Diez compañías vascas colaboran en un ambicioso proyecto para desarrollar soluciones que protejan la red eléctrica de ciberataques

- **La ciberseguridad de la red eléctrica es uno de los principales retos que aborda el sector energético.**
- **Liderado por Ingeteam, el proyecto Sec2Grid se desarrollará hasta 2024 con una inversión de 6,4M€. Está enmarcado en el programa Hazitek 2022 del Gobierno Vasco.**
- **La red eléctrica es un sistema completo y complejo, y lo novedoso de Sec2Grid es que aborda sus múltiples servicios, infraestructuras y equipamientos, para desarrollar medidas de ciberseguridad que eviten posibles ataques y vulnerabilidades.**
- **Destaca asimismo el aspecto colaborativo del proyecto en el que compañías competidoras comparten conocimientos e información en una cuestión tan estratégica como la ciberseguridad.**
- **Participan: Ingeteam, Iberdrola, Arteche, Barbara IoT, Ormazabal, PwC, Zigor, ZIV, Ikerlan y el Clúster GAIA**

30 de marzo de 2023.- La incorporación de nuevas tecnologías y la digitalización están transformando la red eléctrica en una infraestructura inteligente (*Smart Grid*). Esta transformación implica nuevos riesgos, ya que la digitalización expone al sistema energético a ciberataques e incidentes que pueden amenazar la seguridad de la red. **La ciberseguridad de la red eléctrica se ha convertido**, por lo tanto, **en un elemento clave y en uno de los principales retos a los que se enfrenta el sector.**

Ante esta realidad, **10 entidades vascas se han unido en el proyecto Sec2Grid que arrancó el pasado año y se desarrollará hasta finales de 2024 con un presupuesto de 6,4M€.** El objetivo es dotar a toda la cadena de valor del sector eléctrico de la capacidad para responder de una manera coordinada y rápida a los incidentes de ciberseguridad que puedan afectar a la red eléctrica.

Como resultado global del proyecto, se obtendrá una infraestructura creada de manera federada (realizada de manera conjunta y compartiendo los datos consolidados de todos los participantes), para dar soporte a un servicio que sea capaz de buscar y encontrar de manera inteligente las vulnerabilidades en todos los componentes que integran la red eléctrica, utilizando para ello inteligencia artificial y otras tecnologías. Una vez identificadas esas vulnerabilidades, la operadora obtendrá una visión clara de las mismas para analizar su importancia, urgencia de resolución, etc.

En este sentido, desde el consorcio recuerdan que es **fundamental tratar las vulnerabilidades que aparecen en la red eléctrica a lo largo del tiempo antes de que puedan ser utilizadas por posibles atacantes.** Hay que tener en cuenta que un ataque a la red eléctrica -que es una de las principales infraestructuras en un país-, puede tener consecuencias graves e impredecibles en espacios críticos tales como hospitales, bancos, infraestructuras militares, policía, etc.

El Proyecto **Sec2Grid** está financiado por el programa Hazitek 2022 del Gobierno vasco, liderado por **Ingeteam** y cuenta con la participación de **Iberdrola, Arteche, Barbara IoT, Ormazabal, PwC, Zigor, ZIV, Ikerlan y el Clúster GAIA.** Aúna, por tanto, a empresas fabricantes (que desarrollarán su labor en el diseño de los dispositivos finales y que son conocedores del producto), entidades de I+D+i, proveedores de soluciones de ciberseguridad y partners de investigación.

En el marco del proyecto Sec2Grid se contemplan aspectos como:

- Diseño de **mecanismos avanzados de detección precoz de vulnerabilidades**. Para ello, es preciso conocer y mantener todos y cada uno de los componentes desplegados a lo largo y ancho de la red susceptibles de tener algún tipo de vulnerabilidad. Según explican desde Ingeteam: “esto hay que hacerlo en tiempo real y de un modo federado o consolidado. En ciberseguridad el elemento más débil de la cadena es el que marca el nivel de seguridad del sistema. Es necesario abarcar toda la cadena de valor”, inciden.

- También es necesario disponer de **mecanismos de análisis de riesgo acordes a las características de las redes eléctricas.** Estos riesgos son los que podrán utilizarse para tomar las decisiones apropiadas a la hora de saber cómo actuar. Los riesgos hay que evaluarlos teniendo en cuenta el sistema completo.

- Además, hay que ser capaces de **corregir los problemas detectados, probando de un modo ágil y desplegando mediante mecanismos seguros las soluciones desarrolladas**. “En esta fase pueden aparecer retos que no son sencillos de abordar cuando hablamos de equipos que operan en infraestructuras críticas”.

A lo largo del proyecto se desarrollarán diferentes soluciones que se desplegarán como prueba de concepto o **piloto dentro del *Global Smart Grids Innovation Hub* (GSGIH) de Iberdrola en Bilbao,** desde el que la compañía podrá recoger información y hacer chequeo de vulnerabilidades.

Asimismo, el proyecto generará **nuevo conocimiento que pemitirá la innovación en tecnologías y soluciones disruptivas para hacer frente a los retos de ciberseguridad del sector eléctrico**.

Colaboración para llegar más lejos

Una característica peculiar del proyecto es el espíritu colaborativo del mismo. “Participamos un consorcio de empresas que representan de un modo significativo la cadena de valor dentro de la red eléctrica, y nos hemos puesto a trabajar conjuntamente para abordar un problema de primera necesidad como es la ciberseguridad. No hay que olvidar que muchas de las empresas que lo conformamos somos competencia directa, y colaborar de este modo no es algo habitual”, subrayan desde el consorcio.

En este sentido, agregan que disponer de marcos como HAZITEK y clústeres como GAIA que promuevan este tipo de colaboraciones y que sirvan para aunar fuerzas -no solo en el ámbito de optimización de recursos, sino también en el del conocimiento-, “**permiten remar en la misma dirección, obtener resultados más enriquecedores y llegar más lejos en áreas específicas como en este caso la ciberseguridad**”.