inc be lab_

Laboratorio, *test center* y centro demostrador de ciberseguridad de nuevas tecnologías de INCIBE

Objetivos

01. Elevar
la ciberseguridad y la resiliencia, además de aumentar la confianza digital en las tecnologías emergentes como las comunicaciones **5G**, el **Internet de las Cosas (IoT)** o la **Inteligencia Artificial (IA)**.

02. Posilibitar
que los centros de investigación, empresas y demás agentes relacionados puedan ensayar diferentes **soluciones** que estén desarrollando, reduciendo el coste y el tiempo necesario para poner en el mercado nuevos productos.

A través de

- Los mecanismos de los **fondos Next Generation EU** y en el marco del plan estratégico de INCIBE.
- La adopción de regulaciones de ciberseguridad en nuevas tecnologías, como el **Esquema Nacional de Ciberseguridad 5G o la 'Cyber Resilience Act' (CRA) de la Comisión Europea**.
- La estrecha colaboración con fabricantes **líderes en el sector y un grupo experto de la Universidad de León**, para la compartición de conocimiento y experiencia.
- Espacios colaborativos y dinamizando la relación entre fabricantes de **tecnología 5G e IoT**, y los laboratorios privados en España.
- **Dos grandes proyectos**:

IoT
Evaluación de ciberseguridad de dispositivos domésticos conectados (IoT).

Redes 5G
Evaluación de ciberseguridad para redes 5G.

Evaluación de ciberseguridad de **dispositivos conectados (IoT)**

Establecimiento
de las bases técnica y tecnológica para llevar a cabo una **vigilancia de mercado que permita supervisar el cumplimiento de la futura normativa CRA** (Cyber Resilience Act).

Metodología
para medir el nivel de ciberseguridad de dispositivos **IoT** de consumidor, con alta presencia en hogares:

- *Electrodomésticos*
- *Enchufes inteligentes*
- *Bombillas inteligentes*
- *Cámaras IP*
- *Juguetes*

¿Cómo lo hacemos?

Mediante un **banco o sistema de pruebas** que se pueda ajustar y adaptar a futuras necesidades:

Contamos con un conjunto de **herramientas** de ciberseguridad y escenarios de prueba que simulan entornos reales.

Tenemos un proceso de evaluación que incluye un total de **202 pruebas específicas** mediante las cuales se verifican distintos requisitos de ciberseguridad, de protección de datos y superficies de ataque.

Evaluación de ciberseguridad de **redes 5G**

Refuerzo
de la capacidad técnica y tecnológica del Ministerio para la Transformación Digital y de la Función Pública para el ejercicio de sus funciones en el **Esquema Nacional de Seguridad de redes y servicios 5G** (Real Decreto 443/2024, de 30 de abril).

Metodología
de análisis de ciberseguridad de **redes 5G**, basada en los estándares de referencia internacionales (GSMA y 3GPP).

¿Cómo lo hacemos?

- Desarrollando un **procedimiento técnico de evaluación** de propósito general aplicable a los distintos elementos y funciones que componen una red 5G:

  Capacidad para llevar a cabo **78 pruebas distintas** de ciberseguridad sobre cada elemento.

  Flexible y actualizable a las futuras amenazas que afecten a elementos 5G.

- Construyendo un **entorno tecnológico** altamente equipado, constituido por:

  Redes privadas 5G reales de los principales fabricantes.

  Conjunto de **herramientas de evaluación.**

  Infraestructura de evaluación y *hardware* para configurar los escenarios de prueba.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD