Ciberseguridad y Smart Cities en Andalucía

El desarrollo de las ciudades inteligentes (Smart Cities) debe ir acompañado de la implantación de acciones, políticas y estrategias de Ciberseguridad

La Consejería de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía ha abierto el pasado martes 11 de febrero de 2020 la convocatoria de ayudas para el desarrollo de '**Smart Cities**' en Andalucía, por valor de 10 millones de euros. **¿Qué pinta la Ciberseguridad aquí?**

Los beneficiarios de estas ayudas son ayuntamientos y entidades locales andaluzas **de menos de 20.000 habitantes**.

Entre las actuaciones subvencionables, encontramos proyectos de plataformas tecnológicas, infraestructuras de software y hardware, formación de personal, o servicios de transparencia.

Es por ello por lo que la Ciberseguridad se hace esencial en estas Smart Cities.

No debe olvidarse que una Smart City es un ecosistema complejo, en el que intevienen numerosas y diferentes tecnologías.

Estas tecnologías, además, se enfrentan a retos como la escalabilidad, la capacidad, la movilidad y la **ciberseguridad** y **privacidad** de la información.

Todos estos proyectos (Open Data, portales de transparencia, optimización de energía y agua, sensores para el tráfico…) no pueden llevarse a cabo sin un estudio y una serie de medidas implantadas en materia de **Seguridad Informática**.

La Ciberseguridad sigue siendo un punto débil para las Smart Cities.

Según datos de ABI, el gasto previsto en Ciberseguridad para 2024 de infraestructuras críticas se centrará en las infraestructuras TI y de defensa.

Techco Security alerta de la necesidad de integrar la Ciberseguridad en las futuras smart cities españolas.

Desde Dolbuck, advertimos y recomendamos que la Seguridad Informática sea un **pilar** y la **base transversal** para la concepción y el desarrollo de las Smart Cities andaluzas.

En este sentido, ponemos el foco en la necesidad de integrar acciones y securizar los proyectos de ciudad inteligente, como pueden ser la gestión de residuos, el tráfico urbano, o la optimización de recursos.

Cada vez, los ataques cibernéticos son más sofisticados en infraestructuras críticas, como pueden ser los ayuntamientos o los centros sanitarios.

A finales de enero de 2020, los servicios informáticos del ayuntamiento de la **ciudad de DuBois** (Pensilvania) fueron atacados por un grupo de cibercriminales, provocando así la suspensión de dichos servicios.

El rescate para la desencriptación de los ficheros ha trascendido, y la cantidad es de 10 bitcoins (aproximadamente equivale a $85,000).

El pasado mes de octubre de 2019, '**Ryuk**' entró a la red del **Ayuntamiento de Jerez** a través de correo electrónico, bloqueando y encriptando los archivos de los

servidores. A continuación, los ciberdelincuentes exigieron un rescate en bitcoins, cuya cantidad aún no ha trascendido.

En conclusión, cuanto más *smart* sea una *city*, más amplio será el espectro de ciberataques posibles.

Cuanto más extensa sea una red, más difícil será detectar las vulnerabilidades y dónde se encuentran.

Los proyectos de Smart City que afecten o precisen una infraestructura compleja de red, **deberán ir acompañados de un plan integral de Ciberseguridad**.