

CÓMO ASEGURAR LA CIBERSEGURIDAD. LA IMPORTANCIA DE LA CERTIFICACIÓN Y DE LA CORRECTA DEFINICIÓN DE REQUISITOS DE CIBERSEGURIDAD PARA ASEGURAR UN ENTORNO CIBERSEGURO

**Marta Castro, Saioa Bilbao, Libertad Moro, Mikel Vergara
TECNALIA**

Los sistemas AMI han evolucionado hacia sistemas complejos que incluyen comunicaciones e intercambio de datos. Esta inteligencia y comunicaciones permiten una gestión más eficiente de la red, así como tener una mayor información de las incidencias y hábitos de consumo. Sin embargo, el hecho de tener múltiples puntos de acceso a los equipos de la red implica que existe un mayor riesgo y una mayor exposición a ciberataques.

Los contadores contienen información de carácter confidencial de millones de usuarios y es importante asegurar la confidencialidad de los datos, así como la integridad del remitente de las peticiones, para evitar acceso a dicha información, pero también para evitar una suplantación de identidad y ataques a mayor escala. No obstante, hay que llegar a un compromiso entre el nivel de seguridad y la velocidad y disponibilidad de los datos que se requiere para cada caso de uso. Es por tanto, muy importante analizar las diferentes casuísticas y funcionalidades que existen en la red y los diferentes niveles de seguridad con el que se puede securizar los equipos y los sistemas.

La ciberseguridad y la interoperabilidad de las soluciones de diferentes fabricantes es algo crítico para el correcto despliegue y funcionamiento de los sistemas AMI, de forma que es muy importante definir una metodología que asegure la calidad de los equipos desplegados. Esta metodología parte de la correcta definición de requisitos, hasta la certificación final de los productos.