



## Cátedra Internacional "Smart Rural IoT and Secured Environments"

# Guía Formativa y Divulgativa

## Observatorio SRISE - IoT, Ciberseguridad y entornos Rurales

Diciembre 2025

*Este documento forma parte de la Cátedra Internacional "Smart Rural IoT and Secured Environments", financiado por el Plan de Recuperación, Transformación y Resiliencia de la Unión Europea NextGeneration-EU, a través de INCIBE».*





## Contenido

|                                                              |   |
|--------------------------------------------------------------|---|
| 1. Presentación .....                                        | 3 |
| 2. Conceptos básicos del Internet de las Cosas (IoT).....    | 3 |
| 3. Riesgos y vulnerabilidades en entornos rurales.....       | 3 |
| 4. Soluciones de seguridad y enfoques preventivos .....      | 4 |
| 5. Laboratorio, experimentación y aprendizaje práctico ..... | 4 |
| 6. Formación reglada y cursos especializados .....           | 5 |
| 7. Divulgación para públicos no técnicos.....                | 5 |
| 8. Recursos adicionales .....                                | 5 |
| 9. Bibliografía y lecturas recomendadas .....                | 6 |
| 10. Cierre .....                                             | 6 |



## 1. Presentación

La presente *Guía Formativa y Divulgativa* se enmarca en las actividades de la Cátedra Internacional SRISE con el objetivo de promover la investigación, la formación y la divulgación del conocimiento en el ámbito del Internet de las Cosas (IoT) y la ciberseguridad, con especial atención a su aplicación en entornos rurales.

Esta guía está concebida como un instrumento accesible y pedagógico, dirigido a un público amplio que incluye estudiantes universitarios, personal docente e investigador, técnicos de administraciones locales y ciudadanía interesada en comprender y utilizar de forma segura las tecnologías digitales en el territorio. Su enfoque combina rigor técnico con vocación divulgativa, facilitando la comprensión de conceptos clave y fomentando una cultura de seguridad digital adaptada a las necesidades del medio rural.

---

## 2. Conceptos básicos del Internet de las Cosas (IoT)

El Internet de las Cosas constituye un ecosistema tecnológico basado en la interconexión de dispositivos físicos capaces de capturar datos del entorno y comunicarlos a sistemas de procesamiento. Una arquitectura IoT típica se compone de sensores y actuadores, dispositivos de adquisición, pasarelas de comunicación (*gateways*), capas de computación en el borde (*edge computing*) y plataformas en la nube para almacenamiento y análisis.

La comunicación entre estos elementos se apoya en protocolos específicos diseñados para entornos con restricciones de energía, ancho de banda o latencia. Entre los más utilizados se encuentran MQTT y CoAP, orientados a comunicaciones ligeras, y LoRaWAN, especialmente relevante en entornos rurales por su largo alcance y bajo consumo energético.

El despliegue de estos sistemas introduce también nuevas superficies de ataque. Entre las amenazas más habituales se incluyen los ataques de denegación de servicio, la intrusión en dispositivos mal protegidos y la manipulación o interceptación de datos transmitidos.

---

## 3. Riesgos y vulnerabilidades en entornos rurales

Los sistemas IoT desplegados en entornos rurales presentan vulnerabilidades específicas derivadas tanto de limitaciones técnicas como de factores organizativos. El uso de contraseñas por defecto, la falta de actualización del firmware o la ausencia de mecanismos de autenticación robusta son ejemplos de debilidades frecuentes.

En este contexto, pueden producirse ataques como la manipulación de sensores agrícolas, el acceso no autorizado a dispositivos de monitorización ambiental o la alteración de sistemas de control de infraestructuras locales. Las consecuencias de estos incidentes van desde la pérdida



o corrupción de datos hasta la interrupción de servicios esenciales e incluso riesgos para la seguridad física de personas y bienes.

La identificación y comprensión de estos riesgos resulta fundamental para concienciar a los distintos actores implicados y promover prácticas responsables en el uso de la tecnología.

---

## 4. Soluciones de seguridad y enfoques preventivos

La mitigación de los riesgos asociados a la IoT requiere la adopción de un conjunto de buenas prácticas de seguridad. Entre ellas destacan la utilización de mecanismos de autenticación robusta, el cifrado de los datos tanto en tránsito como en reposo y la aplicación de políticas de actualización periódica del software y firmware de los dispositivos.

La Inteligencia Artificial desempeña un papel creciente en la detección temprana de ataques, mediante el análisis de patrones de comportamiento anómalos y la identificación de desviaciones respecto al funcionamiento normal de los sistemas. Estas técnicas permiten mejorar la capacidad de respuesta ante incidentes de seguridad.

Asimismo, el enfoque de *secure by design* promueve la integración de la seguridad desde las fases iniciales de diseño de los sistemas, evitando soluciones reactivas y reduciendo la aparición de vulnerabilidades estructurales.

---

## 5. Laboratorio, experimentación y aprendizaje práctico

La formación en IoT y ciberseguridad se refuerza mediante actividades prácticas que permiten aplicar los conocimientos adquiridos en contextos controlados. La simulación de escenarios IoT mediante software educativo facilita la comprensión del funcionamiento de los sistemas y de los posibles vectores de ataque.

El Observatorio SRISE promueve el uso de laboratorios remotos, como la plataforma IoT@UNED, que permiten el acceso a recursos experimentales reales sin necesidad de desplazamiento. Estas herramientas resultan especialmente valiosas para estudiantes y profesionales ubicados en zonas rurales.

Además, se fomentan retos prácticos, como ejercicios tipo *Capture the Flag* o el diseño de prototipos IoT seguros, que favorecen el aprendizaje activo y el desarrollo de competencias técnicas.



## 6. Formación reglada y cursos especializados

La Cátedra SRISE impulsa una oferta formativa orientada a distintos niveles de conocimiento, que incluye cursos en línea abiertos y actividades presenciales. Entre ellos destaca el MOOC *"IA Technologies for Cybersecurity and IoT"*, accesible a través del portal oficial de la Cátedra.

Asimismo, se organizan cursos de verano de la UNED centrados en IoT y ciberseguridad, así como recursos docentes complementarios como laboratorios, estudios de caso y guías prácticas, diseñados para apoyar tanto la docencia universitaria como la formación continua.

## 7. Divulgación para públicos no técnicos

Una parte esencial de la misión del Observatorio SRISE es acercar el conocimiento tecnológico a públicos no especializados. Para ello, se desarrollan materiales divulgativos que abordan preguntas frecuentes sobre IoT y ciberseguridad en entornos rurales, ofreciendo explicaciones claras y accesibles.

Estos contenidos incluyen consejos prácticos de seguridad para usuarios finales y ejemplos de casos de uso reales, como aplicaciones de IoT seguro en agricultura, gestión energética o movilidad local. El objetivo es fomentar un uso informado y responsable de la tecnología, reduciendo la brecha digital.

## 8. Recursos adicionales

La presente guía se apoya en recursos externos contrastados que permiten ampliar y actualizar los conocimientos en materia de IoT, ciberseguridad y territorios inteligentes. Como mínimo, se recomiendan las siguientes referencias institucionales y educativas:

- **INCIBE – Guías y estudios de ciberseguridad:** repositorio oficial de guías prácticas, informes y materiales divulgativos sobre seguridad digital en distintos ámbitos, incluyendo ciudadanía, educación y sector público. Disponible en: <https://www.incibe.es/guias>
- **Proyecto "Ciberseguridad en aulas conectadas" (IoTSafeEdu):** iniciativa orientada a la concienciación y formación en ciberseguridad aplicada a entornos educativos conectados, con materiales didácticos y casos prácticos. Disponible en: <https://iotsafeedu.com/el-proyecto/>
- **Guías de Smart Rural de la Junta de Castilla y León:** conjunto de guías divulgativas centradas en la aplicación de tecnologías inteligentes en zonas rurales, con especial atención a sostenibilidad, digitalización y servicios públicos. Referenciadas en: <https://www.20minutos.es/noticia/5048748/0/la-junta-publica-seis-guias-divulgativas-sobre-aplicacion-del-territorio-inteligente-en-zonas-rurales/>



Estos recursos constituyen una base mínima de referencia para actividades formativas, divulgativas y de sensibilización promovidas por el Observatorio SRISE.

---

## 9. Bibliografía y lecturas recomendadas

Para profundizar en los contenidos abordados en esta guía, se recomienda la consulta de bibliografía académica y recursos docentes contrastados, entre los que se incluyen:

- **Universidad VIU.** *Redes avanzadas, IoT y servicios de nueva generación.* Material docente universitario orientado a la comprensión de arquitecturas de red, servicios IoT y tecnologías emergentes.
- **ArXiv (2023).** *Adaptive Smart Environments for Cybersecurity Education.* Artículo académico centrado en el uso de entornos inteligentes adaptativos para la formación en ciberseguridad.
- **UNED.** *Curso MOOC: IA Technologies for Cybersecurity and IoT.* Curso abierto en línea que aborda la aplicación de técnicas de Inteligencia Artificial a la ciberseguridad y al Internet de las Cosas.

Estas referencias constituyen un punto de partida sólido para la ampliación de conocimientos y la actualización continua en el ámbito de la IoT segura y la ciberseguridad aplicada.

---

## 10. Cierre

La presente Guía Formativa y Divulgativa constituye una herramienta clave para la difusión del conocimiento y la capacitación en IoT y ciberseguridad en entornos rurales. Su enfoque accesible, combinado con el rigor técnico, contribuye a fortalecer las capacidades digitales del territorio, promoviendo el desarrollo de entornos inteligentes seguros, inclusivos y sostenibles.