

La ciberseguridad en el sector público no se reduce a tecnología, alcanza a cuestiones organizacionales y de toma de conciencia

El Club de los Miércoles, que organiza Aranzadi LA LEY, celebró ayer una nueva edición en la que se debatió sobre la articulación de la ciberseguridad en el sector público: la Directiva NIS2 y el Esquema Nacional de Seguridad (ENS).

En el encuentro, que estuvo moderado por Leandro Escudero Atienza, Professional & Consulting Services Director – PMP en Aranzadi LA LEY, intervinieron como ponentes: Miguel Angel Lubian, CEO CÍES (Grupo Seresco) Seguridad y Cumplimiento y Virginia Moreno Bonilla, coordinadora del grupo de trabajo Ciberseguridad, protección de datos/identidad digital e IA en la Red de Ciudades para la Participación y la Transparencia, FEMP, directora Estrategia Corporativa, Aeioros Servicios.

Leandro Escudero comenzó su intervención encuadrando los temas a debatir, y recordó que existe un anteproyecto de ley en proceso para transponer la Directiva NIS2, por lo que es clave conocer cuanto antes cómo va a afectar la futura ley a todo el sector público, su convivencia con el ENS, la articulación del estatuto del CISO/Director de seguridad de la información, la gestión de los riesgos de ciberseguridad y las particularidades a tener en cuenta en las entidades locales. A continuación, dio paso a los ponentes.

Virginia Moreno resaltó las dificultades en ciberseguridad a las que se enfrentan los ayuntamientos pequeños. De ahí que, desde el Equipo de Trabajo multidisciplinar que ella coordina se está elaborando una guía práctica en la que se concretan los pasos a seguir. Incluso, a través de un formulario, tipo encuesta, sobre las herramientas tecnológicas puestas a disposición, se quiere recopilar información e incluir las conclusiones en la citada guía para proponer mejoras.

Apuntó que en ciberseguridad el elemento diferencial es la responsabilidad del equipo directivo, el compromiso y la inversión. La ciberseguridad no se reduce a cuestiones tecnológicas, es una cuestión organizacional y de toma de conciencia. Es imprescindible que la entidad tenga todo organizado para que no haya fuga de información. En este punto, la capacitación y formación de todos los que forman parte del ecosistema es vital. Considera que, a pesar de la casuística que puede presentarse en las EE.LL., el impacto de la transición del ENS a la NIS2, será mínimo.

Por su parte, Miguel Ángel Lubian, con un discurso optimista, apuntó que a pesar de todas las amenazas y riegos que nos acechan actualmente, estamos mejor que hace unos años y evolucionamos muy bien, a lo que hay que añadir que, afortunadamente, ya ha calado la necesidad de invertir en ciberseguridad.

Una cuestión importante es que estamos en un país excesivamente regulado, por lo que desde el principio conocemos qué tenemos que hacer; aunque la implementación tecnológica no es igual en el sector público que en el privado.

Destacó la importancia de identificar y empoderar al Responsable de la Seguridad. No se trata de hacer un cambio de modelo, sino de colocar a las personas en el centro, desarrollar un cultura y tomar decisiones adecuadas, con unos sistemas más conectados e interoperables y aprovechar la oportunidad que nos brinda la NIS2.

Estar certificado en el ENS no garantiza evitar ciberataques pero, dado que entre el ENS y la NIS2 hay muchos paralelismos, hay que seguir trabajando en el ENS y concretamente en la responsabilidad. Seguro que cuando se materialice la transposición de la Directiva, tendremos que aplicar pequeños ajustes.

Ante la prevención y la resiliencia, siempre la gestión de los riesgos a los que estamos expuestos debe prevalecer.

Fuente: https://www.legaltoday.com/

LINK DE LA NOTICIA