necesaria para la vida, llega a cada hogar sin que tengamos posibilidad de cambiarla. Por ello, el control del agua de consumo, junto con las vacunaciones, es una de las competencias del Ministerio de Sanidad más antiguas.

En conclusión, una muy interesante jornada que sirvió para encuadrar la situación de la PIC en estos momentos en los que nos encontramos.