



Departamento de
Sistemas de
Comunicación
y Control



Ponferrada

Cátedra Internacional "Smart Rural IoT and Secured Environments"

Guía de Referencia y Normativa

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».



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE POLÍTICAS DIGITALES
E INICIATIVAS TURNO-2025



Plan de
Recuperación,
Transformación
y Resiliencia



INCIBE
INSTITUTO NACIONAL DE CIBERSEGURIDAD





Contenido

1. Introducción.....	3
2. Marco normativo legal: ámbito nacional y europeo	3
Reglamento General de Protección de Datos (RGPD).....	3
Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).....	4
Medidas de Seguridad y Privacidad	4
3. Estándares técnicos y de seguridad aplicables	4
3.1 ISO/IEC 30141:2024 — Arquitectura de referencia para IoT	4
3.2 ISO/IEC 27400:2022 — Ciberseguridad y privacidad en IoT.....	5
3.3 ISO/IEC 27404:2025 — Etiquetado de seguridad en IoT	5
3.4 ISA/IEC 62443 — Seguridad en sistemas de automatización y control	5
3.5 ITU-T Y.2060 — Marco global de IoT.....	5
4. Buenas prácticas normativas y operativas.....	5
4.1 Evaluación y gestión de riesgos.....	5
4.2 Privacidad desde el diseño y por defecto	5
4.3 Gobernanza de los datos	6
5. Coordinación institucional y cumplimiento	6
6. Conclusión	6



1. Introducción

La presente *Guía de Referencia y Normativa* tiene como objetivo establecer el marco legal, normativo y de estándares técnicos que rige las actividades desarrolladas en el ámbito del Observatorio SRISE y de la Cátedra-Laboratorio "Smart Rural IoT and Secured Environments". Este documento amplía y consolida los contenidos inicialmente planteados, transformándolos en una referencia normativa estructurada, coherente y aplicable en la práctica.

La guía describe los principios metodológicos que sustentan las actuaciones del Observatorio, así como las obligaciones legales y técnicas que deben cumplirse en el diseño, despliegue y operación de soluciones basadas en IoT, analítica avanzada e Inteligencia Artificial en entornos rurales. Asimismo, aborda aspectos clave como la evaluación de riesgos, la transparencia, la gobernanza de los datos y la contribución al desarrollo territorial, alineando la actividad tecnológica con los valores de responsabilidad social y sostenibilidad.

Este documento sirve, por tanto, como una herramienta de apoyo a la toma de decisiones, a la coordinación institucional y a la transferencia de conocimiento, garantizando que todas las actuaciones se desarrollen conforme a la normativa vigente y a las mejores prácticas reconocidas a nivel nacional e internacional.

2. Marco normativo legal: ámbito nacional y europeo

El desarrollo de actividades basadas en la gestión intensiva de datos y el despliegue de sistemas IoT requiere un estricto cumplimiento del marco legal vigente, especialmente en lo relativo a la protección de datos personales y los derechos digitales.

Reglamento General de Protección de Datos (RGPD)

El Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (RGPD), constituye la norma fundamental en materia de protección de datos personales en el ámbito europeo. Su aplicación es obligatoria para cualquier tratamiento de datos que permita identificar directa o indirectamente a una persona física.

En el contexto del Observatorio SRISE, el RGPD resulta especialmente relevante en aquellas actividades que implican la recogida de datos procedentes de sensores, plataformas digitales o sistemas de monitorización que puedan asociarse a personas, ubicaciones o comportamientos. El cumplimiento del RGPD exige definir bases legales para el tratamiento, aplicar el principio de minimización de datos, garantizar la seguridad de la información y respetar los derechos de las personas interesadas.



Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

La Ley Orgánica 3/2018 complementa y desarrolla el RGPD en el ordenamiento jurídico español. Esta norma regula de forma específica los derechos digitales, así como las obligaciones de responsables y encargados del tratamiento.

Entre los aspectos más relevantes para el Observatorio se incluyen la obligación de mantener un registro de actividades de tratamiento, la aplicación de medidas técnicas y organizativas apropiadas, y la garantía de los derechos de acceso, rectificación, supresión y limitación del tratamiento. La LOPDGDD refuerza, además, la necesidad de anonimizar o seudonimizar los datos siempre que sea posible, especialmente en contextos de investigación y análisis.

Las referencias legales completas se encuentran disponibles en el Boletín Oficial del Estado (BOE), y deberán ser consultadas y actualizadas de forma periódica.

Medidas de Seguridad y Privacidad

Para asegurar el cumplimiento del marco legal, el Observatorio SRISE deberá implementar medidas de seguridad adecuadas al nivel de riesgo de los tratamientos realizados. Estas medidas incluyen el control de acceso a la información, el cifrado de los datos tanto en tránsito como en reposo, la aplicación de técnicas de seudonimización o anonimización, y el registro sistemático de las actividades de tratamiento.

La adopción de estas medidas no solo responde a una obligación legal, sino que constituye un elemento esencial para generar confianza entre los actores implicados y garantizar la sostenibilidad de las actividades del Observatorio.

3. Estándares técnicos y de seguridad aplicables

Además del marco legal, el Observatorio SRISE se apoya en estándares técnicos internacionales que proporcionan directrices reconocidas para el diseño, implementación y operación de sistemas IoT seguros e interoperables.

3.1 ISO/IEC 30141:2024 — Arquitectura de referencia para IoT

La norma ISO/IEC 30141 define una arquitectura de referencia para sistemas IoT, proporcionando un marco conceptual que facilita la interoperabilidad, la escalabilidad y la integración de componentes heterogéneos. Esta norma sirve como base para el diseño de la arquitectura técnica del Observatorio, permitiendo una evolución ordenada de sus infraestructuras.



3.2 ISO/IEC 27400:2022 — Ciberseguridad y privacidad en IoT

La ISO/IEC 27400 establece principios y guías para la gestión de riesgos de ciberseguridad y privacidad en entornos IoT. Su aplicación permite identificar amenazas, definir controles de seguridad y proteger tanto los dispositivos como los datos y servicios asociados.

3.3 ISO/IEC 27404:2025 — Etiquetado de seguridad en IoT

Este estándar propone un marco para el etiquetado del nivel de seguridad y privacidad de los productos IoT, facilitando la evaluación de riesgos y la toma de decisiones informadas. Su adopción contribuye a la transparencia y a la mejora de la confianza en los sistemas desplegados.

3.4 ISA/IEC 62443 — Seguridad en sistemas de automatización y control

La serie de normas ISA/IEC 62443 establece requisitos y buenas prácticas para la protección de sistemas industriales y de automatización, aplicables también a infraestructuras IoT en entornos rurales. Estas normas resultan especialmente relevantes en casos de uso relacionados con energía, agua, agricultura o infraestructuras críticas.

3.5 ITU-T Y.2060 — Marco global de IoT

La recomendación ITU-T Y.2060 proporciona una definición conceptual y arquitectónica del Internet de las Cosas, estableciendo un marco global que complementa los estándares ISO y facilita la alineación con iniciativas internacionales.

4. Buenas prácticas normativas y operativas

4.1 Evaluación y gestión de riesgos

La evaluación de riesgos deberá abordarse de forma sistemática, combinando la gestión de la seguridad de la información conforme a la norma ISO/IEC 27005 con el cumplimiento de las obligaciones derivadas del RGPD y la LOPDGDD. Esta evaluación permitirá identificar amenazas técnicas, legales y organizativas, así como definir medidas de mitigación proporcionadas.

4.2 Privacidad desde el diseño y por defecto

El Observatorio SRISE adoptará el enfoque de *Privacy by Design* y *Privacy by Default*, integrando la protección de la privacidad desde las fases iniciales de cualquier proyecto. Esto implica limitar la cantidad de datos recogidos, aplicar técnicas de anonimización o seudonimización siempre que sea viable, y garantizar la transparencia en el tratamiento de los datos y la obtención del consentimiento cuando corresponda.



4.3 Gobernanza de los datos

La gobernanza de los datos requiere la definición de políticas claras que regulen el registro, almacenamiento, acceso, uso y eliminación de la información. Estas políticas deberán contemplar mecanismos de control, clasificación de los datos según su sensibilidad y procedimientos internos de auditoría, revisión y mejora continua.

Una gobernanza sólida permite asegurar el cumplimiento normativo, mejorar la calidad de los datos y facilitar la rendición de cuentas.

5. Coordinación institucional y cumplimiento

La aplicación efectiva de esta guía requiere una coordinación estrecha entre las distintas unidades y entidades implicadas en el Observatorio SRISE. Se deberán establecer responsabilidades claras en materia de cumplimiento normativo, seguridad de la información y protección de datos, así como canales de comunicación que faciliten la resolución de incidencias y la actualización de los procedimientos.

6. Conclusión

Las normativas y estándares descritos en esta Guía de Referencia y Normativa son plenamente aplicables a un observatorio institucional universitario en España. Su correcta implementación garantiza el cumplimiento legal, la protección de los datos personales, la seguridad de las infraestructuras IoT y la creación de entornos inteligentes confiables.

Este documento proporciona un marco sólido para el desarrollo responsable de iniciativas tecnológicas en entornos rurales, reforzando la credibilidad institucional del Observatorio SRISE y contribuyendo a la generación de valor social, científico y territorial.