



## Proyecto SLISE

### Ventajas del 5G en el proyecto SLISE

El 5G supone una gran revolución en el campo tecnológico llegando a conectar multitud de dispositivos en una sola red. Una ventaja que, por ejemplo, permite a Redeia inspeccionar sus activos eléctricos en remoto para seguir optimizando el mantenimiento de sus instalaciones y reforzar su seguridad. También ofrece la oportunidad de independizar los sistemas comunicaciones y optimizar las infraestructuras.

En este marco de actuación, Redeia y su plataforma tecnológica, Elewit, han impulsado el proyecto SLISE. Es una iniciativa centrada en la ciberseguridad y cuyo objetivo es mitigar las posibles vulnerabilidades que las nuevas tecnologías de la arquitectura 5G pueden traer al nuevo paradigma de las comunicaciones como servicio.

Es un proyecto promovido por un consorcio de 8 empresas españolas, entre las que se encuentran Redeia y Elewit, y que tendrá una duración de 37 meses. En su desarrollo, se involucrarán tecnologías que proponen la investigación en **nuevos algoritmos de análisis de incidentes, de cifrado, de identificación y de respuesta automatizada**; en un contexto más flexible para enfrentar los riesgos inherentes a las tecnologías de virtualización.

Todo ello se estudiará, definiendo unos indicadores exigentes que cubran ampliamente estos objetivos, en un conjunto de escenarios de uso que presentan diferentes prioridades de protección y que incluyen el uso de las comunicaciones en el contexto de la gestión de infraestructuras críticas, así como el uso de las comunicaciones en la industria de manufactura.

El proyecto se compone de cuatro líneas de trabajo:

- **Definición de requisitos y casos de uso:** En la que se define de forma detallada los objetivos **técnicos, análisis de requisitos, definición de arquitectura técnica, definición de estructura virtualizada, definición de políticas configurables e interfaces de comunicación y definición y alcance de los sistemas generadores**. Esta primera fase está prevista para realizarse durante este año.
- **Definición de la protección del sistema 5G y detección de ataques y anomalías:** Descripción del sistema de protección 5G y prevención de posibles vulnerabilidades.



- **Análisis de los ataques de inyección, extracción de información y control de sesiones de la actividad:** Estudio de los procesos de extracción de la información mediante un control de la actividad.
- **Evaluación del proyecto:** Análisis y medición de todo lo realizado anteriormente para testar su viabilidad.

Las empresas del consorcio participan en el proyecto como respuesta a su posicionamiento estratégico en sus diferentes objetivos de la ciberseguridad, los distintos riesgos, o el escenario de estudio de las investigaciones. De esta forma **los objetivos de ciberseguridad se alinean con el conjunto de vulnerabilidades más aceptadas en el sector de las comunicaciones para que puedan ser demostrados en un conjunto de escenarios muy relevantes para su validación.**

El consorcio hace este planteamiento porque considera que facilitará la difusión y adopción de los resultados obtenidos, así como la búsqueda de nuevos retos a partir de la experiencia adquirida. La colaboración, complementación y coordinación de todos los miembros del consorcio darán cobertura y solución a todos los objetivos del proyecto.

### **El papel de Elewit, plataforma tecnológica de Redeia**

Desde Elewit, como proveedor tecnológico del sector energético, tenemos como objetivo **desarrollar el estado del arte en los ámbitos en los que es un referente, como son en este caso, la investigación sobre el uso de la IA en la detección de ataques en las subredes compartidas y las exploraciones necesarias para permitir la integración de proveedores con interfaces de comunicación 5G** en las arquitecturas de comunicación gestionadas o controladas por la compañía, ampliando la capacidad de colaboración y desarrollo de negocio

**Este proyecto está financiado por:**



**Financiado por  
la Unión Europea**  
NextGenerationEU