



Cátedra Internacional "Smart Rural IoT and Secured Environments"

Guía Metodología del Laboratorio

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. Resumen.....	3
2. Introducción.....	3
3. Principios metodológicos.....	3
1. Investigación aplicada y experimental.....	3
2. Colaboración institucional.....	3
3. Optimización para entornos limitados.....	4
4. Transferencia y formación continua.....	4
5. Ética, calidad y gobernanza abierta.....	4
4. Fases de trabajo.....	5
Fase 1: Planificación.....	5
Fase 2: Infraestructura experimental.....	5
Fase 3: Desarrollo de modelos y detección.....	5
Fase 4: Transferencia y difusión.....	5
Fase 5: Formación.....	5
5. Evaluación y seguimiento.....	6
6. Gestión de riesgos.....	6
Riesgos y medidas de mitigación:.....	6
7. Transparencia y datos abiertos.....	6
8. Contribución al territorio rural.....	6



1. Resumen

Esta memoria describe de forma detallada la metodología de trabajo de la Cátedra-Laboratorio *Smart Rural IoT and Secured Environments*. El documento establece un marco estructurado que integra investigación aplicada, desarrollo experimental, formación especializada y transferencia de conocimiento, con el objetivo de generar impacto científico, tecnológico y social en entornos rurales.

La metodología propuesta sirve como guía de buenas prácticas para la coordinación institucional, la ejecución de proyectos de I+D+i, la gestión responsable de datos y la difusión de resultados. Asimismo, está orientada a fortalecer la resiliencia digital, la ciberseguridad y la adopción de tecnologías IoT en territorios rurales, contribuyendo a su sostenibilidad y competitividad.

2. Introducción

La metodología de la Cátedra tiene como misión garantizar que todas las actividades de investigación, formación y transferencia se desarrollen con rigor científico, coherencia metodológica y orientación a resultados. Se apoya en un enfoque interdisciplinar que combina ingeniería, ciencias de la computación, ciberseguridad y análisis socioeconómico del territorio.

El marco metodológico se articula sobre tres ejes fundamentales: **ciberseguridad**, **Internet de las Cosas (IoT)** y **entornos rurales inteligentes**, alineándose con las estrategias europeas de digitalización, resiliencia y desarrollo territorial. La colaboración entre la UNED, la Universidade NOVA y el Consorcio de Ponferrada permite integrar capacidades académicas, tecnológicas y territoriales, favoreciendo una aproximación realista y aplicada.

3. Principios metodológicos

1. Investigación aplicada y experimental

- La Cátedra prioriza la investigación aplicada orientada a la resolución de problemas reales en entornos rurales. Para ello, se combinan experimentos en entornos reales con simulaciones controladas que permiten validar hipótesis de forma segura y reproducible.
- Se utilizan redes IoT instrumentadas, bancos de pruebas (testbeds) y sandboxes que facilitan la captura de datos de tráfico, sensores y metadatos. Este enfoque experimental posibilita el análisis profundo de amenazas, vulnerabilidades y comportamientos anómalos, así como la evaluación comparativa de distintas soluciones tecnológicas.

2. Colaboración institucional

- La metodología se fundamenta en una gobernanza colaborativa claramente definida. La UNED asume la coordinación científica y operativa, asegurando la coherencia metodológica



y la calidad académica de los resultados. La Universidade NOVA contribuye con su experiencia en entornos simulados, inteligencia artificial y laboratorios avanzados, mientras que el Consorcio de Ponferrada proporciona infraestructura física, acceso al territorio y recursos humanos especializados.

- Esta cooperación institucional favorece la transferencia bidireccional de conocimiento y la optimización de recursos, evitando duplicidades y potenciando sinergias.

3. Optimización para entornos limitados

- Los entornos rurales presentan restricciones específicas en términos de conectividad, disponibilidad energética y capacidad de cómputo. Por ello, la metodología incorpora desde su diseño la optimización de modelos y arquitecturas para dispositivos de bajo consumo, como nodos edge y fog.
- Se evalúan métricas de latencia, consumo energético, robustez y fiabilidad, garantizando que las soluciones desarrolladas sean viables en escenarios reales y sostenibles a largo plazo.

4. Transferencia y formación continua

- La transferencia de conocimiento constituye un pilar esencial de la metodología. Los resultados obtenidos se publican, siempre que sea posible, en abierto, facilitando su reutilización por la comunidad científica, las administraciones y el sector productivo.
- Paralelamente, se desarrollan acciones formativas continuas mediante cursos, seminarios, MOOCs y eventos divulgativos.
- El Observatorio actúa como nodo de seguimiento de tendencias tecnológicas (en IA, IoT y ciberseguridad), promoviendo la actualización permanente de contenidos y competencias.

5. Ética, calidad y gobernanza abierta

- La metodología incorpora principios éticos y de calidad en todas las fases del trabajo. Se aplican buenas prácticas de gestión de datos, alineadas con los principios FAIR, y se elaboran planes de gestión que garantizan la seguridad, privacidad y trazabilidad de la información.
- Asimismo, se definen indicadores clave de rendimiento (KPIs) para medir impacto científico, transferencia tecnológica y formación de talento, promoviendo la transparencia y la rendición de cuentas entre las instituciones participantes.



4. Fases de trabajo

Fase 1: Planificación

- En esta fase se define el plan operativo global de la Cátedra, incluyendo objetivos de investigación, transferencia y formación.
- Se asignan responsabilidades, se establecen cronogramas y se identifican recursos necesarios.
- Los KPIs definidos permiten monitorizar el progreso y realizar ajustes tempranos.

Fase 2: Infraestructura experimental

- Se despliegan redes IoT basadas en tecnologías como LoRa, ZigBee, MQTT y CoAP, adaptadas a escenarios rurales.
- Paralelamente, se implementan entornos simulados, honeypots y laboratorios virtuales que permiten reproducir ataques y escenarios de fallo.
- La captura sistemática de datos incluye tráfico de red, señales de sensores y metadatos contextuales, garantizando la calidad y representatividad de los conjuntos de datos.

Fase 3: Desarrollo de modelos y detección

- A partir de los datos recopilados, se desarrollan y entrenan modelos de inteligencia artificial orientados a la detección de anomalías, intrusiones y fallos.
- Se evalúan métricas de precisión, robustez y eficiencia computacional
- Optimización para hardware de bajo consumo (FPGAs, microcontroladores...).

Fase 4: Transferencia y difusión

- Los resultados se difunden a través de informes en el Observatorio AI4IoT, publicaciones científicas y participación en congresos.
- Se organizan jornadas y eventos dirigidos a empresas, administraciones, universidades y ciudadanía, fomentando la adopción de las soluciones desarrolladas..

Fase 5: Formación

- Diseño de cursos (Título de Experto, MOOCs) orientados a distintos perfiles.
- Premios a TFG, TFM y tesis para impulsar el talento.
- Evaluación con métricas de satisfacción y seguimiento de egresados.



5. Evaluación y seguimiento

- KPIs principales: diseño de redes IoT, número de modelos IA, publicaciones, patentes, asistentes a eventos, matriculados en cursos, premios, visitas al observatorio.
- Reuniones periódicas entre instituciones.
- Dashboards para visualizar indicadores.
- Ajustes metodológicos basados en resultados y *feedback*.

6. Gestión de riesgos

Riesgos y medidas de mitigación:

Riesgo	Plan de mitigación
Falta de financiación	Colaboraciones externas y optimización de recursos existentes.
Retrasos en actividades	Redistribución de recursos y ajuste del cronograma.
Escasa participación en cursos o premios	Mayor difusión y colaboración con entidades públicas y empresas.
Problemas técnicos en redes IoT rurales	Pilotos previos, validación en escenarios reales y uso de IA ligera.

7. Transparencia y datos abiertos

- Los datasets generados se gestionan bajo políticas de acceso abierto siempre que sea posible, respetando la normativa vigente.
- Documentación pública de experimentos y métodos (cuadernos de laboratorio, informes técnicos), reforzando la reproducibilidad y la confianza en los resultados.
- El Observatorio AI4IoT publica informes, boletines y análisis periódicos.

8. Contribución al territorio rural

- Impulso a la innovación en la "España vaciada" mediante tecnología IoT y ciberseguridad.
- Participación de administraciones, empresas y ciudadanos para co-crear soluciones reales.



- Formación de talento local mediante cursos y prácticas para fortalecer capacidades en la región.

Estas acciones fortalecen las capacidades locales y favorecen un desarrollo digital equilibrado y sostenible.