Observatorio de
Transición Justa
de Asturias

Principado de
Asturias

Mejorar las redes eléctricas con gemelos digitales. Oportunidades e impactos.

1. INTRODUCCIÓN. 5
2. ESTADO DEL ARTE. AÑO 2026. 8
2.1 REDES INTELIGENTES. DEFINICIÓN 8
2.1.1 IMPACTO ECONÓMICO SOBRE EL CONSUMIDOR DOMÉSTICO. 9
2.1.2 IMPACTO ECONÓMICO SOBRE CONSUMIDORES COMERCIALES Y TERCIARIOS. 11
2.1.3 IMPACTO ECONÓMICO EN CONSUMIDORES INTENSIVOS. 13
2.1.4 NORMA IEC 61850. 14
2.1.5 FLEXIBILIDAD ENERGÉTICA COMO NUEVO RECURSO ECONÓMICO. 16
2.1.6 INTEGRACIÓN DE GENERACIÓN RENOVABLE Y AUTOCONSUMO INDUSTRIAL. . 18
2.1.7 LIMITACIONES ECONÓMICAS ACTUALES. 19
2.2 IMPACTO AMBIENTAL DE LAS REDES INTELIGENTES EN ASTURIAS. 19
2.2.1 CONTRIBUCIÓN A LA DESCARBONIZACIÓN DEL SISTEMA ELÉCTRICO. 20
2.2.2 REDUCCIÓN DE PÉRDIDAS ENERGÉTICAS. 21
2.2.3 IMPULSO AL AUTOCONSUMO Y LA GENERACIÓN DISTRIBUIDA. 21
2.2.4 ELECTRIFICACIÓN DE SECTORES ESTRATÉGICOS. 23
2.3 GEMELOS DIGITALES Y SU INTEGRACIÓN EN LAS REDES INTELIGENTES. 24
2.3.1 DEFINICIÓN Y COMPONENTES ESENCIALES. 24
2.3.2 MARCO DE REFERENCIA: EL MODELO NIST DE SMART GRID. 25
2.3.3 HERRAMIENTAS Y TECNOLOGÍAS HABILITADORAS. 27
2.3.4 APLICACIONES POR DOMINIO DE GENERACIÓN Y DISTRIBUCIÓN. 30
2.3.5 ANÁLISIS DE IMPACTO: SOCIAL, ECONÓMICO Y AMBIENTAL. 31
2.3.6 CIBERSEGURIDAD. 35
2.3.7 PANORAMA DE AMENAZAS Y JUSTIFICACIÓN REGULATORIA. 36
2.3.8 DIRECTIVA NIS2. 38
2.3.9 MEDIDAS DE GESTIÓN DE RIESGOS. 39
2.3.10 OBLIGACIÓN DE NOTIFICACIÓN DE INCIDENTES. 44
2.3.11 SISTEMA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y COORDINACIÓN AUTONÓMICA. 44
2.3.12 INTERACCIÓN ENTRE EL RÉGIMEN CNPIC Y LA NIS2. 45
2.3.13 NORMAS TÉCNICAS DE REFERENCIA PARA EL GEMELO DIGITAL. 46
2.3.14 REQUISITOS DE ARQUITECTURA SEGURA DEL GEMELO DIGITAL. 48
2.3.15 IMPACTO ECONÓMICO DEL CUMPLIMIENTO DE LA CIBERSEGURIDAD EN ASTURIAS. 50
2.3.16 IMPACTO SOCIAL Y AMBIENTAL DE LA CIBERSEGURIDAD. 51

2.4 MARCO LEGISLATIVO SOBRE EL DATO. 52
2.4.1 TRATAMIENTO DE DATOS DE USUARIOS DE LA RED. 53
2.4.2 BASES JURÍDICAS DEL TRATAMIENTO. 53
2.4.3 EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS. 54
2.4.4 DERECHOS DE LOS USUARIOS. 54
2.4.5 INTERCAMBIABILIDAD E INTERCAMBIO DE DATOS ENTRE EMPRESAS. 55
2.4.6 DIRECTIVA 2019/944/UE Y MODELO DE ACCESO A DATOS. 55
2.4.7 EL DATA ACT (REGLAMENTO UE 2023/2854) Y LOS DATOS B2B. 55
2.4.8 EL DATA GOBERNANCE ACT (REGLAMENTO UE 2022/868) Y EL ESPACIO EUROPEO DE DATOS ENERGÉTICOS. 56
2.4.9 LÍMITES AL INTERCAMBIO: SECRETO INDUSTRIAL Y SEGURIDAD. 56
2.4.10 PROTECCIÓN Y ALMACENAMIENTO DE DATOS. 57
2.4.11 IMPACTO ECONÓMICO DE LA REGULACIÓN. 59
2.4.12 IMPACTO SOCIAL DE LA REGULACIÓN. 60
2.4.13 IMPACTO AMBIENTAL DE LA REGULACIÓN. 61
3. IA EN REDES ELÉCTRICAS INTELIGENTES. 62
3.1 ECOSISTEMA DE IA PARA REDES INTELIGENTES. 62
3.2 MACHINE LEARNING. 63
3.3 DEEP LEARNING (DL). 64
3.3.1 IMPACTO DEL DEEP LEARNING. 66
3.4 REINFORCEMENT LEARNING (RL). 67
3.4.1 DEEP REINFORCED LEARNING (DRL) Y APLICACIONES CONCRETAS. 68
3.4.2 MULTI-AGENT REINFORCED LEARNING. 68
3.4.3 IMPACTO DEL REINFORCED LEARNING. 69
3.5 FEDERATED LEARNING (FL). 69
3.5.1 ARQUITECTURAS Y VARIANTES. 70
3.5.2 APLICACIONES EN LA RED ASTURIANA. 71
3.5.3 IMPACTO DEL FEDERATED LEARNING. 71
3.6 LLM: GRANDES MODELOS DE LENGUAJE Y SU APLICACIÓN EN LA RED. 71
3.6.1 ADAPTACIÓN AL DOMINIO ENERGÉTICO. 72
3.6.2 INTELIGENCIA GENERATIVA PARA GESTIÓN DE RED Y CIBERSEGURIDAD. 72
3.6.3 LIMITACIONES DE LOS LLMS. 73
3.6.4 IMPACTO DE LOS LLMS. 73

4. ARQUITECTURA PROPUESTA 74
4.1 CAPA FÍSICA: ACTIVOS E INFRAESTRUCTURA DE LA RED ASTURIANA. 74
4.2 CAPA DE COMUNICACIONES: CONECTIVIDAD E INTEROPERABILIDAD 75
4.3 CAPA DE MODELADO Y SIMULACIÓN. 76
4.4 CAPA DE DECISIÓN E INTEGRACIÓN DE LOS LLMS. 77
4.5 IMPACTO ECONÓMICO. 77
4.6 IMPACTO SOCIAL. 78
4.7 IMPACTO AMBIENTAL. 78
5. LIMITACIONES DE LAS REDES INTELIGENTES. 79
5.1 LIMITACIONES TÉCNICAS 79
5.2 RETOS RELACIONADOS CON LA GENERACIÓN DISTRIBUIDA. 80
5.3 RETOS DEL EQUILIBRIO DE LA RED Y SU SENSIBILIDAD 80
5.4 RETOS RELACIONADO CON LA CONGESTIÓN. 81
5.5 CIBERSEGURIDAD Y SEGURIDAD FISICA COMO RIESGOS CONVERGENTES. 82
5.6 ESCALABILIDAD DEL GEMELO DIGITAL 82
5.7 FALSOS POSITIVOS Y FATIGA POR ALERTAS. 83
5.8 DEPENDENCIA DE LA SINCRONIZACIÓN TEMPORAL. 84
5.9 VIDA ÚTIL DESIGUAL DE LOS COMPONENTES. 84
5.10 EXCESO DE PARADAS POR SOBRE-SENSIBILIDAD. 85
6. CONCLUSIONES 86
7. BIBLIOGRAFÍA 88
7.1 LEGISLACIÓN EUROPEA 88
7.2 LEGISLACIÓN ESTATAL ESPAÑOLA 88
7.3 NORMAS TÉCNICAS INTERNACIONALES 88
7.4 DOCUMENTOS DE REFERENCIA INSTITUCIONAL 89
7.5 SMARTGRIDS Y APLICACIONES IA 89
7.6 GEMELOS DIGITALES 90

1. INTRODUCCIÓN.

Las aplicaciones, beneficios y desafíos asociados a la integración del uso de gemelos digitales (*Digital Twins*) en la operación de las redes de distribución eléctrica, evaluando su potencial para mejorar la operación, supervisión y planificación de los sistemas eléctricos modernos, son aspectos muy relevantes para la economía asturiana. Así está recogido en la Estrategia Industrial de Asturias. Asimismo, las condiciones técnicas, económicas y de ciberseguridad que surgirán durante su implantación, influyen en la planificación y desarrollo de dichas tecnologías.

Actualmente, el sector energético se encuentra inmerso en un proceso de transición energética caracterizado por la evolución desde un modelo tradicional de generación centralizada hacia un sistema más distribuido, flexible y sostenible. Históricamente, la generación eléctrica se ha basado principalmente en grandes centrales de producción conectadas a la red, incluyendo máquinas síncronas de elevada potencia e inercia, que aportaban servicios a la red para su control, lo que aseguraba la continuidad y calidad del suministro. Este modelo está evolucionando.

La descarbonización y los avances tecnológicos han impulsado una rápida incorporación de fuentes renovables al sistema eléctrico. En el caso de España, según los datos publicados por Red Eléctrica de España (REE), durante enero de 2026 se generaron unos 23.778 GWh de energía eléctrica, de los cuales el 55,7 % procedió de fuentes renovables. Dentro de estas tecnologías, la energía eólica representó el 31,9 % de la producción total, seguida por la energía hidráulica y la energía solar fotovoltaica.

Ilustración 1.Estructura de Generación Energética en España en enero de 2026.[1]

En el ámbito regional y desde el punto de vista de la capacidad de producción[2] y del número de instalaciones, Asturias dispone de 3.835 MW, de los cuales aproximadamente el 37,6 %

[1] Fuente: Asociación Empresarial Eólica 3 de diciembre 2018.

[2] Datos regionales obtenidos del BEPA 2024 publicado por FAEN.

corresponde a tecnologías renovables descentralizadas (hidroeléctrica, eólica, biomasa y solar fotovoltaica). A nivel industrial y regional, la región cuenta con más de 60 grandes centros de producción eléctrica[3]. En el caso de la generación hidráulica unas 12 grandes centrales hidráulicas que proveen a la red con unos 778MW[4]además de las 24 centrales de generación mini hidráulica cuentan 24. Respecto a las centrales eólicas la comunidad cuenta con unos 24 parques eólicos operativos, en términos de generación basada en combustibles fósiles Asturias cuenta actualmente con dos centrales térmicas (Aboño y Soto de Ribera). En términos de generación fotovoltaica son 5.459 instalaciones.[5]

Esta transformación introduce nuevos desafíos operativos derivados de la naturaleza variable e intermitente de dichas fuentes energéticas y del elevado número de instalaciones que participan en la parte de generación. Respecto de la variabilidad puede observarse en la siguiente gráfica tomada de un ejemplo de instalación de producción fotovoltaica, donde sombras y nubosidad condicionan la generación de la instalación.

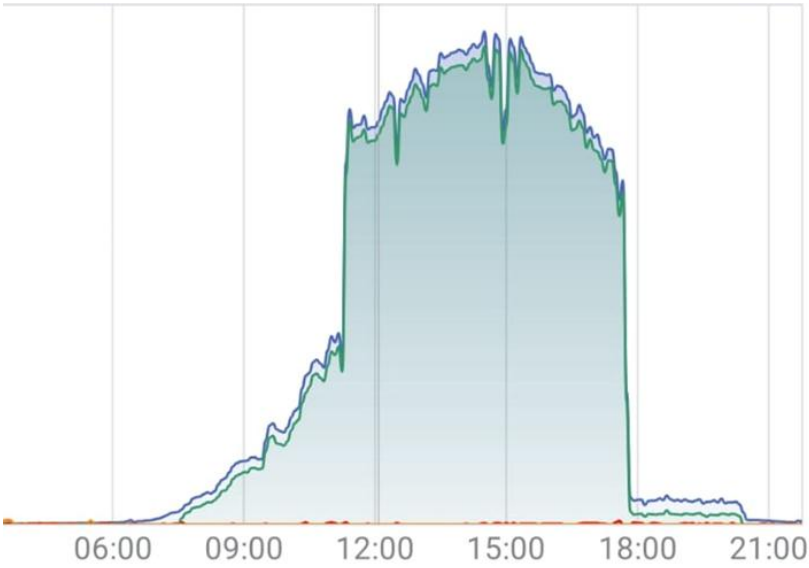

Ilustración 2. Perfil de generación de una instalación FV en Asturias (07/06/2026).

Las fluctuaciones en los recursos con los que se originan las renovables (lluvias, viento o radiación solar) dificultan establecer el equilibrio permanente entre generación y demanda que requiere el sistema eléctrico para garantizar su estabilidad, lo que obliga a contar con almacenamiento y una gestión mucho más compleja de la que existía y además totalmente diferente, pero manteniendo la red eléctrica ya construida.

[3] Fuente: Conectaindustria.es
[4] https://www.idepa.es/documents/20147/98160/Energia_ES.pdf/bfbabc6e-f173-bb52-ae09-299a723e4cc9
[5] Fuente FAEN.

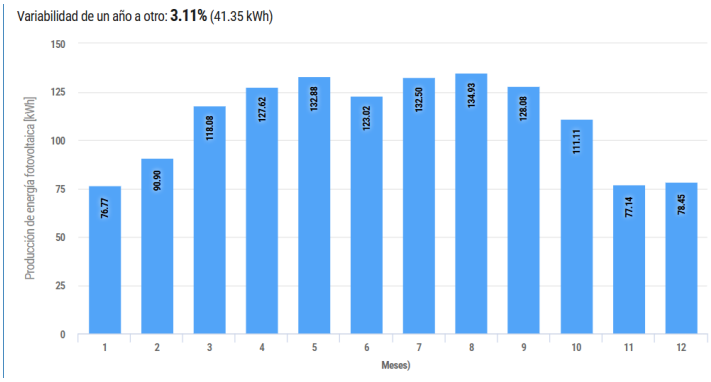

Ilustración 3. Variación de la radiación solar en Gijón (Asturias).

En relación con el almacenamiento energético, los nuevos sistemas deben evolucionar y ser más avanzados para ofrecer nuevos servicios más allá que un mero aporte de energía a la red en determinados momentos. A ello ha de añadirse la necesidad de contar con herramientas capaces de garantizar, supervisar, predecir y optimizar el comportamiento de la red en tiempo real. La gestión de estos sistemas requiere el procesamiento continuo de grandes volúmenes de información procedentes de sensores, contadores inteligentes, sistemas SCADA[6] y dispositivos IoT[7] distribuidos a lo largo de toda la infraestructura eléctrica, desde los puntos de generación a los de consumo.

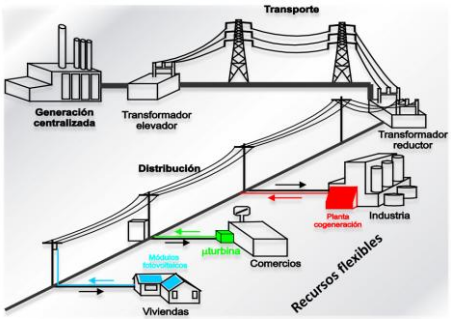

Ilustración 4. Esquema de red eléctrica distribuida[8]

En este contexto, tecnologías como la inteligencia artificial (IA), el aprendizaje automático (*Machine Learning*) y los modelos de lenguaje de gran escala (*Large Language Models*, LLMs) ofrecen nuevas capacidades para el análisis de datos, la predicción de eventos[9] y el apoyo a la

[6] Sistema de Supervisión y Control, normalmente basado en autómatas programables y servidores.

[7] IoT: Internet of the Things, entendido este como el concepto de interconexión de la industria 4.0.

[8] Elaboración propia.

[9] Cualquier suceso o circunstancia imprevista, como un fallo, maniobra o fenómeno meteorológico, que altera el estado normal de funcionamiento de la red y afecta la generación, transmisión o distribución de energía.

toma de decisiones operativas. Paralelamente, los gemelos digitales emergen como una de las tecnologías más prometedoras para la transformación digital del sector energético.

Un gemelo digital puede definirse como una representación virtual dinámica de un activo físico, proceso o sistema, capaz de reproducir su comportamiento mediante la integración de modelos matemáticos, datos históricos y datos obtenidos en tiempo real. Aplicados al ámbito eléctrico, los gemelos digitales permiten construir réplicas virtuales de redes, subestaciones, centros de transformación o instalaciones de generación, facilitando la simulación de diferentes escenarios operativos sin comprometer la seguridad de las infraestructuras reales.

Gracias a esta capacidad, los operadores pueden evaluar estrategias de control, analizar contingencias, optimizar el mantenimiento y anticipar posibles fallos. Además, la integración de los gemelos digitales con herramientas de inteligencia artificial abre la puerta al desarrollo de redes eléctricas más resilientes, eficientes y adaptables a los retos derivados de la transición energética.

Evaluemos el estado actual de los gemelos digitales aplicados a las redes de distribución eléctrica, analizando sus principales aplicaciones, beneficios potenciales y limitaciones, así como su posible papel dentro de la evolución hacia las futuras redes inteligentes (*Smart grids*).

2. ESTADO DEL ARTE. AÑO 2026.

2.1 REDES INTELIGENTES. DEFINICIÓN.

Según la definición propuesta por la Comisión Europea, una *Smart grid* o red inteligente será una red eléctrica capaz de integrar de manera eficiente el comportamiento y las acciones de todos los usuarios conectados, garantizando el suministro eléctrico seguro, sostenible y económicamente competitivo.

Las redes eléctricas inteligentes unen los desarrollos en ingeniería eléctrica y almacenamiento energético con los avances en tecnologías de la información. Con ello se pueden integrar las actividades del sector, que van desde la generación, el transporte, la distribución, el almacenamiento a la comercialización. Y a partir de esta integración, se abre la posibilidad de colaboración y coordinación entre las diferentes áreas y todos los actores implicados.

Las principales ventajas que ofrecen de las *Smart grids* son las siguientes:

- Mejorar la integración de la generación distribuida, es decir, facilitar que se pueda generar energía desde muchas más instalaciones de menor tamaño como pueden ser los hogares sin que esto tengan un impacto negativo en la red.
- Monitorizar en tiempo real la operación del sistema, entendiendo esta característica como la capacidad de poder supervisar el sistema con una latencia[10] lo suficientemente baja como para poder conocer qué sucede exactamente en cada momento.

[10] Retraso temporal en la comunicación de datos a través de una red

- Automatizar la operación de la red.
- Lograr una gestión activa de la demanda.
- Integrar del almacenamiento energético en la red.
- Dotar a la red de mayor capacidad de respuesta ante incidencias. Conseguir la participación activa del consumidor considerando el papel del prosumidor (el consumidor asume también el papel de productor).

La transformación de las redes eléctricas tradicionales hacia el modelo de las redes inteligentes supone una mejora tecnológica para los operadores del sistema y genera importantes efectos económicos sobre los distintos consumidores. Entre otros, la capacidad de monitorizar gestionar y optimizar el flujo de la energía en tiempo real permite una utilización más eficiente de los recursos energéticos, reduciendo costes operativos y facilitando una mayor participación de los usuarios en el mercado eléctrico.

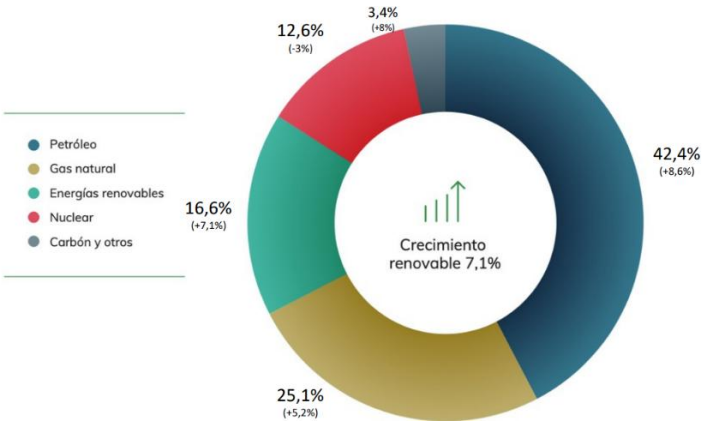

Ilustración 5.Representación del consumo energético por fuentes en España[11]

2.1.1 IMPACTO ECONÓMICO SOBRE EL CONSUMIDOR DOMÉSTICO.

Tradicionalmente, el papel del consumidor residencial se limitaba a un rol pasivo en el sistema eléctrico. Simplemente consumía energía suministrada por las compañías eléctricas y no tenía acceso a datos detallados de sus rutinas, patrones de consumo o precios en cada franja horaria. La implementación de contadores inteligentes y sistemas de gestión energética ha hecho evolucionar esta situación de forma que los usuarios pueden acceder a la información prácticamente en tiempo real sobre su demanda eléctrica y tomar decisiones sobre su consumo.

Los usuarios pueden identificar equipos con mayores consumos energéticos, optimizar sus rutinas en el uso de determinados electrodomésticos, recarga de vehículos o adaptar determinados consumos a periodos horarios con menor coste de electricidad.

[11] *APPA Renovables*

La principal fuente de ahorro económico para el consumidor aparece con las tarifas dinámicas, lo que unido al conocimiento de los patrones de consumo permite al consumidor desplazar su demanda a las horas donde la energía tenga un coste menor.

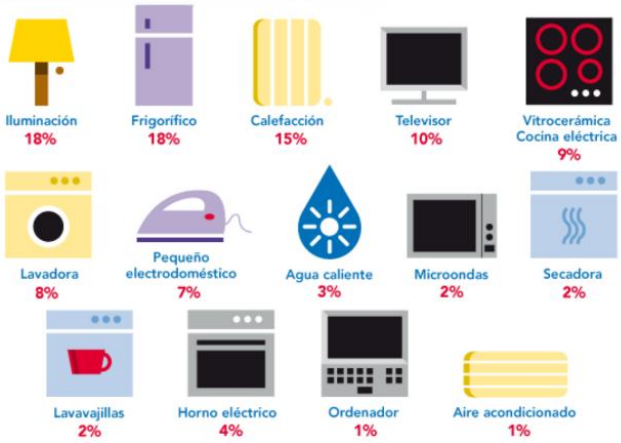

Ilustración 6. Reparto del Consumo Eléctrico Promedio en los hogares españoles[12].

En este contexto el nuevo papel del consumidor en la red eléctrica viene de la mano de otro nuevo concepto: el autoconsumo energético, que se extiende gracias al crecimiento del número de instalaciones fotovoltaicas residenciales. Este tipo de instalaciones ha permitido que numerosos hogares provean una parte significativa de su propia demanda energética, generando además interacciones muy diversas con la red. Sólo a través de redes inteligentes es posible la integración de este tipo de consumidor productor (prosumidor) dentro del sistema eléctrico, puesto que con ellas llega el uso de sistemas de monitorización, gestión y control de los excedentes, lo que facilita el aprovechamiento de la energía generada de forma local.

Con la generalización de las instalaciones fotovoltaicas domésticas llega otra necesidad: el almacenamiento. De esta forma se adaptan los ciclos productivos que desarrolla un panel solar para hacerlos coincidir con los ciclos de consumo de un hogar y optimizar las inversiones y los costes de la energía en la vivienda.

Entre los problemas a los que se enfrenta el consumidor doméstico medio con este tipo de instalaciones de almacenamiento está el elevado coste que representa la instalación, el mantenimiento y la operación. No es descartable que en el futuro la inclusión de las tecnologías V2H (*Vehicle to home*) permitan que la propia batería del coche permita combinar el consumo energético de la vivienda con el del vehículo electrificado. Esto se analiza en otro documento realizado por FAEN.

[12] Fuente: Instituto para la Diversificación y Ahorro de la Energía (IDAE).

Ilustración 7. Representación de la tecnología V2H/V2G[13]

En regiones como Asturias, donde existe un modelo de edificación muy disperso que favorece la creciente implantación de instalaciones de autoconsumo, las redes inteligentes representan una herramienta fundamental para facilitar la integración de pequeños productores dentro del sistema eléctrico sin comprometer la estabilidad de la red.

2.1.2 IMPACTO ECONÓMICO SOBRE CONSUMIDORES COMERCIALES Y TERCIARIOS.

El sector terciario también se verá beneficiado por la implantación de las redes inteligentes en Asturias. Tradicionalmente, la gestión energética de edificios de oficinas, centros comerciales, hoteles, instalaciones sanitarias o edificios administrativos se limitaba a medidas pasivas de eficiencia y a la contratación de tarifas planas o con discriminación horaria simple. En estos casos no solía contarse con acceso a los datos suficientes del perfil de consumo ni capacidad de respuesta automática a las señales del mercado. Gracias a las plataformas de adquisición de datos (hardware y software), esta situación ha ido evolucionando.

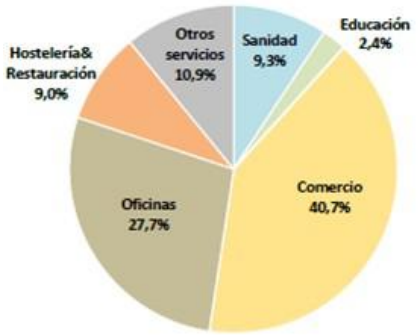

Ilustración 8. Desglose del consumo energético del sector terciario[14].

La generalización de los contadores inteligentes o de sistemas de gestión energética avanzada ha transformado el panorama, permitiendo a los gestores de inmuebles acceder en tiempo real a información detallada sobre sus perfiles de demanda, identificar ineficiencias por circuito o equipo y actuar sobre ellas de forma automatizada.

[13] Fuente: Iberdrola
[14] Fuente: I.D.A.E.

Una de las principales fuentes de ahorro económico para el sector terciario reside, al igual que en el caso doméstico, en la combinación de las tarifas dinámicas con el conocimiento preciso de los patrones de consumo propios. En edificios con perfiles de demanda complejos, con puntas marcadas en el horario comercial y valles marcados en fines de semana o en festivos, la capacidad de desplazar cargas flexibles favorece ahorros significativos, por ejemplo, en:

- recarga de las flotas de vehículos eléctricos de empresa.
- precalentamiento o preenfriamiento de espacios.
- funcionamiento de equipos de frio industrial.
- optimización de la iluminación.

Estas operaciones se programan en periodos de menor precio pudiendo representar ahorros anuales que, para establecimientos de mediano y gran tamaño en Asturias, pueden variar entre 10% y un 25% de la factura eléctrica, según los datos del IDAE.

Los sistemas de climatización e iluminación, responsables de entre el 50% y el 70% del consumo eléctrico en el segmento de oficinas y comercio, son el principal objetivo de optimización. La integración de sistemas de gestión energética basados en inteligencia artificial permite anticipar patrones de consumo vinculados a la ocupación real del edificio, las previsiones meteorológicas y los precios del mercado mayorista, adaptando el funcionamiento de los equipos sin afectar a la calidad del servicio prestado ni a las condiciones de confort de los ocupantes. En el contexto asturiano, donde una mayor pluviometría y variabilidad térmica entre estaciones climatológicas generan demandas de climatización significativas durante la mayor parte del año, esta capacidad de anticipación tiene un valor económico especialmente relevante.

Otro vector de impacto económico es la participación de los consumidores del sector terciario en los mercados de flexibilidad como proveedores de respuesta de la demanda. A través de los agregadores habilitados por la Directiva 2019/944/UE y por la Ley 24/2013 del Sector Eléctrico, instalaciones con suficiente capacidad de modulación de carga (grandes superficies comerciales, instalaciones hoteleras, centros logísticos o polígonos industriales) pueden ofertar reducciones de demanda programadas a los mercados de servicios de ajuste de Red Eléctrica de España, percibiendo una retribución adicional por aportar esta capacidad de flexibilidad de la red eléctrica. Este mecanismo convierte un coste operativo fijo en una fuente complementaria de ingresos variables, siempre que la infraestructura de medida y control habilitada por la red inteligente permita la verificación en tiempo real de las reducciones comprometidas.

El autoconsumo colectivo y las comunidades energéticas representan también representan una oportunidad para el sector terciario asturiano. Polígonos empresariales o agrupaciones de pequeño comercio en núcleos urbanos pueden constituir comunidades energéticas que compartan la generación de instalaciones fotovoltaicas colectivas o el almacenamiento realizado en baterías, reduciendo sus costes energéticos y mejorando la rentabilidad de las instalaciones. Esto es posible gracias a la monitorización y el control que proporcionan las redes inteligentes.

En un plano diferente, la implantación de redes eléctricas inteligentes ofrece una oportunidad adicional para las empresas asturianas, al facilitar el cumplimiento de las nuevas obligaciones

europeas en materia de información sobre sostenibilidad, especialmente las derivadas de la Directiva CSRD (Corporate Sustainability Reporting Directive) y de las normas ESRS E1 sobre cambio climático. Estas disposiciones exigen que las medianas y grandes empresas dispongan de información energética precisa, verificable y actualizada, lo que hace insuficientes los sistemas tradicionales. Para responder a estas exigencias resulta necesario incorporar tecnologías de digitalización e internet de las cosas (IoT), capaces de medir y registrar el consumo energético de forma continua. Además de los contadores inteligentes, que permiten conocer en tiempo real la energía consumida y su intercambio con la red, serán necesarios submedidores, que identifican el consumo de edificios, procesos o líneas de producción concretas, sistemas de gestión energética (EMS), que integran y analizan toda esta información para optimizar el funcionamiento de las instalaciones o analizadores de redes, que supervisan parámetros como la tensión, la intensidad o la calidad del suministro eléctrico.

Todos estos equipos forman parte de la arquitectura de una smart grid y convierten los datos energéticos en una potente herramienta de gestión, facilitando la identificación de oportunidades de ahorro, la integración del autoconsumo y el almacenamiento, la participación en programas de flexibilidad de la demanda y la elaboración de informes de sostenibilidad fiables y auditables.

2.1.3 IMPACTO ECONÓMICO EN CONSUMIDORES INTENSIVOS.

El desarrollo de smart grids también afecta al consumo energético en las industrias electrointensivas, cuya competitividad depende del coste de la energía eléctrica. En el caso de Asturias, es un aspecto a considerar en detalle, debido a la importante presencia de un tejido industrial compuesto por empresas de los sectores siderúrgico, metalúrgico, químico y manufacturas y también por nuevas oportunidades de captación de inversiones que pueden aparecer respectos de consumidores intensivos (centros de proceso de datos). Para estas empresas, jugar el papel de prosumidor es complejo, ya que contar en un mismo emplazamiento con generación renovable (o no renovable) suficiente para abastecer su propio consumo suele ser poco viable para plantas de esas características.

Ilustración 9. ARCELOR MITTAL Asturias[15]

Sin embargo, la tendencia a emplear sistemas de almacenamiento facilita cierta autonomía para cubrir demandas de procesos críticos. El desarrollo de protocolos de operación que permiten la

[15] Fuente: La Voz de Asturias 7 junio de 2024

desconexión de parte de la planta para facilitar una mejor operación de la red eléctrica puede representar una opción económicamente viable. Estos programas de respuesta a la demanda permiten que determinados consumidores industriales reciban compensaciones económicas por colaborar en la estabilidad de la red, reduciendo temporalmente su consumo cuando el operador del sistema lo solicita. Este tipo de mecanismos resulta especialmente relevante en escenarios con alta penetración de energías renovables, donde las fluctuaciones de producción junto con las variaciones de carga del sistema pueden generar desequilibrios temporales.

A pesar de todos estos condicionantes, al tener estas industrias consumos tan elevados, cualquier mejora en los costes económicos obtenida a través de inversiones en renovables o gestión de consumos, pueden traducirse en importantes reducciones de los costes operativos y mejoras de la competitividad relevantes.

2.1.4 NORMA IEC 61850.

Uno de los desarrollos que más peso tendrá en las futuras mejoras de la red española por parte de REE es la digitalización de la red eléctrica, que irá desde los equipos de análisis y mantenimiento de la red a la infraestructura en sí.

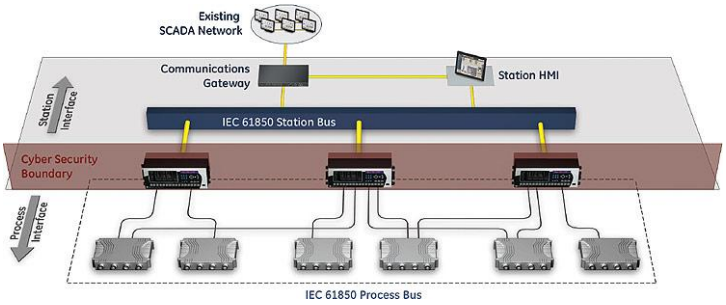

Ilustración 10. Representación[16] de sistemas incluidos en la norma IEC 61850.

En la imagen previa se observa el esquema propio de una subestación eléctrica digitalizada que usa el estándar de esta norma. Muestra como viaja la información desde los equipos de campo hasta el centro de control, a través de relés internos y por una red interna. Los equipos que manejan el flujo de información (de abajo a arriba en la imagen) serían los siguientes:

- ***Equipos de campo:*** son los dispositivos que están en contacto directo con la red eléctrica (transformadores, interruptores, sensores de corriente y voltaje, etc.). En el diagrama se representan seis equipos pequeños.
- ***IED's o relés de protección (representados en la parte media, son los tres equipos con pantalla roja):*** son los "cerebros" intermedios. Reciben la información de los equipos de campo y la procesan. Aquí es donde empieza realmente la parte "digital" e inteligente del sistema.
- ***Bus de estación ("IEC 61850 Station Bus"):*** es como una autopista de datos que conecta a todos los IED's entre sí y con los sistemas de supervisión.

[16] Fuente: General Electric.

Gateway de comunicaciones y HMI de estación (arriba):

- El **Gateway** traduce y envía la información hacia afuera, hacia el sistema SCADA central (que puede estar en otra ciudad u oficina central).
- El **HMI (interfaz hombre-máquina)** es la pantalla local donde un operador en la propia subestación puede ver y controlar todo.
- **SCADA existente (la nube de arriba)**: es el sistema central que monitorea muchas subestaciones a la vez, no solo esta.

Atendiendo a la normativa aplicable en el caso de las redes inteligentes, la estandarización viene a través de la NORMA IEC 61850. Con esta norma, se persigue la incorporación en la red eléctrica de tecnologías de comunicación e información que permitan el intercambio bidireccional de datos, de forma que se habiliten las operaciones necesarias de la red. El estándar de la norma se presenta como una propuesta normalizada única y completa considerando el modelado, la configuración y las comunicaciones para asegurar la interoperabilidad entre los distintos fabricantes. Actualmente, los sistemas de control están basados en soluciones que dependen del suministrador del equipo que se trate de operar. Esta dependencia del proveedor hace vulnerables a las compañías ante subidas de precio de la tecnología con la que operan, además de reducir el abanico de soluciones disponibles que puedan aplicar a la red. Todo ello tiene una base común: falta de interoperabilidad para la mayoría de los equipos.

El desarrollo de las redes locales o LAN (*Local Area Network*) de subestación, necesarias para la implantación de la norma, abre la puerta a un nuevo mercado de servicios, gracias a las posibilidades TIC. Se plantean estas alternativas gracias a tratamiento de la información de la subestación, acceso remoto o análisis avanzado de eventos. Más allá de las subestaciones, la norma va ampliando su alcance para cubrir las exigencias de las centrales de energías renovables y de la *Smart grid*: comunicación entre centros, los sistemas de recursos distribuidos, el control de cargas en el sistema o la recarga de vehículo eléctrico.

Desde un punto de vista social, la norma generará que dentro del sector eléctrico se necesiten profesionales especializados en las nuevas tecnologías, de forma que dentro del contexto asturiano se abren oportunidades para incorporar formación que incluya a la digitalización dentro de sus programas de cualificación y recualificación de profesionales.

En el caso de equipos, actualmente se busca la implantación de equipos de ensayo y mantenimiento (similares a OMICRON CMC 500 recogido en la imagen); estos equipos presentan mejoras respecto a la generación anterior como modularidad, digitalización y capacidad de operación conjunta de los equipos.

Ilustración 11. OMICRON CMC 500[17]

2.1.5 FLEXIBILIDAD ENERGÉTICA COMO NUEVO RECURSO ECONÓMICO.

La figura del prosumidor aparece porque dentro de las redes inteligentes, los consumidores dejan de ser únicamente parte de la demanda energética y se convierten también en agentes activos que pueden aportar generación y servicios de valor al sistema, entre ellos la flexibilidad de su consumo.

El Operador del Sistema debe disponer de mecanismos de corrección que actúen con rapidez. Esos mecanismos son los denominados servicios de ajuste, regulados por la Comisión Nacional de los Mercados y la Competencia (CNMC) a través de los Procedimientos de Operación (POs) aprobados mediante resoluciones publicadas en el BOE. Los procedimientos operativos se pueden definir como un conjunto de normativas y directivas técnicas orientadas a garantizar el equilibrio de operación del sistema eléctrico. Los servicios de ajuste del sistema eléctrico peninsular español se articulan en varios niveles de respuesta, ordenados de mayor a menor velocidad de actuación:

- El primero es la regulación primaria, también llamada respuesta inercial de frecuencia, que actúa de forma automática e instantánea en los generadores para estabilizar la frecuencia de la red ante perturbaciones repentinas. Es una obligación técnica de los agentes generadores de energía habilitados para operar en la red. Gracias a esta regulación se mantiene la frecuencia en un valor 50 Hz. Este valor de la frecuencia es común para la red en Europa. En otras zonas del mundo la frecuencia tiene otros valores (por ejemplo, en Japón el país tiene zonas en las que se trabaja a 50 Hz y otras en las que se opera a 60 Hz).
- La regulación secundaria (aFRR, *automatic Frequency Restoration Reserve*), regulada por el PO 7.2 aprobado por la CNMC, opera de forma automática en un horizonte de segundos a minutos, y su objetivo es restablecer la frecuencia de la red y el programa de intercambios internacionales tras una perturbación, entendida como perturbación de la red como cualquier alteración, anomalía o fluctuación en la tensión o corriente eléctrica que se desvía de su onda sinusoidal normal. Algunos generadores de electricidad están habilitados específicamente para proveer este servicio a la red. Para

[17] OMICRON ENERGY (https://www.omicronenergy.com/es/productos/cmc-500/)

ello deben superar pruebas técnicas específicas y son retribuidos tanto por la reserva de banda comprometida para mantener la frecuencia dentro de ella, como por la energía efectivamente activada en esa frecuencia. En 2024, conforme al Informe de Servicios de Ajuste de REE, la repercusión de los servicios de ajuste en el precio medio final de la energía fue de 11,43 €/MWh. Esto supuso el 15% del precio medio final de la energía, lo que ilustra la relevancia económica de estos mercados.

- La regulación terciaria (mFRR, *manually activated Frequency Restoration Reserve*), regulada por el PO 7.3., actúa en un horizonte de hasta quince minutos y sirve para restituir la reserva de regulación secundaria consumida[18]. A diferencia de la regulación secundaria, la terciaria se activa manualmente por el Operador del Sistema y las energías se negocian en mercados gestionados vía ESIOS. Conforme al Reglamento (UE) 2017/2195, los servicios de regulación terciaria y secundaria se realizan mediante plataformas europeas, lo que integra al sistema eléctrico español en el mercado único europeo de flexibilidad.
- El cuarto nivel son las reservas de sustitución (RR, *Replacement Reserves*), reguladas por el PO 3.3. Son el recurso de mayor tiempo de respuesta —hasta una hora— y se activan para liberar la capacidad comprometida en regulación terciaria y permitir la reposición de reservas ante situaciones sostenidas de desequilibrio. En resumen, su función es asumir el equilibrio del sistema a más largo plazo, liberando la regulación terciaria para que pueda utilizarse nuevamente en caso de ser necesario.

Hasta hace unos años, todos estos servicios de ajuste eran prestados exclusivamente por las centrales de generación convencionales como las hidráulicas, de ciclo combinado o cogeneración. Las redes inteligentes han cambiado radicalmente este paradigma al hacer posible que la demanda (consumidores industriales, comerciales e incluso residenciales agregados) participe como proveedor de estos servicios. Este mecanismo se denomina respuesta activa de la demanda y constituye el vehículo más relevante para que consumidores asturianos conviertan su flexibilidad en un recurso económico.

El instrumento específico para España es el Servicio de Respuesta Activa de Demanda (SRAD), regulado por el PO 7.5, aprobado por la CNMC mediante Resolución de 19 de octubre de 2023 y modificado en noviembre de 2025 (BOE-A-2025-22853). El SRAD tiene por objeto reglamentar el funcionamiento del servicio específico de balance de respuesta activa de la demanda del sistema eléctrico peninsular español, para hacer frente a situaciones en las que se identifique una insuficiencia de reserva de regulación terciaria a subir. En la práctica, cuando REE detecta que no tiene suficientes recursos para mantener el equilibrio del sistema, activa a los consumidores habilitados en el SRAD para que reduzcan su consumo de forma coordinada y remunerada.

Para el contexto asturiano, este marco abre oportunidades económicas concretas en varios sectores. Las industrias electro intensivas presentes actualmente en la región (siderurgia,

[18] Este servicio permite reponer la reserva de regulación secundaria en el caso de que esta ya haya sido utilizada, asegurando que el sistema siga disponiendo de capacidad para responder a nuevos desequilibrios del sistema.

química, aluminio, papel) disponen de cargas flexibles significativas (hornos eléctricos, electrólisis, bombeo, sistemas de refrigeración) que pueden modularse temporalmente sin comprometer sus procesos productivos. Su participación en los servicios de ajuste no solo genera ingresos directos por la retribución del SRAD (del orden de 56 a 65 euros por MW disponible y hora, más la retribución por las activaciones efectivas al precio de la regulación terciaria vigente en cada momento) sino que contribuye a reducir el coste global del sistema, beneficiando indirectamente a todos los consumidores a través de un menor precio medio final de la energía.

La infraestructura digitalizada de la red inteligente es la condición técnica imprescindible para que este mercado funcione: telemedida cuarto-horaria certificada, sistemas de telegestión que permitan la activación en 12,5 minutos y los canales de comunicación con ESIOS[19]. Invertir en la digitalización de la demanda industrial representa la oportunidad de acceso a un nuevo flujo de ingresos que la propia arquitectura regulatoria española incentiva y remunera.

2.1.6 INTEGRACIÓN DE GENERACIÓN RENOVABLE Y AUTOCONSUMO INDUSTRIAL.

El otro aspecto a considerar es el efecto en el contexto energético asturiano de los sistemas de generación renovables asociados a las instalaciones industriales o se servicios. La reducción de costes experimentada por la tecnología fotovoltaica ha favorecido la instalación de sistemas de autoconsumo en polígonos industriales y centros de producción.

Ilustración 12.Ejemplo del autoconsumo industrial[20]

Las redes inteligentes facilitan esa integración mediante la gestión bidireccional de los flujos energéticos, realizando un control de los excedentes de la producción en los puntos, además de permitir la coordinación de la red con los sistemas de generaicón y de almacenamiento. El resultado es que las empresas pueden reducir su dependencia del mercado eléctrico y mejorar su competitividad al no estar tan expuestas a las fluctuaciones de los costes energéticos.

Además, esta estrategia contribuye al cumplimiento de los objetivos de descarbonización establecidos tanto por la Unión Europea como por las administraciones nacionales y autonómicas.

[19] ESIOS (Sistema de Información del Operador del Sistema) es la plataforma de Red Eléctrica que permite el intercambio de información con los participantes del mercado y la publicación de datos sobre la operación del sistema eléctrico y los mercados de ajuste.
[20] Cambio energético (https://www.cambioenergetico.com/autoconsumo-industrial/)

2.1.7 LIMITACIONES ECONÓMICAS ACTUALES.

Pese a las ventajas previas se debe considerar que la implementación de redes inteligentes presenta desafíos económicos y temporales. La digitalización de la red requiere de una inversión inicial elevada, dado que es necesario usar sensores inteligentes o instalar una infraestructura de comunicación de los mismos, lo que implica plazos de implantación. Además, dicha estructura y dichos sensores deben ser integrados dentro de sistemas SCADA que puedan operar en conjunto con plataformas de datos o tecnologías IoT (internet de las cosas). Los costes de equipos de almacenamiento y la gestión también representan una barrera de desarrollo por el coste inicial o las reposiciones por obsolescencia:

- Los pequeños consumidores (empresas o personas físicas) podrán tener barreras de acceso a este tipo de redes.
- Otro aspecto que representa una barrera será el mantenimiento y la actualización de la infraestructura digital. Es un nuevo coste que la infraestructura previa no tenía, tanto el software (requiere actualizaciones periódicas o emplear un mantenimiento especializado), como los costes asociados a las licencias (software estándar y protección frente a ciberataques) son aspectos a considerar en el desarrollo de la red.

Finalmente se debe considerar el riesgo y las limitaciones asociadas a la dependencia de sistemas informáticos y de comunicaciones, que introducen limitaciones operativas y económicas.

2.2 IMPACTO AMBIENTAL DE LAS REDES INTELIGENTES EN ASTURIAS.

Las redes eléctricas inteligentes son también esenciales para alcanzar los objetivos de sostenibilidad y descarbonización establecidos tanto a nivel europeo como nacional. Su desarrollo permite operar mayor número de instalaciones y reducir el impacto ambiental que está asociado a la producción, distribución y consumo de la electricidad.

Para su desarrollo es necesario analizar la situación de partida. En Asturias, de las redes eléctricas en Asturias se caracterizan por la necesidad de crecimiento y refuerzo (especialmente con infraestructuras como el anillo central) y por una situación de competitividad operativa buena, con indicadores positivos.

Ámbito	**Situación / pérdidas**
Red de transporte mundial	Las pérdidas en redes eléctricas fueron inferiores al 8 % de la generación mundial en 2022, incluyendo transporte y distribución.
Transporte – Unión Europea	Las pérdidas técnicas de las redes de transporte + distribución de la UE fueron aproximadamente 6,7 % de la generación en 2022.
Transporte – España	En el sistema peninsular, las pérdidas de transporte fueron 2.529 GWh en 2024
Distribución – referencia europea	Estudios europeos sitúan las pérdidas típicas de distribución en muchos sistemas europeos en torno al 4–6 %, aunque existe una gran dispersión según red y país.

Ámbito	Situación / pérdidas
Distribución – España	Las pérdidas de transporte + distribución en España fueron 8,29 % de la generación en 2024.
Distribución – operador EDP	En 2024, EDP Redes registró 4,8 % de pérdidas de red sobre la energía distribuida.

Ámbito	Potencial con redes inteligentes
Red de transporte mundial	La IEA estima que llevar las pérdidas mundiales hacia niveles eficientes próximos al 5 %.
Transporte – Unión Europea	El potencial de digitalización se centra tanto en pérdidas como en optimización de flujos, congestiones, mantenimiento y utilización de activos.
Transporte – España	El margen de reducción es relativamente menor que en distribución porque la red de alta tensión ya presenta una eficiencia elevada.
Distribución – España	La distribución tiene potencial de mejora, especialmente mediante sensorización, automatización y gestión activa.
Distribución – operador EDP España	El operador establece objetivos de eficiencia y utiliza telemedida y digitalización para mejorar la operación.

2.2.1 CONTRIBUCIÓN A LA DESCARBONIZACIÓN DEL SISTEMA ELÉCTRICO.

El principal beneficio ambiental de las redes inteligentes es su capacidad para facilitar la integración de las fuentes de energía renovable, el almacenamiento o consumos específicos como los coches eléctricos. Asturias parte de un modelo energético en el que durante décadas tuvieron un peso muy importante las grandes centrales térmicas de carbón, asociadas a una generación concentrada en determinados emplazamientos. La transformación de este modelo hacia otro con una mayor presencia de energía eólica, solar, autoconsumo o baterías implica una generación más distribuida y variable que responden a nuevas formas de consumo eléctrico muy dispares y diferentes.

Esta nueva configuración requiere una red más flexible y capaz de adaptarse rápidamente a cambios en la producción y en el consumo. Las redes inteligentes permiten hacerlo mediante sistemas avanzados de monitorización, automatización, comunicaciones y control, que proporcionan información sobre el estado de la red y facilitan una respuesta más rápida ante cambios en las condiciones de operación y de su propio entorno. En Asturias, esta capacidad será especialmente importante a medida que aumente la conexión de nuevas instalaciones renovables y se avance en la electrificación de la industria, el transporte y otros sectores como la edificación.

La digitalización permite, además, aprovechar mejor la energía renovable disponible y reducir los vertidos. De esta forma, las *smart grids* permiten que todo el sistema se utilice de una manera más eficiente y coordinada.

2.2.2 REDUCCIÓN DE PÉRDIDAS ENERGÉTICAS.

Dentro de los beneficios ambientales aportados por las redes inteligentes se encuentra la posibilidad de reducir y controlar mejor las pérdidas energéticas que se producen durante el transporte y la distribución de electricidad. En cualquier sistema eléctrico una parte de la energía se pierde debido, principalmente, a la resistencia de los conductores eléctricos y al funcionamiento de los transformadores. Estas pérdidas dependen, entre otros factores, de la intensidad que circula por las líneas, de la longitud de los recorridos y del nivel de carga de las instalaciones.

En Asturias, donde conviven grandes consumidores industriales, redes de distribución urbanas y rurales junto con una generación renovable cada vez más distribuida, disponer de información detallada sobre el funcionamiento de la red puede ayudar a localizar puntos con pérdidas elevadas, identificar sobrecargas y mejorar la planificación de las actuaciones de mantenimiento y refuerzo. La incorporación de sensores, equipos de medida y sistemas de análisis de datos permite conocer con mayor precisión cómo se comportan las distintas partes de la red y adoptar medidas correctoras cuando sea necesario.

Asimismo, la gestión inteligente de los flujos de potencia y la integración de generación distribuida pueden contribuir a reducir determinados recorridos de la electricidad entre el punto de generación y el de consumo. Esto resulta especialmente relevante en el desarrollo del autoconsumo industrial, residencial y colectivo, ya que una parte de la electricidad puede producirse y utilizarse en el propio entorno donde se consume.

Desde una perspectiva ambiental, una mejor gestión de las redes permite utilizar de forma más eficiente la energía generada y reducir la necesidad de producir electricidad adicional para compensar las pérdidas. No obstante, debe tenerse en cuenta que la reducción de pérdidas depende de las características concretas de cada red, por lo que las *Smart grids* deben complementarse con actuaciones físicas de renovación, ampliación y mejora de las líneas, centros de transformación y subestaciones.

2.2.3 IMPULSO AL AUTOCONSUMO Y LA GENERACIÓN DISTRIBUIDA.

Durante los últimos años se ha producido en Asturias un crecimiento de las instalaciones de generación renovable destinadas al autoconsumo, tanto en edificios como en instalaciones industriales. Esta evolución está acompañada por la incorporación de sistemas de almacenamiento y por el desarrollo de nuevas fórmulas de autoconsumo colectivo y comunidades energéticas. El propio Principado ha tramitado programas de apoyo a estas instalaciones y, en marzo de 2026, informó de la concesión de 4.921 ayudas para instalaciones de autoconsumo y almacenamiento, asociadas a 123,62 MW de generación renovable y 16,17 MWh de capacidad de almacenamiento.

Esta evolución supone un cambio importante en la forma de utilizar la red eléctrica. Un consumidor puede pasar a producir parte de la electricidad que necesita y, en determinados momentos, disponer de excedentes que pueden ser utilizados por otros consumidores o inyectados a la red.

La generación distribuida permite acercar parte de la producción al lugar donde se consume, reduciendo determinados intercambios de energía con la red y favoreciendo un uso más eficiente de la electricidad generada. Sin embargo, su integración requiere una red capaz de gestionar flujos de energía que pueden cambiar de dirección y de intensidad a lo largo del día.

Las redes inteligentes permiten conocer en tiempo real el comportamiento de estas instalaciones, anticipar posibles problemas de tensión o congestión y coordinar generación, consumo y almacenamiento.

Por tanto, el desarrollo del autoconsumo y la generación distribuida no debe entenderse únicamente como una cuestión de instalar paneles solares. Requiere también digitalizar las redes de distribución, incorporar sistemas de medida y control y mejorar la capacidad de las infraestructuras para gestionar un número creciente de pequeños y medianos productores.

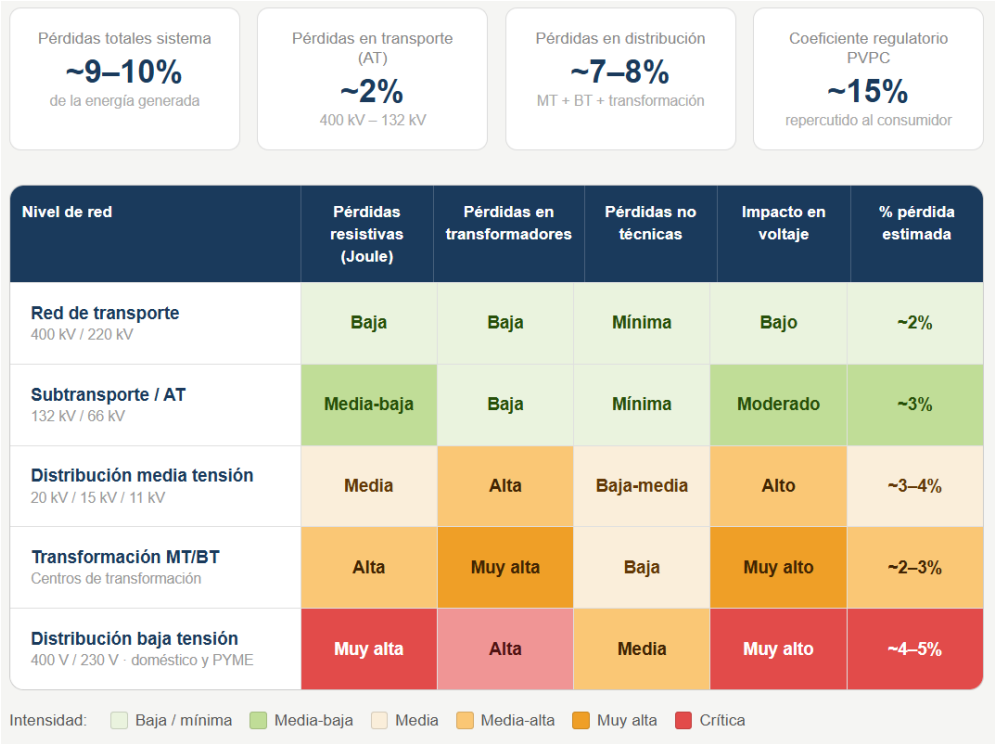

Ilustración 13. Mapa[21] de las Pérdidas Energéticas de la red eléctrica.

La figura anterior muestra cómo se distribuyen las pérdidas de energía eléctrica a lo largo de toda la red, desde el de transporte en alta tensión hasta la distribución final en baja tensión. Se puede observar que a medida que disminuye el nivel de tensión aumentan las pérdidas. Esto se debe a un principio físico básico: para transportar la misma potencia a menor tensión, es necesaria una corriente mayor y las pérdidas resistivas (efecto Joule) crecen con el cuadrado de la corriente. Por eso la red de transporte en 400/220 kV apenas pierde un 2%, mientras que la distribución en baja tensión (400V/230V), donde la corriente es mucho mayor para la misma potencia, llega a perder entre un 4% y un 5%.

[21] Fuente: www.miteco.gob.es

A esta causa física se suma un efecto acumulativo de infraestructura: cuanto más bajamos en tensión, más equipos y más kilómetros de red hay por unidad de energía transportada (más transformadores, más cableado, más puntos de conexión con usuarios finales), lo que incrementa tanto las pérdidas. El resultado es que la mayor parte de las pérdidas totales del sistema (9-10%) se concentra precisamente en los últimos tramos de la red, los más cercanos al consumidor y no en el transporte de larga distancia, que resulta comparativamente mucho más eficiente.

2.2.4 ELECTRIFICACIÓN DE SECTORES ESTRATÉGICOS.

La electrificación constituye una de las principales estrategias para alcanzar los objetivos de neutralidad climática establecidos por la Unión Europea. Es el caso de sectores como el transporte, la climatización o determinados procesos industriales, que están experimentando una progresiva sustitución de tecnologías basadas en combustibles fósiles por sistemas eléctricos de mayor eficiencia.

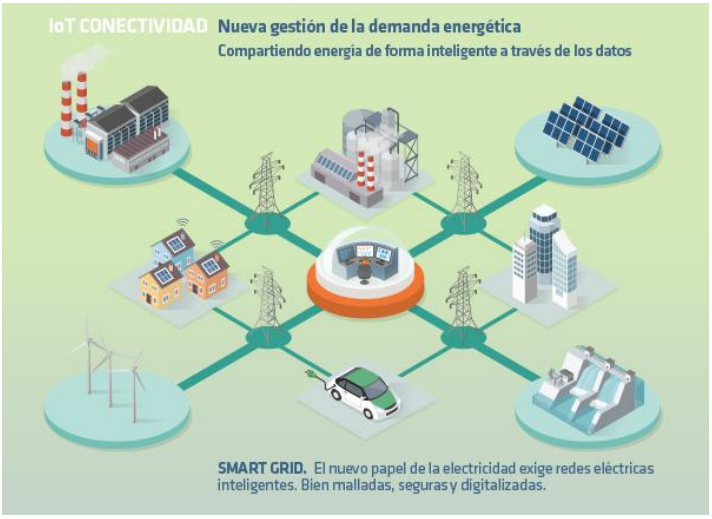

Ilustración 14. Representación[22] de la nueva Electrificación de la Red.

Este proceso implica un incremento significativo de la demanda eléctrica que debe ser gestionada adecuadamente para evitar problemas de congestión o sobrecarga de la red. Las redes inteligentes proporcionan las herramientas necesarias para coordinar la carga de vehículos eléctricos, gestionar sistemas de almacenamiento energético y optimizar el funcionamiento de nuevas cargas eléctricas. De esta forma, contribuyen a acelerar la electrificación de la economía sin comprometer la seguridad y estabilidad del sistema eléctrico.

[22] Fuente: https://www.prysmianclub.es/cambios-en-la-edificacion-la-normativa-que-viene-de-europa-iv/

2.3 GEMELOS DIGITALES Y SU INTEGRACIÓN EN LAS REDES INTELIGENTES.

La digitalización de las infraestructuras críticas es uno de los principales ejes estratégicos de la política energética de la unión europea para la década de 2020-2030.

Como se mencionó previamente, Asturias presenta un perfil energético singular, una región con larga tradición en la generación térmica y la industria pesada, que afronta la transición hacia una economía descarbonizada bajo los compromisos del Pacto Verde Europeo y la Ley de Cambio Climático y Transición Energética[23].

2.3.1 DEFINICIÓN Y COMPONENTES ESENCIALES.

El término de gemelo digital fue acuñado en el año 2002 por Grieves, considerado como uno de los padres de la digitalización. Aun así, no existe una definición universalmente aceptada ni en el ámbito académico ni en el ámbito industrial. La definición más referenciada actualmente fue aportada por la NASA (2012). Un gemelo digital es una "*simulación multifísica, multiescala y probabilística integrada de un vehículo o sistema que utiliza los mejores modelos físicos disponibles, actualizaciones de sensores e historial de flota para reflejar la vida de su gemelo real*".

Si se realiza un análisis de las definiciones existentes se identifican cuatro elementos comunes en un gemelo digital que son:

- Representación virtual del sistema físico.
- Comunicación bidireccional entre la entidad real y la virtual.
- Capacidad de simulación dinámica.
- Conexión a lo largo de todo el ciclo de vida del activo.

La arquitectura típica de un gemelo digital para infraestructuras eléctricas articula cinco dimensiones funcionales:

- Entidad Física: Es el sistema o activo real que se está monitorizando.
- Entidad Virtual: Es el modelo digital con las capacidades de simulación y predicción.
- Comunicación Bidireccional: el canal de datos en tiempo real que sincroniza ambas entidades.
- Gestión de datos: la infraestructura de adquisición, procesado y almacenamiento.
- Servicios: las funcionalidades que aportan valor operativo (diagnóstico, optimización, planificación).

Atendiendo al nivel de desarrollo del gemelo digital este se puede clasificar como:

- Modelo Digital (sin conexión al sistema real).
- Sombra Digital (flujo unidireccional de datos desde lo físico a lo virtual).

[23] España,Ley 7/2021, 20 de mayo, "BOE núm 121"

- Gemelo Digital propiamente dicho (comunicación bidireccional y actualización continua)

Esta distinción resulta crítica para evaluar el potencial real de las implementaciones existentes.

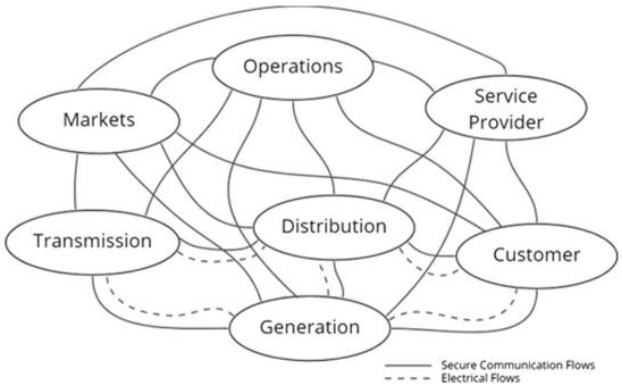

Ilustración 15.Esquema Conceptual NIST de una red inteligente

El modelo conceptual NIST[24] es un método de representación empleado para facilitar la interoperabilidad entre los distintos agentes y tecnologías que integran el sistema eléctrico, promoviendo una coordinación eficiente, segura y flexible que permite establecer una estructura común en la que los diferentes actores de la red puedan ser integrados.

2.3.2 MARCO DE REFERENCIA: EL MODELO NIST DE SMART GRID.

El modelo conceptual de la red inteligente propuesto por NIST define 7 dominios interoperables: transmisión, distribución, generación, clientes, mercados, operaciones y proveedores de servicios. En términos sencillos, este modelo es un “mapa” que divide toda la red eléctrica en "departamentos especializados”, cada uno con una función concreta, pero todos conectados entre sí mediante flujos constantes de información y de energía.

Los dominios se relacionan entre si mediante dos tipos de flujos:

- ***Flujo de energía:*** sigue el camino físico tradicional, desde la generación (centrales, parques solares etc…), pasando por transmisión y distribución hasta llegar al dominio de clientes.
- ***Flujo de información:*** es el que hace inteligente a la red y no necesariamente sigue el mismo camino que la energía. Por ejemplo, un cliente con paneles solares no solo recibe energía del distribuidor, sino que también envía información (cuánto genera, cuánto consume) hacia el dominio de operaciones (que gestiona la red en tiempo real) y hacia el dominio de mercados (que determina precios y mecanismos de compensación). El dominio de proveedores de servicios actúa como intermediario que ofrece aplicaciones (facturación, gestión de energía, mantenimiento) apoyándose en esa información.

[24] National Institute of Standards and Technology: Instituto Nacional de Estándares y Tecnología.

Para un usuario doméstico o industrial, este modelo significa que ya no es un actor pasivo que simplemente recibe electricidad. Puede adoptar una figura nueva, la del prosumidor, que ya se ha comentado.

Para que estos dominios puedan comunicarse se apoya en distintas capas de interoperabilidad, que de forma simplificada son:

- ***Capa técnica:*** los protocolos y estándares de comunicación (como el IEC 61850 visto en el primer esquema) que permiten que equipos de distintos fabricantes se entiendan entre sí.
- ***Capa informativa:*** el significado y formato de los datos intercambiados (por ejemplo, que "consumo" signifique lo mismo en todos los sistemas).
- ***Capa organizativa:*** los acuerdos, normativas y procesos de negocio que regulan cómo y cuándo se comparte esa información entre actores (distribuidoras, comercializadoras, reguladores).

Aunque se desarrollará en más profundidad más adelante, se debe considerar el concepto de la ciberseguridad que aplica sobre el sistema. Cuantos más dominios se conectan y más información circula entre ellos, mayor es la superficie expuesta a posibles ataques. Por eso, en el primer esquema analizado se señalaba una "frontera de ciberseguridad" alrededor de los equipos de control físico (relés, IED's). Esa misma lógica se aplica a escala de todo el modelo NIST.

No obstante, no toda la información debe tratarse igual. Los flujos relacionados con el control físico de la red (dominio de operaciones, distribución) requieren protocolos de seguridad mucho más estrictos que los flujos puramente comerciales o informativos (dominio de mercados), porque un fallo de seguridad en los primeros puede causar interrupciones de suministro o daños físicos, mientras que en los segundos el riesgo principal es la privacidad de los datos o el fraude económico.

Además de la seguridad frente a ataques, el modelo NIST obliga a pensar en la privacidad de los datos que circulan entre dominios. Los contadores inteligentes, por ejemplo, generan información muy detallada sobre los hábitos de consumo de un hogar (a qué hora se enciende la calefacción, cuándo no hay nadie en casa, etc…). Esta información viaja entre el dominio de clientes y los dominios de operaciones**,** mercados y proveedores de servicios, lo que significa que múltiples actores —no solo la distribuidora— pueden tener acceso a datos sensibles sobre la vida privada de las personas. Por eso, la interoperabilidad entre dominios no es solo un reto técnico de comunicación, sino también un reto regulatorio: hay que definir claramente qué actor puede ver cada dato, con qué finalidad y durante cuánto tiempo se conserva.

Finalmente, se debe considerar qué aportan los gemelos digitales a este modelo. En el marco de los siete dominios del NIST resulta especialmente útil para analizar dónde y cómo se están aplicando los gemelos digitales dentro de la red eléctrica, ya que permite clasificar cada caso de uso según el dominio al que pertenece.

Tomando como referencia la revisión sistemática de Heluany y Gkioulos (2024), que analizó 2.238 artículos científicos sobre gemelos digitales aplicados a sistemas eléctricos, se identifican patrones claros que pueden situarse dentro de dos de los dominios del modelo NIST:

- En distribución, el caso de uso más frecuente es la gestión, es decir, gemelos digitales que simulan el comportamiento de la red para optimizar su operación en tiempo real; seguido por su aplicación en el diagnóstico de fallos (detectar averías o anomalías antes de que provoquen una interrupción del suministro).
- En generación, predomina el uso de gemelos digitales para el diagnóstico de fallos en equipos de generación (turbinas, paneles, inversores), seguido por la optimización del rendimiento y el mantenimiento predictivo (anticipar cuándo un equipo necesitará revisión antes de que falle).

Además, la revisión identifica dos hallazgos transversales que afectan a la viabilidad real de estas tecnologías:

- ***La inteligencia artificial como habilitador técnico:*** la mayoría de los estudios analizados incorporan técnicas de IA o aprendizaje automático para dar "vida" a estos gemelos digitales, es decir, para que el modelo virtual no sea solo una réplica estática, sino que aprenda y se ajuste dinámicamente al comportamiento real del equipo o la red que representa. Esto conecta directamente con el modelo NIST porque estas capacidades de IA son las que permiten que los flujos de información generados en los dominios de distribución y generación se traduzcan en decisiones operativas útiles en tiempo real (por ejemplo, en el dominio de operaciones).
- ***Una brecha relevante en la consideración de los grupos de interés:*** menos del 10% de los estudios de implementación analizan el papel de actores como reguladores, distribuidoras, comercializadoras o los propios usuarios finales en el diseño e implementación de estos proyectos de gemelos digitales. Esto es significativo porque, como hemos visto, el modelo NIST está construido precisamente sobre la idea de que la red inteligente requiere la interoperabilidad entre múltiples actores y dominios, no solo entre tecnologías. Un gemelo digital técnicamente bien diseñado pero que no contempla cómo se integrará con las necesidades de operadores, reguladores o clientes (dominios completos del propio modelo NIST) difícilmente podrá implementarse con éxito a escala de todo el sistema eléctrico, más allá de un proyecto piloto aislado. Es, por tanto, una limitación que pone en duda la madurez real de estas tecnologías para una adopción generalizada, más allá de su solidez técnica o puede reflejar una evolución de los modelos actuales hacia otros con menor número de grupos de interés, lo que sería un contrasentido con el desarrollo conceptual.

2.3.3 HERRAMIENTAS Y TECNOLOGÍAS HABILITADORAS.

En conjunto, estas herramientas y tecnologías se estructuran como diferentes capas de un modelo:

- El proceso comienza en el sistema físico, donde sensores, contadores, equipos de protección y dispositivos de campo capturan información sobre el estado de la red.
- Los protocolos de comunicación permiten transmitir e intercambiar estos datos entre equipos y sistemas, mientras que las tecnologías de procesamiento y almacenamiento los organizan y preparan para su utilización.
- Sobre esta base se construye el modelo matemático y digital de la infraestructura mediante herramientas de modelización, que posteriormente puede ejecutarse mediante diferentes técnicas de simulación para reproducir su comportamiento bajo distintas condiciones.
- Finalmente, las herramientas de analítica avanzada e inteligencia artificial permiten identificar patrones, detectar anomalías, realizar predicciones y apoyar la toma de decisiones.

Para que una Smart Grid y su gemelo digital puedan funcionar como un sistema conectado, es necesario disponer de tecnologías de comunicación que permitan recoger, transmitir, intercambiar e integrar datos procedentes de sensores, equipos de campo, sistemas de control y plataformas digitales. Estos estándares y protocolos constituyen la "capa de comunicación" que conecta el mundo físico con el digital, garantizando que equipos de distintos fabricantes y generaciones puedan intercambiar información de forma fiable y, cuando es necesario, en tiempo real. Entre los más relevantes se encuentran:

- ***OPC UA:*** protocolo estándar para que máquinas y sistemas de distintos fabricantes intercambien datos de forma segura, muy usado en entornos industriales.
- ***MQTT:*** protocolo ligero diseñado para enviar pequeños paquetes de datos de forma muy eficiente, ideal cuando hay miles de sensores con conexión limitada.
- ***IEC 61850:*** estándar específico del sector eléctrico (visto en el primer esquema) para la comunicación entre equipos de subestaciones.
- ***Protocolos industriales (Modbus, DNP3, etc…):*** son formas más antiguas o específicas de comunicación entre dispositivos de campo y sistemas de control.

Una vez capturados y comunicados los datos procedentes de la red, el siguiente reto es procesarlos para convertir grandes volúmenes de información en datos útiles para la operación, supervisión y simulación del sistema eléctrico. En este ámbito se combinan tecnologías capaces de analizar grandes cantidades de datos de forma masiva con soluciones de computación distribuida que permiten procesarlos cerca del lugar donde se generan, reduciendo los tiempos de respuesta. Entre las principales se encuentran:

- ***Apache Spark:*** plataforma que permite procesar enormes cantidades de datos en paralelo, útil cuando se analizan históricos completos de una red.
- ***Computación en el borde (edge computing):*** procesar los datos cerca de donde se generan (en el propio sensor o subestación) en lugar de enviarlo todo a un servidor central, lo que reduce la latencia y permite respuestas casi instantáneas.

El procesamiento de estos datos genera información que debe conservarse, organizarse y estar disponible para su consulta por las diferentes aplicaciones de la Smart Grid y del gemelo digital.

Además de los datos procesados, en muchos casos es necesario conservar los datos originales para realizar análisis históricos, entrenar modelos predictivos o reconstruir el comportamiento de la red. Para ello existen diferentes tecnologías y arquitecturas de almacenamiento, entre las que destacan:

- ***MongoDB***: base de datos flexible, pensada para guardar datos con estructuras variables (no siempre la misma tabla rígida), habitual en proyectos con muchos tipos de sensores distintos.
- ***Cloud (Microsoft Azure, AWS):*** plataformas de almacenamiento y computación remotas que permiten guardar y acceder a los datos sin necesidad de servidores propios, escalando según la necesidad.

Una vez recopilados, procesados y almacenados los datos, el siguiente nivel consiste en extraer de ellos información útil para comprender el comportamiento de la red, detectar anomalías, anticipar posibles problemas y apoyar la toma de decisiones. Esta capa de analítica avanzada combina técnicas de inteligencia artificial, aprendizaje automático y métodos de razonamiento capaces de identificar patrones que no siempre son evidentes mediante un análisis convencional. En un gemelo digital, estas herramientas permiten pasar de una representación de lo que está ocurriendo en la red a una capacidad de diagnóstico y predicción de lo que puede ocurrir. Entre las principales tecnologías se encuentran:

- ***TensorFlow:*** herramienta para construir y entrenar modelos de inteligencia artificial, muy usada para tareas como predicción de fallos o de demanda.
- ***Redes neuronales:*** tipo de modelo de IA inspirado en el cerebro humano, capaz de aprender patrones complejos a partir de muchos datos (por ejemplo, reconocer cuándo un transformador empieza a fallar).
- ***Lógica difusa:*** técnica que permite tomar decisiones con información imprecisa o "a medias" (por ejemplo, clasificar una situación como "algo caliente" en lugar de exigir un valor exacto), útil en sistemas de control con incertidumbre.

Una vez que se dispone de los datos y de las herramientas de analítica, el siguiente paso es construir el modelo matemático que representa el comportamiento del sistema físico. La modelización permite traducir los componentes y procesos reales de una Smart Grid — generadores, líneas, transformadores, cargas, sistemas de almacenamiento, etc.— a ecuaciones y modelos computacionales capaces de reproducir su comportamiento. Esta representación constituye el núcleo del gemelo digital, ya que permite disponer de una réplica virtual del sistema sobre la que posteriormente pueden realizarse análisis y simulaciones. Entre las principales herramientas de modelización se encuentran:

- ***MATLAB/Simulink:*** entorno muy usado en ingeniería para crear modelos matemáticos y simular su comportamiento dinámico (por ejemplo, cómo responde una red ante una variación de carga).
- ***OpenDSS:*** software especializado en simular redes de distribución eléctrica.
- ***PowerFactory (DIgSILENT):*** software profesional para el análisis y planificación de redes eléctricas (flujos de carga, estabilidad, cortocircuitos).

- ***Modelica:*** lenguaje de modelado que permite representar sistemas físicos complejos (eléctricos, mecánicos, térmicos) de forma unificada.

Una vez construido el modelo matemático, la simulación permite utilizarlo como un entorno virtual de experimentación. En lugar de intervenir directamente sobre la infraestructura real, pueden reproducirse diferentes condiciones de funcionamiento, introducir perturbaciones o modificar variables para observar cómo respondería el sistema. Esto permite evaluar escenarios futuros, detectar posibles problemas, analizar riesgos y optimizar el funcionamiento de la red sin asumir los costes o riesgos de realizar las pruebas sobre la infraestructura física. Entre las principales técnicas y herramientas de simulación se encuentran:

- ***Simulación Monte Carlo:*** técnica que repite un cálculo miles de veces con datos de entrada ligeramente distintos (aleatorios) para estimar la probabilidad de distintos resultados, útil por ejemplo para evaluar el riesgo de fallo de un equipo.
- ***Método de elementos finitos:*** técnica que divide un objeto físico en pequeñas piezas ("elementos") para calcular cómo se comporta ante esfuerzos, calor o campos eléctricos, usada por ejemplo para simular el desgaste de un transformador.
- ***OpenFAST:*** software especializado en simular el comportamiento dinámico de turbinas eólicas (cargas, vibraciones, rendimiento).

2.3.4 APLICACIONES POR DOMINIO DE GENERACIÓN Y DISTRIBUCIÓN.

En el ámbito de generación eléctrica, los equipos modelados con mayor frecuencia son turbinas eólicas, sistemas fotovoltaicos, turbinas de vapor y de gas, y reactores nucleares. Para cada tipo de instalación, el gemelo digital se aplica habitualmente a nivel de componente o subsistema, modelando los elementos críticos del proceso de generación.

En el caso de la energía eólica, con los gemelos digitales se puede monitorizar en tiempo real el estado de cajas de engranajes, generadores y sistemas de pitch o de control de paso[25], anticipando averías que reducen tiempos de parada y mejoran la rentabilidad de la instalación. En energía solar fotovoltaica, suelen emplearse para la detección de anomalías, utilizando técnicas de *deep learning* y mejorar con ello la predicción de la potencia generada en función de condiciones meteorológicas. En el caso de la generación térmica, la modelización suele centrarse en la optimización del proceso de combustión, simulando el comportamiento de turbinas de gas y la gestión de la combustión. Curiosamente la generación hidráulica no está tan habitualmente modelada, a pesar de su importancia global, por la complejidad de generar un modelo digital realista de las instalaciones de generación hidráulica.

En el ámbito de la distribución, hay que contar con el lado de la generación (número de instalaciones y sus características) y la predicción de la demanda para el desarrollo de la modelización. Pero los sistemas y equipos físicos considerados en distribución son: microrredes,

[25] Sistemas de orientación de pala para optimizar la captura de energía en viento o para frenar la máquina.

subestaciones, redes de media tensión con integración de DERs[26] y centros de control SCADA. La arquitectura digital de la distribución eléctrica se apoya habitualmente en plataformas basadas en la nube para el alojamiento del gemelo, permitiendo que operadores de red (DSOs) y otros *stakeholders*[27] accedan a servicios de estimación de estado, planificación de operaciones y análisis de perturbaciones.

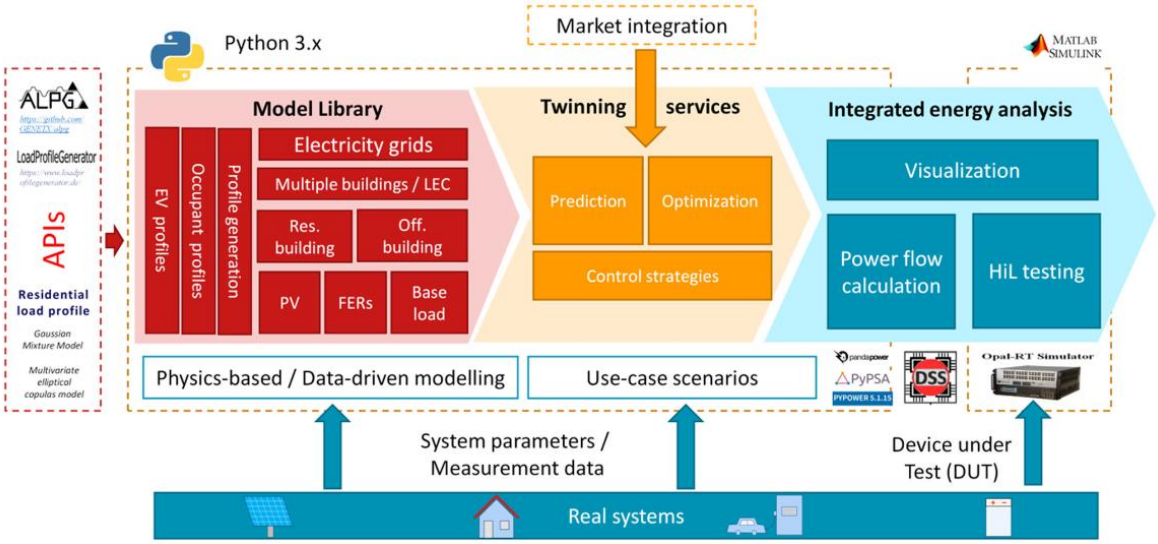

Ilustración 16. Representación[28] del gemelo digital de la red eléctrica

2.3.5 ANÁLISIS DE IMPACTO: SOCIAL, ECONÓMICO Y AMBIENTAL.

Impacto Social:

La adopción de gemelos digitales en la red eléctrica asturiana presenta implicaciones sociales que van más allá del aspecto técnico. Un gemelo digital permite simular el comportamiento de la red ante distintos escenarios (sobrecargas, fallos de equipos, eventos meteorológicos) y, gracias a esa simulación, anticipar averías antes de que ocurran y activar respuestas automáticas de control que evitan o acortan los cortes de suministro. Esta capacidad de anticipación beneficia principalmente a los ciudadanos y a las actividades económicas que dependen de un suministro estable. Puede resultar especialmente relevante en zonas rurales y de montaña, donde la red eléctrica suele tener menos puntos de redundancia y, por tanto, un fallo concreto tiene más probabilidades de dejar sin suministro a una zona entera durante más tiempo. En estos territorios, además, un corte de electricidad no es solo una molestia: puede significar la pérdida de productos en una explotación ganadera, la parada de un negocio turístico o la imposibilidad de mantener en marcha equipos médicos en el domicilio, de ahí que la mejora de

[26] Distributed Energy Resources se refieren a aquellos recursos de generación, almacenamiento o gestión de la energía que están conectados cerca de los puntos de consumo pudiendo llegar a ser a su vez puntos de consumo en sí mismos.
[27] Un stakeholder es cualquier persona, grupo u organización que tiene interés, influencia o que puede verse afectado por el funcionamiento o las decisiones de bien las instalaciones o proyectos.
[28] Fuente: https://link.springer.com/article/10.1007/s10207-023-00784-x

fiabilidad tenga aquí un impacto proporcionalmente mayor sobre la calidad de vida y la competitividad económica de la zona.

En términos de empleo, la implantación de esta tecnología implica una doble dinámica. Por un lado, genera demanda de nuevos perfiles profesionales como ingenieros de datos, expertos en modelización de sistemas eléctricos, especialistas en ciberseguridad industrial y técnicos de mantenimiento con competencias digitales avanzadas. Por otro lado, exige procesos de reconversión y formación del personal técnico que actualmente trabaja en las empresas del sector energético regional, cuyas competencias se han desarrollado en torno al mantenimiento correctivo tradicional y no necesariamente en torno al análisis de datos o la interpretación de modelos digitales. Esto puede suponer pérdida de empleo local y generación de empleo deslocalizado. No siempre el balance de generación de empleo es positivo.

La relación entre los gemelos digitales y las comunidades energéticas merece un análisis específico por la importancia que puede tener en el futuro. Una comunidad energética es una agrupación de consumidores (vecinos, pequeñas empresas, ayuntamientos) que comparten instalaciones de generación renovable y gestionan colectivamente su energía. Para que este tipo de instalaciones funcionen de forma segura y eficiente, se tiene que calcular en tiempo real cuánta energía produce cada instalación, cuánta consume cada miembro de la comunidad y cómo repartir los excedentes sin sobrecargar la red local. Un gemelo digital de la red de distribución es precisamente la herramienta que puede permitir simular y gestionar ese reparto, identificando si en un momento dado la red puede absorber sin problemas la energía que la comunidad quiere intercambiar. Por eso, cuantas más comunidades energéticas emergen en Asturias, mayor es la necesidad de contar con esta capacidad de simulación y más importante es que sus miembros entiendan y participen en cómo se diseña el sistema que va a gestionar su energía. Esa participación ciudadana en el diseño e implementación de estas soluciones no es solo deseable por motivos democráticos, sino que también mejora la probabilidad de que el sistema funcione bien en la práctica, ya que incorpora un elemento crítico en el proceso: el conocimiento real de cómo se usa la energía en cada comunidad.

Desde la perspectiva de la lucha contra la pobreza energética y la consecución una mayor equidad energética —entendida como el derecho de todas las personas a acceder a una energía asequible, fiable y suficiente para cubrir sus necesidades básicas, sin que su nivel de renta determine la calidad de ese acceso— la digitalización de la red puede ayudar significativamente a los hogares con menores recursos en este proceso. Esto puede lograrse de dos maneras concretas:

- por un lado, consiguiendo una red más eficiente que reduzca las pérdidas técnicas del sistema, lo que en teoría se traduce en un coste global del sistema eléctrico más bajo, parte del cual puede repercutir en las tarifas;
- por otro lado, los datos en tiempo real que proporciona una red inteligente permiten ofrecer tarifas dinámicas, donde el precio de la electricidad varía según la hora del día, dando a los consumidores la posibilidad de ahorrar si desplazan su consumo a las horas más baratas.

Sin embargo, aquí aparece un riesgo nuevo: estas tarifas dinámicas solo benefician a quien dispone de la información, el conocimiento y, en muchos casos, la tecnología (aplicaciones móviles, contadores inteligentes, electrodomésticos programables) necesaria para aprovecharlas. Un hogar con menos recursos económicos puede tener también menos acceso a internet, menos familiaridad con estas herramientas digitales o, simplemente, electrodomésticos antiguos que no permiten programar su consumo. Si no se acompaña la digitalización de la red con políticas activas de formación y de acceso equitativo a la tecnología, existe el riesgo de que la llamada brecha digital se traduzca en una brecha energética: los hogares con más recursos aprovechan las tarifas dinámicas para reducir su factura, mientras que los hogares más vulnerables, lejos de beneficiarse, podrían quedar relativamente más expuestos a la pobreza energética que antes. Por eso, el potencial de la digitalización para reducir la pobreza energética depende directamente de que su implantación vaya acompañada de medidas que garanticen el acceso universal a la formación y a las herramientas necesarias para beneficiarse de ella.

Impacto Económico:

La introducción de gemelos digitales puede presentar un impacto económico relevante en la red eléctrica asturiana: la reducción de costes operativos, la generación de nuevos servicios y la atracción de inversión y talento.

La reducción de costes operativos se explica por el cambio de modelo de mantenimiento que permite un gemelo digital. En lugar de esperar a que un equipo falle para repararlo (mantenimiento correctivo), el gemelo digital simula continuamente el estado de la instalación y permite anticipar cuándo un componente empezará a degradarse, programando su revisión antes de que se produzca una avería (mantenimiento predictivo). Esto resulta más económico porque evita las paradas de producción no planificadas, que son las que generan mayores pérdidas de rentabilidad: una parada programada puede organizarse en un momento de baja demanda, mientras que una avería inesperada detiene la producción en cualquier instante, con el coste añadido de la reparación urgente. Se estima que la aplicación de esta estrategia en centrales hidráulicas del tipo de las existentes en Asturias, que de media tienen unos 40 años de antigüedad, podría reducir el coste de mantenimiento entre un 10% y un 25%, dependiendo del grado de desarrollo del gemelo digital implementado. La optimización del rendimiento en las instalaciones genera también un impacto económico directo. Los incrementos de eficiencia son, en principio, modestos —entre el 1% y el 2% en una central de 100 MW—, pero al aplicarse de forma continua durante toda la vida útil de la instalación, ese pequeño porcentaje se traduce en un volumen de energía adicional generada significativo a largo plazo, sin necesidad de invertir en nueva capacidad de generación. Para los operadores de red, existe además un ahorro relacionado con la reducción de pérdidas técnicas en distribución: al poder calcular y ajustar en tiempo real cómo fluye la potencia por la red (en lugar de operar con estimaciones aproximadas), es posible detectar y corregir ineficiencias puntuales. En una red con la extensión y las características topográficas de Asturias —con zonas de orografía complicada y distancias considerables entre puntos de generación y consumo—, esta capacidad de ajuste fino puede traducirse en ahorros relevantes, precisamente porque ese tipo de topografía tiende a generar más pérdidas que una red más compacta y homogénea.

En términos de generación de nuevos servicios, los gemelos digitales abren la puerta a modelos de negocio basados en comercializar capacidad de simulación y análisis predictivo a terceros, como compañías de seguros (que podrían usar esos modelos para evaluar riesgos de fallo de instalaciones), comercializadoras energéticas, agregadores de demanda o promotores de instalaciones renovables. La propia capacidad de modelización de la red asturiana, una vez desarrollada, se convierte en un activo intangible de alto valor para las empresas del sector, comparable al conocimiento o la propiedad intelectual: no es un bien físico, pero puede venderse, licenciarse o usarse como ventaja competitiva.

Finalmente, puede representar una oportunidad de atracción de talento, inversión y nuevas actividades empresariales. La combinación de una base industrial relevante, capacidades en ingeniería y energía y una creciente digitalización del sistema energético puede favorecer la creación de un ecosistema especializado en tecnologías como IA, simulación, analítica de datos, ciberseguridad, automatización y gestión inteligente de redes. Con ello, se podrían atraer empresas tecnológicas, centros de I+D, proyectos piloto e inversión privada, al tiempo que generar demanda de perfiles cualificados y favorecer la retención y captación de talento vinculado a la ingeniería, las TIC y la energía. Además, la posibilidad de utilizar Asturias como entorno de demostración de soluciones digitales para redes eléctricas industriales permitiría convertir las necesidades de modernización del sistema energético en una palanca para desarrollar nuevas capacidades exportables a otros territorios y mercados.

Impacto Ambiental:

Los gemelos digitales contribuyen a reducir las emisiones del sistema eléctrico sin necesidad de construir nueva infraestructura física: lo consiguen analizando y optimizando el uso de los recursos ya existentes. Este impacto se materializa principalmente a través de las tres vías: la optimización e integración de las energías renovables, la reducción de la huella de carbono de las operaciones, y la mejora de la resiliencia de la red ante eventos climáticos adversos.

La mayor capacidad de predicción de la generación renovable intermitente, como la eólica y la fotovoltaica, que ofrecen los gemelos digitales permite al operador de red incrementar la cuota de energía renovable que puede integrarse de forma segura en el sistema, reduciendo la dependencia de unidades de respaldo basadas en combustibles fósiles para gestionar las desviaciones entre generación y demanda. Esta capacidad resulta especialmente relevante para Asturias: el Principado se ha fijado el objetivo de alcanzar un 40% de energía renovable en su mix energético para 2030, y cumplir ese objetivo no depende solo de instalar más capacidad renovable, sino de que la red sea capaz de absorber su naturaleza variable sin poner en riesgo la estabilidad del suministro. Es precisamente esa capacidad de anticipación y ajuste en tiempo real la que permite avanzar hacia la descarbonización sin comprometer la fiabilidad del sistema eléctrico regional.

Los gemelos digitales también contribuyen a alargar la vida útil de los activos de generación hidráulica, al permitir detectar el desgaste de sus componentes con suficiente antelación como para repararlos y sustituirlos de forma parcial, en lugar de tener que renovar el equipo completo de forma prematura. Esto tiene una consecuencia ambiental directa: al retrasarse la sustitución de los equipos, se retrasa también la necesidad de fabricar y transportar nueva maquinaria

pesada, un proceso que por sí mismo consume materiales y energía, y genera con ello emisiones evitables.

La reducción de pérdidas en la red de distribución, posible gracias al cálculo y ajuste en tiempo real de cómo fluye la energía por la red, tiene asimismo un impacto ambiental que puede cuantificarse de forma directa. Toda la energía que se pierde en forma de calor durante su transporte y distribución es energía que la central debe generar de más para cubrir la demanda real, así que reducir esas pérdidas significa que la red necesita generar menos electricidad en total para abastecer al mismo número de consumidores. Si esa generación adicional —la que se evita— procediera de fuentes fósiles o de centrales de respaldo como los ciclos combinados de gas, evitar generarla implica evitar directamente las emisiones de CO_2 asociadas a su producción.

Finalmente, la mejora de la resiliencia de la red ante fenómenos meteorológicos extremos añade una dimensión ambiental que va más allá de lo puramente económico. La capacidad de simular cómo reaccionará la red ante una perturbación y de activar automáticamente respuestas de control para minimizar su impacto reduce el riesgo de apagones prolongados, que en episodios de ola de calor o frío extremo pueden tener consecuencias graves tanto para la salud pública —por ejemplo, al afectar a sistemas de refrigeración o calefacción esenciales para personas vulnerables— como para ecosistemas y actividades que dependen de un suministro eléctrico continuo.

2.3.6 CIBERSEGURIDAD.

La implementación de gemelos digitales dentro de las redes eléctricas inteligentes introduce una nueva exposición a ciberataques que debe afrontar la infraestructura crítica que es la red eléctrica.

El sector eléctrico ya era un objetivo prioritario de protección frente a ciberdelincuentes antes de que la digitalización y los gemelos digitales se incorporaran a la legislación específica, precisamente por tratarse de un servicio esencial cuya interrupción afectaría de forma inmediata a la población, a otros servicios críticos dependientes (hospitales, telecomunicaciones, transporte) y a la actividad económica en su conjunto. El marco regulatorio europeo y español de ciberseguridad ha evolucionado de forma acelerada en los últimos años para dar respuesta a este escenario. La Directiva NIS2 (2022/2555/UE), aplicada en España mediante el Real Decreto-ley 12/2022, representa un salto normativo respecto a la NIS original de 2016, tanto en el alcance de los sujetos obligados como en la intensidad de las medidas exigidas y la responsabilidad personal de los órganos de dirección.

En lo que respecta concretamente al sector energético, NIS2 amplía el ámbito de aplicación más allá de los grandes operadores de transporte y distribución que ya estaban sujetos a la normativa anterior, incorporando a un número mayor de empresas (generadoras, comercializadoras, gestores de instalaciones de almacenamiento y, en determinadas condiciones, operadores de infraestructuras de recarga) y reduciendo los umbrales que determinan la obligatoriedad de cumplimiento. Esta ampliación de lo que se denomina perímetro regulatorio es especialmente relevante en el contexto de los gemelos digitales, ya que estas plataformas no solo replican el

comportamiento de grandes infraestructuras de transporte, sino también de activos más pequeños y distribuidos —microrredes, instalaciones de generación renovable, comunidades energéticas— que hasta ahora podían quedar fuera del foco regulatorio tradicional, pero que pasan a integrarse en el mismo ecosistema digital e interconectado que los grandes operadores. Esta ampliación de sujetos obligados y de superficie de exposición de ciberseguridad conecta directamente con los riesgos específicos de esta materia que introducen los propios gemelos digitales, que se desarrollan en el apartado siguiente.

Paralela y complementariamente, la normativa de protección de infraestructuras críticas gestionada por el CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas, dependiente del Ministerio del Interior) impone un segundo cuerpo de obligaciones que también se relaciona con NIS2.

2.3.7 PANORAMA DE AMENAZAS Y JUSTIFICACIÓN REGULATORIA.

El sector energético europeo ha experimentado un incremento de los ciberataques en los últimos 5 años. Entre los ejemplos más recientes dentro del marco europeo la red eléctrica de Ucrania fue víctima de un ciberataque por parte de malware (BlackEnergy, Industroyer) que demostró que actores externos estaban capacitados para causar interrupciones físicas del suministro eléctrico mediante ataques dirigidos a los sistemas SCADA de la red.

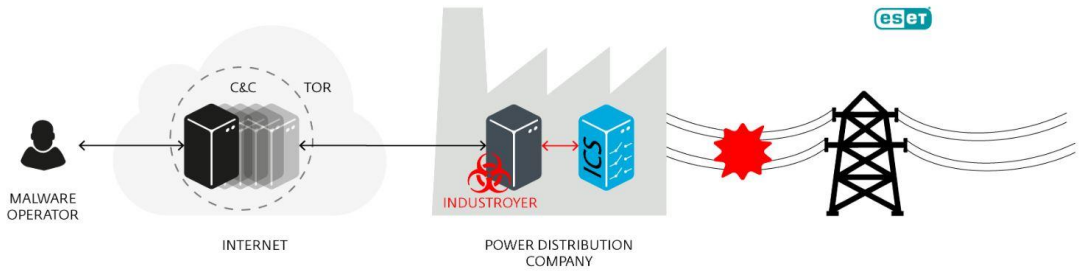

Ilustración 17.Representación[29] de un ciberataque por Industroyer

Desde esos sucesos, la ENISA[30] documenta un incremento de los incidentes dirigidos contra el sector energético. Con el uso de gemelos digitales de la red eléctrica, los tipos de ataque más relevantes que se han identificado son:

- ***Aprovechamiento de fallos de software:*** Como cualquier programa informático, el software que soporta el gemelo digital puede tener errores o "agujeros" de seguridad, a través de los que un atacante puede acceder al sistema sin permiso.
- ***Ataques a través de las herramientas que utiliza el gemelo digital:*** El gemelo digital depende de programas externos (como MATLAB u otras librerías de modelización) que se actualizan con frecuencia. Si un atacante consigue infectar una de estas herramientas

[29] Fuente: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf
[30] Agencia Europea para la Ciberseguridad

en su origen —antes incluso de que la empresa eléctrica la descargue o instale—, ese software malicioso entraría en el sistema de forma indirecta, "camuflado" dentro de una actualización o librería que en apariencia es legítima.

- ***Manipulación de los datos que recibe el gemelo digital:*** El gemelo digital toma decisiones (o ayuda al operador a tomarlas) basándose en los datos que recibe de la red real. Si un atacante consigue alterar esos datos de entrada —por ejemplo, haciendo que el sistema "vea" valores de tensión o consumo erróneos o falsos—, puede engañar al gemelo digital para que recomiende tomar una decisión equivocada, sin que el operador sea consciente de que está actuando sobre información manipulada.
- ***Uso del gemelo digital como puerta de entrada a los sistemas de control reales:*** El gemelo digital necesita comunicarse constantemente con los equipos físicos de la red para mantenerse actualizado y, en algunos casos, para enviarles órdenes de control. Esa misma vía de comunicación, si no está bien protegida, podría ser utilizada por un atacante para "saltar" desde el gemelo digital (un entorno más expuesto, al estar conectado a redes informáticas convencionales) hasta los sistemas de control reales de la red eléctrica (el entorno más sensible, donde un fallo puede tener consecuencias físicas directas, como un corte de suministro).
- ***Saturación de la plataforma del gemelo digital:*** Por último, un atacante podría intentar saturar deliberadamente con peticiones la plataforma donde funciona el gemelo digital, dejándola sin capacidad de respuesta justo en los momentos en los que más se necesita —por ejemplo, durante un pico de demanda o una situación de emergencia—, impidiendo así que el operador disponga de la información que necesita para tomar decisiones en ese momento crítico.

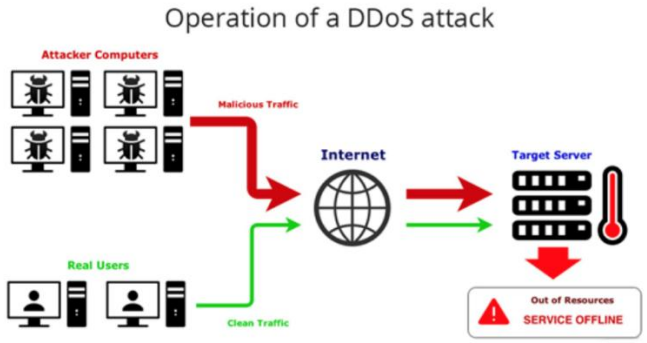

Ilustración 18. Esquema[31] operativo de un ataque DDOS.

El diagrama ilustra el mecanismo central que confiere a este tipo de ataques su capacidad disruptiva. En la imagen se observa cómo se mezcla el tráfico de usuarios legítimos con el tráfico malicioso generado por una red de equipos comprometidos, lo que impide al servidor objetivo discriminar entre ambos y conduce al agotamiento de sus recursos. Esta misma lógica —saturar un canal de comunicación crítico para degradar la capacidad de respuesta de un operador— ya

[31] Fuente: https://nextvision.com/tag/ddos/

se ha observado combinada con otros vectores de ataque en infraestructuras energéticas reales. En el ataque a la red eléctrica ucraniana de 2015, los atacantes no solo tomaron el control de varias subestaciones, sino que bloquearon el servicio telefónico mediante un ataque tipo TDoS dirigido específicamente a impedir que los clientes afectados pudieran reportar el corte, retrasando así la respuesta de los operadores. Este caso muestra que el riesgo de un ataque DDoS no se limita a la indisponibilidad de un servicio digital aislado: cuando se combina con otras técnicas e incide sobre canales de gestión o comunicación críticos, puede amplificar significativamente el impacto de un incidente físico simultáneo, reforzando así la necesidad de que el marco regulatorio exija capacidades de detección y mitigación que abarquen toda la cadena operativa, y no únicamente los sistemas de control industrial.

2.3.8 DIRECTIVA NIS2.

La directiva NIS2 introduce un método de clasificación binaria entre entidades esenciales y entidades importantes, con obligaciones de base similares, pero con una intensidad de supervisión y sanciones diferenciadas.

Ilustración 19. Sectores[32] de Aplicación de NIS2

Para el sector eléctrico, quedan clasificadas como entidades esenciales bajo el Anexo I (con exigencias máximas de ciberseguridad): los gestores de redes de transporte de electricidad, los gestores de redes de distribución que superen los umbrales de tamaño definidos por la normativa (empresas de tamaño medio con más de 50 trabajadores o un volumen de negocio superior a los 10 millones de euros), los operadores de puntos de intercambio de electricidad, los proveedores de servicios de balance de electricidad y los operadores de instalaciones de almacenamiento de energía si tienen carácter esencial para la red.

Un aspecto crítico para los proyectos de gemelo digital es que la NIS2 extiende las obligaciones de ciberseguridad a la cadena de suministro. Obliga a las entidades esenciales a gestionar la seguridad de la cadena de suministro, incluyendo los aspectos de seguridad relativos a las

[32] Fuente: INCIBE (Instituto Nacional de Ciberseguridad de España).

relaciones entre cada entidad y sus proveedores o prestadores de servicios directos. Esto implica también a las empresas de modelización, integradores de sistemas y proveedores de servicios en la nube. Quedan indirectamente vinculados a los requisitos de seguridad, que el operador de red está obligado a trasladarles contractualmente. La distribuidora no puede delegar su responsabilidad del NIS2 en ningún proveedor, pero si puede:

- Realizar diligencias de ciberseguridad antes de contratar proveedores de la plataforma del gemelo.
- Incluir cláusulas contractuales de seguridad (SLAs[33] de parcheado, notificación de incidentes, derecho de auditoría) en todos los contratos con proveedores TIC relevantes.
- Revisar periódicamente la seguridad de sus proveedores críticos.
- Exigir que los proveedores notifiquen cualquier incidente que les pueda afectar.

2.3.9 MEDIDAS DE GESTIÓN DE RIESGOS.

El artículo 21 de la NIS2 es el núcleo de las obligaciones técnicas y organizativas. Impone a las entidades esenciales la adopción de medidas técnicas, operativas y organizativas adecuadas y proporcionales para realizar la correcta gestión de riesgos que se planteen para la seguridad de los sistemas de redes y de información que esas entidades utilizan en sus actividades o en la prestación de sus servicios.

El principio de proporcionalidad es fundamental. Las medidas deben de estar calibradas en función del nivel de riesgo, el tamaño de la entidad y la probabilidad de que se produzcan incidentes además de considerar su gravedad potencial. En los siguientes subapartados se tratará su aplicación al contexto del gemelo digital:

Políticas de análisis de riesgo y seguridad de los sistemas de información:

El operador debe disponer de una metodología documentada de análisis de riesgo que contemple específicamente los sistemas del gemelo digital. Esto implica realizar un inventario de activos del gemelo (plataforma de modelización, bases de datos históricas, interfaces de comunicación con OT, APIs de acceso externo), identificar amenazas y vulnerabilidades para cada activo, valorar el impacto potencial de su compromiso sobre la operación de la red, y documentar las medidas de mitigación adoptadas.

Se emplean la norma ISO/IEC 27005 (gestión de riesgos de seguridad de la información) y la norma IEC 62443-3-2 (evaluación de riesgos de seguridad en sistemas de automatización industrial) como referencias.

[33] Acuerdos de Nivel de Servicio para Parcheado.

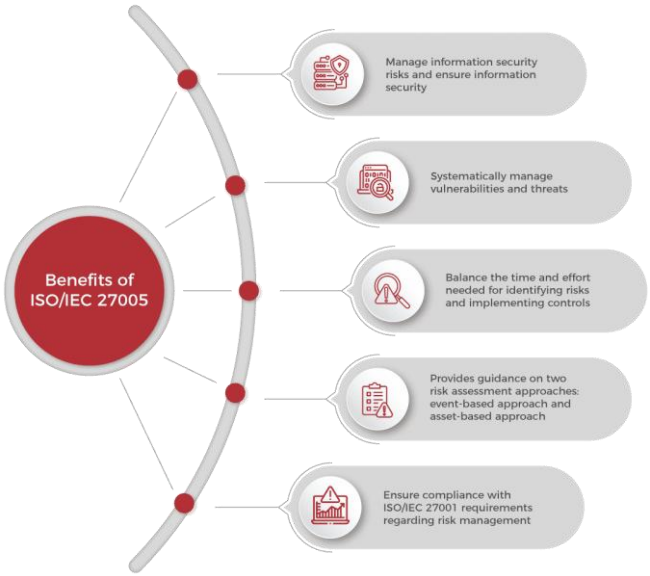

Ilustración 20. Beneficios[34] de la norma ISO/IEC 27005

Para el caso asturiano, el análisis de riesgo debería incluir un apartado específico sobre la interfaz entre el gemelo digital y los sistemas de control de cada tipo de activo de generación presente en la región: centrales hidráulicas (con PLCs de distintas generaciones), parques eólicos (con sistemas de control SCADA siendo este un software que es propiedad de los fabricantes de turbinas) y las nuevas instalaciones fotovoltaicas con inversores conectados a IP. Cada uno de estos entornos presenta un perfil de riesgo diferente que el gemelo digital debe poder gestionar sin constituirse en vector de propagación de incidentes entre instalaciones.

Gestión de incidentes:

La NIS2 impone la existencia de procedimientos documentados para la detección, respuesta, recuperación y notificación de incidentes de seguridad. Para el gemelo digital, esto requiere la integración de los sistemas de monitorización de seguridad del gemelo (logs de acceso, alertas de anomalías de tráfico, detección de comportamientos anómalos en los modelos de datos) con el SOC (Security Operations Center) del operador, si existe, o con un servicio gestionado de ciberseguridad (MSSP) externo.

Un requisito especialmente relevante es la capacidad de operar la red en modo degradado[35] si el gemelo digital es comprometido o no está disponible. El operador debe definir cuáles de las funciones operativas normalmente apoyadas por el gemelo pueden sostenerse con procedimientos manuales o con sistemas alternativos, y cuáles suponen una pérdida de capacidad crítica que activa el plan de continuidad de negocio.

Continuidad de negocio y gestión de crisis

[34] Fuente: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27005

[35] Capacidad de un sistema o infraestructura crítica de seguir funcionando y prestando servicios esenciales, aunque sea de forma limitada o con capacidades reducidas, tras haber sufrido un incidente grave, como puede ser un ciberataque.

La normativa NIS2 es más estricta que las normas anteriores en un punto fundamental: el Plan de Continuidad de Negocio, que debe contemplar también la posibilidad de que el gemelo digital sea atacado o comprometido digitalmente, y no solo los fallos físicos de los equipos o los desastres naturales como inundaciones o tormentas; es decir, hay que prepararse tanto para un hackeo como para una avería.

En la práctica, esto implica que el Plan de Continuidad de Negocio (BCP) del operador de la red de distribución debe definir con claridad cuánto tiempo, como máximo, se puede tardar en recuperar el gemelo digital tras un incidente sin que esto cause un perjuicio grave (RTO, o "tiempo objetivo de recuperación"), así como cuánta información se puede permitir perder en el peor de los casos, medida en el tiempo transcurrido desde la última copia de seguridad fiable (RPO, o "punto objetivo de recuperación").

A esto se suma la necesidad de contar con procedimientos probados para restaurar el sistema a partir de copias de seguridad, asegurándose primero de que estas no hayan sido también comprometidas por el atacante.

Igualmente importante es establecer cómo y cuándo informar a INCIBE-CERT[36], el organismo encargado de supervisar este tipo de incidentes, durante el desarrollo de la crisis, así como contar con mecanismos claros de coordinación con otros operadores de la red que puedan verse afectados si la capacidad de gestión y control se degrada, evitando así que el problema se propague sin control.

Seguridad de la cadena de suministro

Este requisito tiene implicaciones contractuales directas. Todo contrato de adquisición o arrendamiento de software para el gemelo digital, de servicios nube de alojamiento, de integración de sistemas o de mantenimiento de la plataforma debe incluir cláusulas que establezcan:

- obligaciones de seguridad del proveedor alineadas con NIS2,
- derecho del DSO a auditar la postura de seguridad del proveedor,
- obligación de notificación inmediata de incidentes que puedan afectar al DSO,
- y compromisos de plazos de parcheado de vulnerabilidades críticas (máximo 24-72 horas para vulnerabilidades activamente explotadas bajo el Cyber Resilience Act).

Seguridad en la adquisición, desarrollo y mantenimiento de sistemas

Este requisito impone la aplicación de prácticas de desarrollo seguro (Secure Software Development Lifecycle, SSDLC) a los componentes del gemelo digital que sean desarrollados a medida o adaptados. En concreto requiere desarrollar acciones como:

- análisis de composición de software (SCA) para identificar vulnerabilidades en dependencias de terceros,

[36] Es el centro de respuesta a incidentes de seguridad en España disponible para ciudadanos, entidades de derecho y operadores críticos. Su objetivo es prevenir, detectar y mitigar las amenazas cibernéticas.

- revisión de código orientada a seguridad,
- pruebas de penetración del gemelo completo antes de su puesta en producción y en cada actualización mayor,
- y gestión de vulnerabilidades con proceso documentado de priorización y remedición.

Políticas y procedimientos para evaluar la eficacia de las medidas de ciberseguridad

NIS2 impone la evaluación periódica de la eficacia real de las medidas de seguridad, no solo su existencia formal. Para el gemelo digital, esto significa:

- auditorías de seguridad internas y externas con periodicidad mínima anual,
- ejercicios de *red team* (simulación de ciberataques avanzados de alta intensidad y a gran escala) contra la plataforma del gemelo,
- métricas de seguridad operativa (tiempo medio de detección de incidentes, tiempo medio de respuesta, porcentaje de sistemas con vulnerabilidades no parcheadas) reportadas al consejo de administración o órgano equivalente,
- y revisión del análisis de riesgo al menos anualmente o tras cambios significativos en el sistema.

Prácticas básicas de higiene informática

La higiene informática es el conjunto de prácticas básicas y rutinarias que reducen la superficie de ataque de un sistema, de forma análoga a las actuaciones preventivas, no se elimina el riesgo, pero se reduce la probabilidad de que un incidente menor se convierta en uno grave. Normalmente el proceso incluye aspectos como:

- gestión de contraseñas robustas y autentificación multifactorial,
- aplicación regular de parches y actualizaciones de software,
- copias de seguridad periódicas y verificadas,
- control de acceso (privilegios mínimos),
- concienciación frente a phishing e ingeniería social,
- inventario actualizado de activos y software (especialmente relevante en entornos OT/ICS),
- y segmentación de redes.

Legalmente el concepto de “ciberhigiene” queda recogido en la Directiva NIS2 en su artículo 21.2.g, incluye entre las medidas de gestión de riesgos que las entidades deben adoptar *"prácticas básicas de ciberhigiene y formación en materia de ciberseguridad"*. Es una de las pocas directivas europeas que usa literalmente el término "ciberhigiene" en el texto legal, aunque no ofrece una definición cerrada y exhaustiva de qué prácticas concretas la componen — deja ese desarrollo a las autoridades nacionales y a estándares técnicos de referencia (como ENISA o ISO 27001).

Políticas y procedimientos de criptografía

El requisito criptográfico de NIS2 exige el uso de cifrado en todos los canales de comunicación del gemelo digital que transporten datos sensibles (datos de medida, parámetros de configuración, comandos de control) y en los sistemas de almacenamiento que contengan esos datos. Las normas de referencia son: TLS 1.3 (mínimo TLS 1.2) para comunicaciones en tránsito, AES-256 para almacenamiento en reposo, y el guía de criptografía del CCN[37] (CCN-STIC 807) como estándar nacional de referencia para entidades que interactúan con la Administración.

Un aspecto crítico para el gemelo digital de red eléctrica es la gestión de claves criptográficas en un *entorno OT con restricciones de latencia*[38]. Los sistemas SCADA y los protocolos industriales clásicos no fueron diseñados para soportar la sobrecarga de procesamiento del cifrado. La arquitectura de seguridad del gemelo debe resolver esta limitación —por ejemplo, mediante la aplicación de cifrado a nivel de zona de red en lugar de a nivel de paquete en los entornos OT más sensibles a la latencia— sin comprometer los tiempos de respuesta operativa de la red.

Seguridad de los recursos humanos, políticas de control de acceso y gestión de activos

Este requisito abarca tres ámbitos interconectados. En materia de recursos humanos, el operador debe realizar verificaciones de antecedentes del personal con acceso a sistemas críticos del gemelo digital (en línea con lo que ya exige el artículo 14 del Reglamento de la Ley PIC para los operadores de infraestructuras críticas), establecer procedimientos de revocación inmediata de accesos ante ceses o cambios de rol, y gestionar los riesgos de ingeniería social mediante protocolos de verificación de identidad robustos.

En materia de control de acceso, el principio de mínimo privilegio debe aplicarse con rigor especial al gemelo digital: ningún usuario debe tener más acceso del estrictamente necesario para su función. La autenticación multifactorial (MFA) es obligatoria para todos los accesos remotos y para los accesos con privilegios elevados sobre la plataforma del gemelo. El acceso de proveedores externos durante labores de mantenimiento debe gestionarse mediante sesiones de acceso privilegiado controlado (PAM, Privileged Access Management[39]), registradas y auditables en su totalidad.

Uso de soluciones de autenticación multifactor o autenticación continua

NIS2 eleva la autenticación multifactor a requisito explícito para entidades esenciales. Para el gemelo digital, esto implica que todos los accesos a la plataforma —administración del sistema, interfaces de operador, APIs[40] de datos, accesos de proveedores— deben estar protegidos con MFA. Las soluciones basadas únicamente en usuario y contraseña no son admisibles para los

[37] Son el conjunto de normas e instrucciones, criptografía del ENS considerando los requisitos criptográficos del Esquema Nacional de Seguridad en España.
[38] Una OT o tecnología de operación es una red de control industrial donde los procesos físicos dependen de que los datos se transmitan y procesen de forma prácticamente instantánea y en un período de tiempo real estricto, con márgenes de retraso que a menudo se miden en milisegundos (ms) o microsegundos (µs)
[39] Es una solución de ciberseguridad que se centra en la supervisión y control de las cuentas con permisos de administración de forma que el sistema actúe como una caja fuerte digital que evita tanto el robo de credenciales y abuso de privilegios.
[40] *Application Programming Interfaces* , o Interfaces de Programación de Aplicaciones de Datos.

sistemas del gemelo digital de una entidad esencial. El estudio de viabilidad técnica de la implementación del gemelo debe incluir el diseño del sistema de gestión de identidades y accesos (IAM) desde las fases iniciales del proyecto.

2.3.10 OBLIGACIÓN DE NOTIFICACIÓN DE INCIDENTES.

Uno de los cambios más significativos de la normativa NIS2 respecto al régimen anterior es el plazo de notificación de incidentes significativos. Se entiende por incidente significativo aquel que causa o puede causar graves perturbaciones operativas o pérdidas económicas para la entidad afectada, o que afecte a otras personas físicas o jurídicas causando pérdidas considerables.

En el caso de la red eléctrica esto afecta a cualquier incidente que afecte a la disponibilidad del suministro a un determinado número de usuarios que a nivel español aún no ha sido definido. A continuación, se muestra el procedimiento tabulado a seguir:

Plazo	Tipo de comunicación	Contenido mínimo
24 horas	Alerta temprana al CSIRT (INCIBE-CERT)	Tipo de incidente, impacto potencial, medidas iniciales
72 horas	Notificación formal al CSIRT	Causa probable, medidas adoptadas, impacto estimado
1 mes	Informe final	Descripción completa, causa raíz, remedición, lecciones aprendidas

La comunicación con el responsable de ciberseguridad del operador es un aspecto organizativo crítico que debe estar resuelto antes de la puesta en marcha del gemelo digital. Los dos procesos de notificación AEPD[41] bajo RGPD[42] e INCIBE-CERT bajo NIS2 tienen plazos coincidentes pero contenidos y destinatarios diferentes, y en la práctica deben ejecutarse en paralelo durante un incidente que involucre datos personales y compromiso de sistemas.

2.3.11 SISTEMA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y COORDINACIÓN AUTONÓMICA.

Por ley se establece que un sistema de protección de red de una infraestructura crítica deberá involucrar al CNPIC[43], al Ministerio para la Transición Ecológica, los cuerpos y fuerzas de seguridad del estado, los servicios de inteligencia (CNI) y las comunidades autónomas.

[41] Agencia Española de Protección de Datos
[42] Reglamento General de Protección de Datos Europeo
[43] Centro Nacional de Protección de Infraestructuras Críticas (Organismo dependiente del Ministerio del Interior)

Aunque se debe considerar que las comunidades autónomas no tienen competencias propias en la protección de la infraestructura crítica que tengan un carácter nacional, en el caso del principado de Asturias este participa en el sistema a través del Plan Especial de Infraestructuras Críticas de la Región que a su vez está integrado en el catálogo nacional.

Esta coordinación es especialmente relevante para el gemelo digital, porque los incidentes en la red eléctrica tienen efectos que se manifiestan en el territorio de la Comunidad Autónoma y requieren coordinación con los Servicios de Emergencias de Asturias y con la Consejería competente en la materia.

El plan de gestión de crisis del gemelo digital debe incluir los protocolos de comunicación con las autoridades autonómicas en escenarios de incidente grave, y estos protocolos deben formar parte, a su vez, de las instrucciones de entrenamiento del personal. Esto implica que no basta con documentar a quién notificar y en qué plazos: el personal de operación debe practicar la activación real de estos protocolos mediante simulacros periódicos, en los que se definan con claridad quién declara el incidente, en qué momento se notifica a la Consejería de Presidencia o a los Servicios de Emergencias de Asturias, y qué información mínima debe transmitirse en cada notificación. La realización y evaluación de estos simulacros debe quedar documentada, de forma que constituya la evidencia demostrable ante la autoridad supervisora de que el personal está efectivamente preparado para ejecutar el protocolo en un escenario real, y no únicamente sobre el papel.

2.3.12 INTERACCIÓN ENTRE EL RÉGIMEN CNPIC Y LA NIS2.

La coexistencia de la legislación de la ley CNPIC y de la NIS2 crea áreas de solapamiento, tal como se resume dicha información en la siguiente tabla.

Aspecto	Régimen CNPIC	Régimen NIS2 / RDL 12/2022
Autoridad competente	CNPIC (Ministerio del Interior)	INCIBE (sector privado) / CCN (sector público)
Tipo de obligación	Protección física y lógica integral	Gestión de riesgos cibernéticos
Documento clave	PSO + PPE por instalación	Política de gestión de riesgos corporativa
Responsabilidad	DSE (Delegado de Seguridad y Enlace)	Órgano de dirección (art. 20 NIS2)
Notificación de incidentes	CNPIC + autoridad sectorial	INCIBE-CERT: 24h alerta / 72h notificación

Aspecto	Régimen CNPIC	Régimen NIS2 / RDL 12/2022
Periodicidad de actualización	Cada 2 años o tras cambio significativo	Anual o tras cambio significativo
Sanciones	Ley PIC: infracción administrativa	Hasta 10 M€ o 2% volumen de negocio mundial
Publicidad	PSO y PPE: confidenciales	Medidas de seguridad: confidenciales

A la hora de realizar la implementación sería recomendable integrar el cumplimiento de ambas estructuras en un único programa de gestión de seguridad que evite la duplicación de estructuras y de documentación.

2.3.13 NORMAS TÉCNICAS DE REFERENCIA PARA EL GEMELO DIGITAL.

IEC 62443: Estándar de seguridad de referencia

La familia de normas IEC 62443 es el estándar internacional de referencia para la ciberseguridad de los sistemas de automatización y control industrial. Esto incluye los sistemas SCADA y OT de las redes eléctricas. Su relevancia para el gemelo digital es doble dado que es la norma que gobierna la seguridad de los sistemas con los que el gemelo se integra, y es la norma que debería gobernar la seguridad del propio canal de comunicación entre el gemelo y esos sistemas.

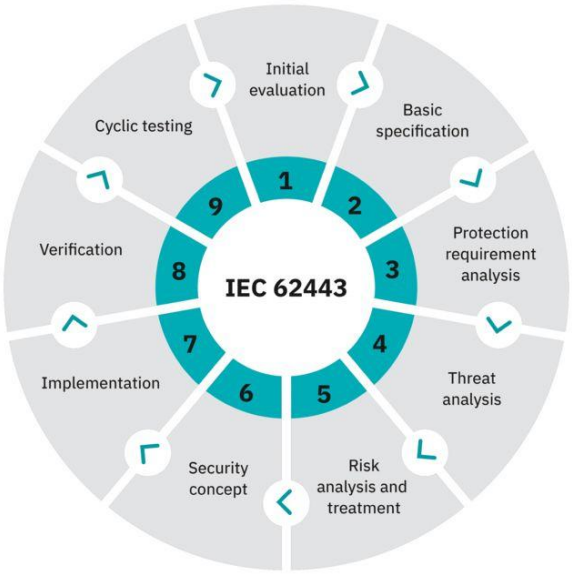

Ilustración 21.Norma[44] IEC 62443

La norma se organiza en cuatro series:

- la Serie 1 (General) establece conceptos y modelos,
- la Serie 2 (Políticas y Procedimientos) define los requisitos para el sistema de gestión de seguridad de los IACS[45],
- la Serie 3 (Sistema) define los requisitos para el sistema de control y sus zonas de seguridad,
- la Serie 4 (Componentes) define los requisitos para los componentes individuales.

La IEC 62443-3-2 (Evaluación de riesgos para el diseño del sistema) es especialmente relevante para el diseño de la arquitectura de seguridad del gemelo digital. Introduce el concepto de Zona de Seguridad (Security Zone) y Conducto (Conduit): el gemelo digital debe situarse en su propia zona de seguridad, separada tanto de la red IT corporativa como de las zonas OT[46] de la red eléctrica, con conductos controlados y auditados que gestionen el flujo de datos entre zonas. Esta "arquitectura de zonas" es el mecanismo fundamental para evitar que un ataque al gemelo se propague a los sistemas de control de la red.

La IEC 62443-2-4 define los requisitos de seguridad para los proveedores de servicios que integran o mantienen sistemas IACS, y es la norma que las distribuidoras asturianas deben exigir a sus integradores de sistemas y proveedores de mantenimiento del gemelo digital. La certificación de proveedores contra IEC 62443-2-4 es la forma más robusta de cumplir con el requisito de seguridad de la cadena de suministro del artículo 21.2.d de la NIS2.

[44] Fuente: Phoenix Contact.
[45] Industrial Automation and Control Systems, es decir, sistemas de automatización y control industrial
[46] Tecnología Operativa dedicada al control de la maquinaria industrial.

ISO/IEC 27019: Seguridad en el sector energético

La ISO/IEC 27019 es una extensión sectorial de la norma ISO/IEC 27001 que proporciona controles específicos para los sistemas de control de los procesos en la industria energética. Su ventaja respecto a la ISO/IEC 27001 genérica es que entiende el contexto operativo especial de las redes eléctricas la prioridad de la disponibilidad sobre la confidencialidad (en un SCADA, que el sistema esté operativo puede ser más crítico que sus datos estén cifrados), los sistemas de tiempo real y sus restricciones de latencia, y la integración de tecnologías OT heredadas.

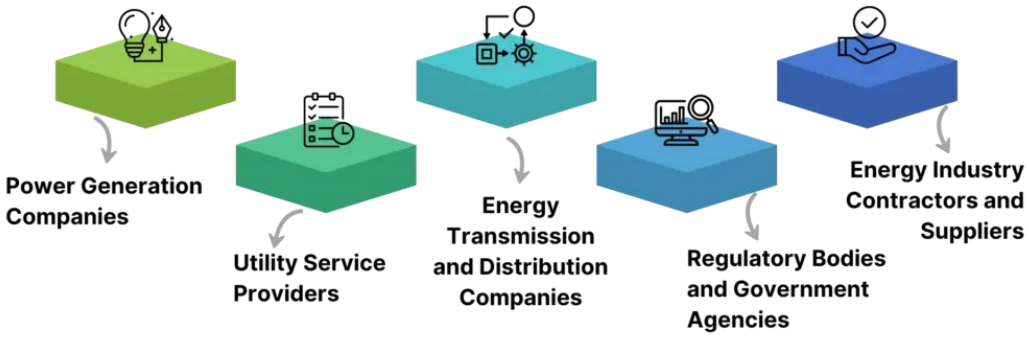

Ilustración 22. Ámbito[47] de aplicación ISO/IEC 27019

Para el gemelo digital, los controles de la ISO/IEC 27019 más relevantes son los relacionados con la gestión de accesos remotos (especialmente relevante para el mantenimiento de la plataforma por proveedores externos), la protección de los canales de comunicación entre OT e IT, la gestión de parámetros de configuración y código fuente de los sistemas de control, y los procedimientos de *backup* y recuperación de sistemas de tiempo real.

2.3.14 REQUISITOS DE ARQUITECTURA SEGURA DEL GEMELO DIGITAL.

La integración de un gemelo digital dentro de la arquitectura de ciberseguridad de la red eléctrica asturiana debe basarse en el modelo de zonas y conductos de la IEC 62443-3-2. El gemelo digital debe ocupar una posición intermedia entre la zona corporativa y la zona de control lo que lo convierte en un punto de entrada para los posibles ataques informáticos sobre la infraestructura en el caso de que no se le asigne una zona de seguridad propia con conductos controlados en ambas fronteras.

[47] Fuente: https://pacificcert.com/iso-iec-27019-certification/

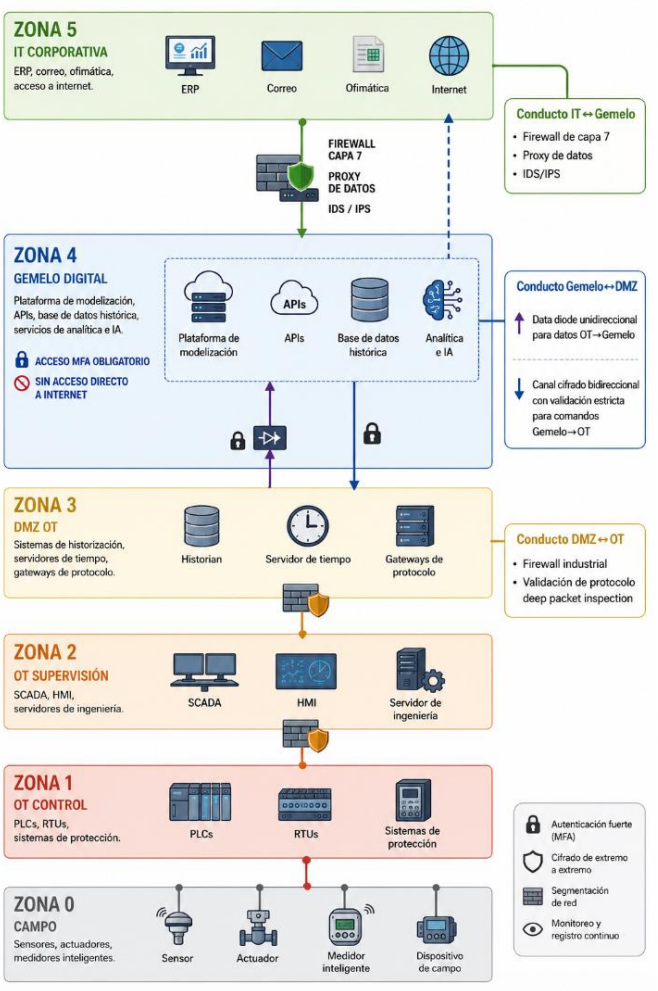

Ilustración 23. Representación[48] de las Zonas de Operación.

El principio fundamental de la división en zonas es que ningún paquete de red debería poder pasar directamente desde la zona de producción a la sección de supervisión sin pasar por zonas de inspección. El gemelo digital, al necesitar datos de ambas zonas es un punto relativamente conflictivo y debe ser diseñado con este principio en mente.

Para que los datos fluyan de manera correcta de la red al gemelo digital la arquitectura más segura es una arquitectura unidireccional mediante diodos de datos, es un concepto similar al dispositivo electrónico. En este caso es un hardware que garantiza físicamente que los datos solamente puedan fluir en una dirección, esto impide que los ataques desde el gemelo hacia los sistemas críticos pasen por ese canal.

La problemática de esta aplicación es que el gemelo digital debe enviar parámetros y ajustes de vuelta a los sistemas de supervisión y control, lo que deriva en que en algunos casos la bidireccionalidad de la comunicación sea un requerimiento indispensable, obligando a que los procesos sean controlados con métodos mucho más estrictos como las firmas digitales, límites

[48] Fuente: Centro de Ciberseguridad Industrial (CCI).

estrictos en los valores que pueden enviar los comandos y la inclusión de supervisión humana obligatoria para los comandos que tengan un impacto significativo.

La gestión de identidades del gemelo digital debe implantarse como un sistema independiente del directorio corporativo, pero con la capacidad de interactuar con él. Esto permite que se puedan aplicar políticas de control de acceso más estrictas para el gemelo sin afectar a las capacidades operativas en general del sistema.

El acceso privilegiado debe gestionarse mediante una solución PAM (*Privileged Access Management*) que registre todas las sesiones, requiera justificación documentada de cada acceso privilegiado, y soporte la revisión periódica de los privilegios concedidos. Para los accesos de proveedores externos, el PAM debe permitir la creación de sesiones de tiempo limitado que expiran automáticamente al finalizar la ventana de mantenimiento, eliminando el riesgo de credenciales persistentes de proveedores.

2.3.15 IMPACTO ECONÓMICO DEL CUMPLIMIENTO DE LA CIBERSEGURIDAD EN ASTURIAS.

El cumplimiento del marco normativo de ciberseguridad descrito implica inversiones en varias categorías, cuya magnitud depende críticamente del alcance del despliegue. Conviene precisar la metodología de estimación: como referencia de coste por entidad individual, el análisis de impacto de la transposición de la Directiva NIS2 calcula que una entidad esencial que deba implementar el conjunto de medidas exigidas por la norma desde cero puede requerir una inversión de hasta 2,15 millones de euros[49]. Dado que un despliegue del gemelo digital a escala de toda la red eléctrica asturiana implicaría integrar múltiples subestaciones, centros de control y activos de generación bajo una misma arquitectura de seguridad —y no una sola instalación—, la inversión total para el conjunto de la región debe escalarse en consecuencia. Tomando como base esa referencia y extrapolándola al número de instalaciones críticas que conformarían el gemelo digital regional, la inversión en infraestructura técnica (arquitectura de zonas y conductos, firewalls industriales, diodos de datos, sistemas IDS/IPS OT, plataforma PAM y sistema SIEM) puede estimarse en un rango de 3 € a 8 millones de €, en función del número final de instalaciones integradas y del nivel de madurez previo de cada una de ellas. Esta cifra debe entenderse como una aproximación orientativa construida por extrapolación, con un alcance limitado a infraestructuras esenciales, y no como el resultado de un estudio de ingeniería específico sobre el despliegue asturiano.

A esta inversión técnica se sumarían los costes de procesos y organización: la elaboración y mantenimiento del sistema de gestión de seguridad y la política de gestión de riesgos (horas de consultoría especializada y revisiones periódicas), la formación de los operarios, y la suscripción a servicios de inteligencia de amenazas orientados específicamente al sector energético.

Las auditorías y certificaciones constituyen otro componente significativo. Dado que un despliegue regional implicaría certificar múltiples instalaciones o, alternativamente, un sistema de gestión único con alcance ampliado, la auditoría de certificación ISO 27001/27019 y la eventual certificación ENS pueden representar entre 150.000 € y 400.000 € para la certificación

[49] Fuente: https://www.tarlogic.com/es/blog/coste-ley-de-ciberseguridad-empresas/

inicial a escala regional, más los costes de las auditorías anuales de mantenimiento. Los test de penetración anuales contra el gemelo digital, incluyendo los ejercicios de *red team* OT distribuidos entre las distintas instalaciones, tendrían un coste estimado de entre 100.000 € y 300.000 € anuales, dependiendo del alcance y del número de entornos a evaluar.

En conjunto, los costes recurrentes anuales de cumplimiento de ciberseguridad para un gemelo digital de la red eléctrica a escala de toda Asturias pueden estimarse en un rango de 1,2 a 2,8 millones de € anuales, una vez superada la inversión inicial. Esta cifra debe contemplarse en el plan de negocio del proyecto desde el primer día, y conviene subrayar que ambos rangos —el de inversión inicial y el de coste recurrente— son estimaciones orientativas sobre una infraestructura básica de la red regional.

Esta inversión debe valorarse frente al coste de no realizarla. El régimen sancionador que contempla la normativa NIS2 alcanza, por sí solo, hasta 10 millones de euros o el 2% del volumen de negocio anual para las entidades esenciales una cifra superior a la inversión necesaria para el cumplimiento de la ley. Aunque aparentemente alta, esta cifra se basa en el impacto financiero que puede tener una interrupción del servicio derivada de un ciberataque (inactividad, pérdida de datos, secuestro de información), que puede superar por término medio los 15 millones de € y demuestra la rentabilidad de inversión en ciberseguridad.

Por último, la certificación de la plataforma del gemelo digital bajo el Esquema Europeo de Certificación de Ciberseguridad permitirá crear una confianza que facilitará la aceptación por parte del CNPIC y de INCIBE de las medidas de seguridad adoptadas. Los proveedores de plataformas en la nube que obtengan la certificación EUCS estarán en posición preferente para los contratos con operadores de infraestructuras críticas europeas, lo que supone una oportunidad para empresas del ecosistema tecnológico asturiano si desarrollan estas capacidades.

2.3.16 IMPACTO SOCIAL Y AMBIENTAL DE LA CIBERSEGURIDAD.

La inversión en ciberseguridad dentro del gemelo digital tiene un impacto positivo directo que se traduce en la reducción del riesgo de interrupciones del suministro eléctrico causadas por ciberataques. Para Asturias, una región con zonas rurales extensas y condiciones meteorológicas que ya generan vulnerabilidad natural en la red, la adición del riesgo cibernético sin las contramedidas adecuadas podría representar un incremento de riesgos poco justificable.

La generación de empleo cualificado en ciberseguridad es el otro impacto social relevante, sobre todo en el campo de los requisitos del área formativa, según INCIBE, la diferencia entre la oferta y la demanda de perfiles de ciberseguridad supera los 24.000 puestos anuales. Asturias presenta condiciones adecuadas para desarrollar iniciativas en formación y empleo en ciberseguridad industrial que atienda no solo al sector eléctrico sino también a la siderúrgica, la química y la logística portuaria.

La transparencia del marco de ciberseguridad, con la publicación de informes de cumplimiento y la participación ciudadana en la gobernanza de la red inteligente, es un factor de confianza pública. Los ciudadanos asturianos que ven cómo sus datos de consumo son gestionados por un

gemelo digital tienen derecho a conocer qué medidas de seguridad protegen esos datos. Los informes anuales de transparencia sobre incidentes de ciberseguridad contribuyen a esta construcción de confianza.

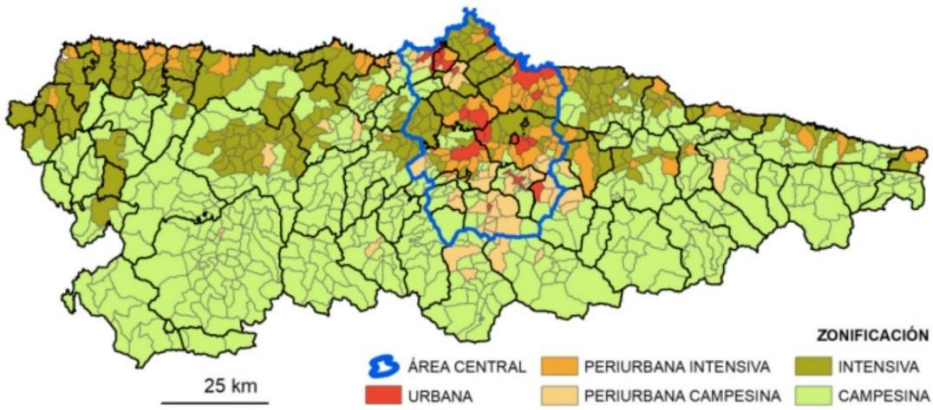

Ilustración 24. Distribución de población en el Principado de Asturias[50]

Se puede establecer un nexo entre la ciberseguridad y los objetivos medioambientales. Aunque de una forma menos evidente, una red eléctrica ciber resiliente que pueda integrar un gemelo digital tiene la capacidad de evitar los accidentes y desastres ambientales asociados a los ciberataques. Los ataques cibernéticos pueden generar daños físicos, en algunos casos llegando a producirse vertidos, inundaciones, incendios o liberaciones de gases.

Finalmente, la reducción de la huella de carbono de los propios sistemas de ciberseguridad es un aspecto emergente de sostenibilidad. Los sistemas SIEM[51], las plataformas de análisis de amenazas y los entornos de simulación para el análisis de malware[52] consumen energía significativa. La elección de proveedores de estos servicios con compromisos verificables de neutralidad de carbono y alimentación con energía renovable es una consideración de sostenibilidad que debe incorporarse en los criterios de contratación, en línea con las guías de Compra Pública Verde de la Comisión Europea.

2.4 MARCO LEGISLATIVO SOBRE EL DATO.

La implantación de gemelos digitales en redes eléctricas inteligentes implica la recogida, transmisión, almacenamiento y análisis continuo de enormes volúmenes de datos procedentes de sensores, contadores inteligentes, sistemas SCADA y plataformas de control distribuido. Cuando los datos permiten identificar de forma directa o indirecta a personas físicas como en el

[50] READER: Red Asturiana De Desarrollo Rural
[51] Security Information and Event Management, es un sistema de ciberseguridad centralizada que analiza los sistemas de la empresa en tiempo real y responde a amenazas en tiempo real.
[52] Programa diseñado bien para infiltrarse y tomar el control de un sistema o dañar los mismos sin el consentimiento del usuario.

caso de las lecturas granulares del consumo eléctrico, entran bajo la protección del derecho fundamental a la intimidad y a la protección de datos personales, reconocido en el artículo 18 de la Constitución Española y en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Dentro de la dimensión regulatoria del dato en el contexto de los gemelos digitales, esta va más allá de la protección individual. La interoperabilidad entre operadores, el intercambio de datos entre empresas del sector energético y la apertura de datos operativos a terceros son imperativos del mercado interior europeo que deben coexistir con los derechos de privacidad de los usuarios. Además, el almacenamiento masivo de datos operativos de infraestructuras críticas introduce riesgos de seguridad, cuya gestión está regulada por un cuerpo normativo específico y en rápida evolución.

2.4.1 TRATAMIENTO DE DATOS DE USUARIOS DE LA RED.

El concepto de datos del usuario en el contexto de las redes inteligentes engloba tres grandes categorías con distintos niveles de sensibilidad y aplicabilidad del Reglamento General de Protección de Datos.

La primera categoría considerada son los datos generados, es decir, los datos de medida de consumo. En el caso de los contadores inteligentes obligatorios en España desde 2018 se registra el consumo eléctrico con granularidad horaria. Cuando esos datos se asocian a una dirección postal o a un CUPS (Código Universal del Punto de Suministro), son datos personales en el sentido del artículo 4.1 del RGPD, pues permiten identificar al titular del contrato.

La segunda categoría comprende los datos de producción y autoconsumo de los prosumidores. Con la irrupción de las comunidades energéticas, un número creciente de ciudadanos y empresas pasan a ser al mismo tiempo productores y consumidores de electricidad. Los datos de su producción, volcados al gemelo digital para optimizar la gestión de la microrred, revelan información sobre patrones de actividad económica y hábitos que van más allá del simple consumo.

La tercera categoría son los datos inferenciales: el gemelo digital, mediante modelos de IA y aprendizaje automático, puede derivar de los datos de medida información que el usuario nunca proporcionó directamente (si hay personas en casa, qué electrodomésticos usa, si alguien está trabajando en turno de noche o recibiendo tratamiento médico doméstico). Esta capacidad inferencial es potencialmente sensible y su tratamiento puede quedar sujeto a las disposiciones reforzadas del artículo 9 del RGPD si los datos inferidos caen en las categorías especiales (datos de salud, vida privada).

2.4.2 BASES JURÍDICAS DEL TRATAMIENTO.

El RGPD exige que todo tratamiento de datos personales tenga una base jurídica explícita del artículo 6:

- Obligación legal (art. 6.1.c): la distribuidora está obligada por la Ley 24/2013 del Sector Eléctrico y por la Directiva 2019/944/UE a gestionar la red, garantizar la calidad del suministro y ejecutar la planificación de la red. El tratamiento de datos de medida necesario para cumplir estas obligaciones queda amparado sin necesidad de consentimiento del usuario.
- Interés legítimo (art. 6.1.f): para usos no directamente exigidos por ley —como la optimización del mantenimiento predictivo o la elaboración de modelos de demanda— la distribuidora puede apoyarse en el interés legítimo, siempre que supere el test de ponderación y no prevalezcan los intereses o derechos fundamentales del interesado.
- Ejecución de contrato (art. 6.1.b): para los servicios de valor añadido que la distribuidora ofrezca al usuario sobre la base de sus datos de consumo (informes de eficiencia, comparativas, etc.).
- Consentimiento (art. 6.1.a): para cualquier uso del dato que no esté cubierto por las bases anteriores, especialmente para compartir datos con terceros con fines comerciales o para el tratamiento de datos inferenciales que puedan ser sensibles.

Los artículos 5.1.b y 5.1.c establecen el principio de minimización y limitación de finalidad. El gemelo digital debe tratar únicamente los datos necesarios para cada finalidad operativa. No es admisible recoger los datos de consumo con granularidad cuarto horaria si la finalidad es obtenible con una recogida horaria de los datos. La arquitectura del gemelo debe de estar orientada a no recoger más datos de los necesarios.

2.4.3 EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS.

El artículo 35 del RGPD impone la realización previa de una Evaluación de Impacto relativa a la Protección de Datos cuando el tratamiento de los mismos implica el uso de nuevas tecnologías, el tratamiento a gran escala de datos personales o la elaboración de perfiles. El gemelo digital de una red eléctrica cumple los tres criterios simultáneamente. La AEPD ha publicado una Lista de tipos de tratamientos que requieren EIPD[53] (2019, actualizada en 2022) en la que se incluyen expresamente los sistemas de monitorización de consumo energético a gran escala.

La EIPD debe realizarse antes del inicio y revisarse cuando cambian las circunstancias del riesgo. En el caso asturiano, deberá incluir la evaluación de la necesidad y proporcionalidad del tratamiento, el análisis de riesgos para los derechos de los usuarios y las medidas previstas para mitigarlos.

2.4.4 DERECHOS DE LOS USUARIOS.

Los usuarios de la red cuyos datos son procesados por el gemelo digital son titulares de todos los derechos reconocidos en los artículos del 15 a 22 del RGPD: acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición. El ejercicio de estos derechos en el contexto del gemelo digital plantea desafíos prácticos relevantes: la supresión de datos históricos puede degradar la calidad de los modelos predictivos; la portabilidad de datos de consumo a otro

[53] Evaluación de Impacto en la Protección de Datos

proveedor de servicios puede entrar en conflicto con las obligaciones de confidencialidad de la distribuidora. Esta debe contar con procedimientos documentados para atender estos derechos en los plazos legales (un mes, prorrogable a tres).

El *Data Act* (Reglamento UE 2023/2854), en vigor desde septiembre de 2025, refuerza y extiende el derecho de acceso al dato generado por dispositivos conectados. En la práctica, el usuario de un contador inteligente tiene derecho a obtener sus datos de consumo en tiempo real en un formato fácilmente legible, sin obstáculos técnicos o contractuales impuestos por la distribuidora o por el fabricante del contador.

2.4.5 INTERCAMBIABILIDAD E INTERCAMBIO DE DATOS ENTRE EMPRESAS.

El funcionamiento óptimo del gemelo digital de una red inteligente no es posible de forma aislada. Requiere de flujos de datos entre distintas entidades: el operador del sistema de transporte, los operadores de las redes de distribución, las comercializadoras, las comunidades de energía, los gestores de cargas flexibles y eventualmente terceros proveedores de servicios de datos.

2.4.6 DIRECTIVA 2019/944/UE Y MODELO DE ACCESO A DATOS.

La Directiva del Mercado Interior de la Electricidad (DMIUE) establece en su artículo 23 el marco de acceso a los datos de medida. Impone a los Estados miembros la obligación de crear un modelo de gestión de datos que garantice el acceso no discriminatorio de todos los participantes del mercado a los datos necesarios para su actividad. España ha implementado este modelo a través del Sistema de Información del Mercado Eléctrico (SIME) gestionado por Red Eléctrica y de las plataformas de acceso a datos de las distribuidoras. El gemelo digital debe integrarse con estas plataformas y respetar las reglas de acceso establecidas.

La Directiva distingue entre tres modelos de gestión de datos: el modelo centralizado (un único hub de datos), el modelo descentralizado (cada distribuidora gestiona sus propios datos y ofrece acceso normalizado) y el modelo híbrido. España ha optado por un modelo descentralizado con estándares comunes definidos por la CNMC. El gemelo digital deberá ser capaz de interoperar con este modelo, lo que exige la adopción del *Common Information Model* (IEC CIM 61968/61970) como estándar de representación del dato.

2.4.7 EL DATA ACT (REGLAMENTO UE 2023/2854) Y LOS DATOS B2B.

El *Data Act* regula el acceso y la reutilización de los datos generados por dispositivos conectados, incluyendo los contadores inteligentes y los sensores de la red eléctrica. Sus disposiciones más relevantes para el intercambio de datos entre empresas son el artículo 5 (acceso a datos por terceros a petición del usuario) y los artículos 8 a 12 (obligaciones de acceso B2B).

En el contexto asturiano, una CE podría exigir que los datos de sus contadores inteligentes sean compartidos directamente con una plataforma de gestión energética de terceros para alimentar su propio gemelo digital de microrred, sin que la distribuidora pueda obstaculizarlo.

Ilustración 25.Imagen promocional del Data Act de la UE

Los artículos 8 a 12 imponen a los titulares de datos (como las distribuidoras) la obligación de poner datos a disposición de las empresas que los necesitan para prestar servicios relacionados, en condiciones justas, razonables y no discriminatorias (principio FRAND). Esta obligación tiene límites: no alcanza a los secretos comerciales, no obliga a compartir datos que pongan en riesgo la seguridad de la infraestructura, y establece mecanismos de resolución de disputas para los casos en que el acceso sea denegado o las condiciones resulten desproporcionadas.

2.4.8 EL DATA GOBERNANCE ACT (REGLAMENTO UE 2022/868) Y EL ESPACIO EUROPEO DE DATOS ENERGÉTICOS.

El *Data Governance Act* (DGA) crea el marco institucional para los intermediarios de datos y el altruismo en lo referente a la cesión de datos, y es la base jurídica sobre la que se construye el Espacio Europeo de Datos Energéticos (EEDES), promovido por ENTSO-E y la DSO Entity. El EEDES será la infraestructura de intercambio de datos de referencia para los operadores de red de toda la UE, y cualquier gemelo digital de una red eléctrica europea deberá integrarse con él cuando esté operativo (previsto para 2026–2027).

Para los operadores y empresas asturianas del sector energético, esto implica dos obligaciones: la adopción de estándares técnicos de interoperabilidad compatibles con el EEDES, y la participación en los mecanismos de gobernanza del espacio de datos para defender sus intereses en la definición de las reglas de acceso.

2.4.9 LÍMITES AL INTERCAMBIO: SECRETO INDUSTRIAL Y SEGURIDAD.

La posibilidad de intercambio de datos no es ilimitada. El artículo 19 del *Data Act* y el artículo 39 del RGPD establecen que los datos cuya divulgación pondría en riesgo secretos industriales o la seguridad de infraestructuras críticas pueden ser protegidos frente a solicitudes de acceso. Para el gemelo digital de una red eléctrica, los datos de la arquitectura de la red, las vulnerabilidades detectadas y los parámetros de configuración de los sistemas de control quedan bajo esta protección, que debe ser invocada de forma motivada y proporcional, sin poder utilizarse como pretexto para bloquear el acceso legítimo a datos de consumo de usuarios.

El *Data Act* obliga a compartir datos, el RGPD y la normativa de infraestructuras críticas limitan ese intercambio. La resolución de este conflicto requiere un diseño de la arquitectura de datos

que permita compartir datos anonimizados o agregados sin exponer información personal o sensible desde el punto de vista de la seguridad.

2.4.10 PROTECCIÓN Y ALMACENAMIENTO DE DATOS.

Principio de la Privacidad por Diseño:

El artículo 25 del RGPD (correlación técnica en las normas ISO/IEC 27001 e ISO/IEC 29101) impone el principio de protección de datos desde el diseño y por defecto. Aplicado al gemelo digital, este principio exige que las decisiones de arquitectura técnica (elección de plataforma cloud, modelo de datos, flujos de integración) incorporen salvaguardas de privacidad desde la concepción del sistema y no como capa añadida a posteriori. La AEPD[54] ha publicado guías prácticas sobre la aplicación de *privacy by design*[55] que son de referencia obligada para los equipos técnicos.

Ilustración 26. Siete Principios de la Privacidad por Diseño[56]

En la práctica, esto se traduce en exigencias concretas: como anonimizar los datos de medida de consumo domiciliario tan pronto como sea posible en el flujo de datos, separación entre los datos operativos necesarios para la gestión de la red (que no requieren identificar al usuario) y los datos de facturación (que sí lo requieren), cifrado en tránsito y en reposo de todos los datos que puedan identificar a personas físicas; y controles de acceso basados en roles con el principio de mínimo privilegio.

Requisitos de Almacenamiento:

El artículo 5.1.e del RGPD prohíbe mantener los datos en una forma que permita la identificación del interesado durante más tiempo del necesario para los fines del tratamiento (principio de limitación del plazo de conservación). Para los datos de medida del gemelo digital, la definición del plazo adecuado requiere un ejercicio de ponderación entre la utilidad de los datos históricos para mejorar los modelos predictivos y el derecho del usuario a no ser permanentemente perfilado. La práctica regulatoria consolidada en la UE fija plazos de retención de datos de consumo individualizado entre 13 y 36 meses para fines operativos, con posibilidad de

[54] Agencia Española de Protección de Datos.
[55] Es un enfoque que considera incorporar la protección de datos personales desde la fase inicial de creación del sistema en lugar de añadirlo a posteriori.
[56] Fuente: PECB (Professional Evaluation and Certification Board).

conservación indefinida en formato anonimizado o agregado para fines de planificación o investigación.

Si el gemelo digital se despliega sobre infraestructura pública en la nune, con centros de datos fuera del Espacio Económico Europeo (EEE) (situación habitual con las grandes plataformas americanas), las transferencias internacionales de datos personales deben ajustarse al Capítulo V del RGPD. Las alternativas jurídicas disponibles son: la Decisión de Adecuación de la Comisión Europea (actualmente vigente para EE.UU. bajo el Marco de Privacidad de Datos UE—EE.UU. de julio de 2023, aunque en situación de incertidumbre jurídica); las Cláusulas Contractuales Tipo (CCT) adoptadas por la Comisión en 2021; o las normas corporativas vinculantes (BCR) para grupos de empresas multinacionales.

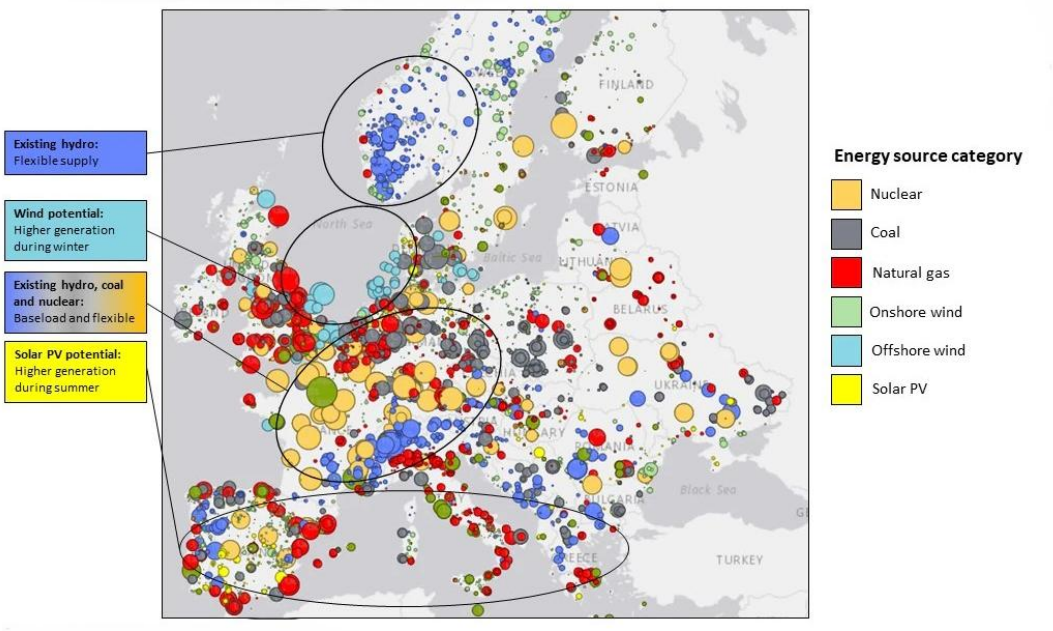

Ilustración 27.Fuentes Energéticas del Espacio Económico Europeo[57]

Para instalaciones de la red eléctrica asturiana que procesen datos de infraestructuras críticas, la tendencia regulatoria europea apunta claramente hacia la soberanía digital: almacenamiento y procesamiento dentro de la UE, preferiblemente bajo certificación EUCS (European Union Cloud Security Scheme) o equivalente nacional. La contratación de plataformas cloud americanas o asiáticas para este tipo de datos puede ser cuestionada por la AEPD o por el CNPIC en el contexto de la normativa de infraestructuras críticas.

El artículo 32 del RGPD exige medidas técnicas y organizativas adecuadas al riesgo para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. Para el gemelo digital de una red eléctrica, estas medidas deben ser especialmente robustas dada la naturaleza de infraestructura crítica del sistema. Las normas de referencia son: ISO/IEC 27001 (gestión de la seguridad de la información), ISO/IEC 27019 (sector energético), IEC 62443

[57] El Periódico de la Energía

(sistemas de automatización industrial) y el Esquema Nacional de Seguridad (ENS, RD 311/2022) para los sistemas con participación pública.

La obligación de notificar violaciones de seguridad que afecten a datos personales —en 72 horas a la AEPD y, si el riesgo es elevado, sin demora a los interesados (arts. 33 y 34 RGPD)— requiere que el operador cuente con un plan de respuesta a incidentes integrado con el procedimiento de notificación al INCIBE-CERT exigido por NIS2.

2.4.11 IMPACTO ECONÓMICO DE LA REGULACIÓN.

El cumplimiento del RGPD, el *Data Act*, el *AI Act* y las normas de ciberseguridad (NIS2, ENS) exige inversiones sustanciales en cuatro áreas: la arquitectura tecnológica del gemelo digital (cifrado, controles de acceso), los procesos organizativos (DPD[58], políticas de retención, procedimientos de ejercicio de derechos), la auditoria/certificación (ISO 27001, ENS, conformidad RGPD) y la formación continua del personal.

Para los operadores de distribución eléctrica presentes en Asturias, estos costes no son nuevos en su totalidad: la obligación de desplegar contadores inteligentes y gestionar sus datos ya había generado estructuras de cumplimiento. Sin embargo, la complejidad añadida del gemelo digital y la aceleración legislativa europea de los últimos tres años (Data Act, AI Act, NIS2 y CRA[59] en vigor casi simultáneamente) supone una presión sobre los recursos jurídicos y técnicos de las empresas de menor tamaño (como instaladores o fabricantes de equipos), que dificultan gestionar sin apoyo externo.

Se estima que los costes de cumplimiento normativo en proyectos de digitalización de redes en Europa representan entre el 8% y el 15% del coste total del proyecto, dependiendo del nivel de madurez previa de la organización. Para un proyecto de gemelo digital de la red de distribución de Asturias con un coste estimado de 15–25 millones de euros, los costes de cumplimiento podrían situarse entre 1,2 y 3,75 millones de euros, una magnitud significativa que justifica la inclusión explícita de estos costes en el plan de negocio del proyecto.

La apertura regulatoria de los datos de red, combinada con las obligaciones de interoperabilidad, tiende a reducir las barreras de entrada para nuevos competidores en el mercado eléctrico. Las comercializadoras independientes y los agregadores de demanda podrán acceder a datos más precisos y en tiempo más real para diseñar ofertas de valor añadido para los consumidores. Esto puede traducirse en una mayor competencia en el mercado minorista, con el consiguiente efecto moderador sobre los precios y la mejora de la calidad del servicio. Sin embargo, este escenario requiere que los marcos de acceso sean efectivamente aplicados y supervisados. La CNMC, como regulador sectorial competente en España, deberá desempeñar un papel activo de vigilancia, papel que en el ámbito autonómico puede ser complementado por el organismo regulador del Principado.

[58] Delegado de Protección de Datos, es el encargado de encargarse de cumplir con la normativa de privacidad y tratamiento de datos personales.
[59] Ley de Ciberresiliencia.

2.4.12 IMPACTO SOCIAL DE LA REGULACIÓN.

El marco regulatorio analizado reconoce al ciudadano asturiano no solo como destinatario del servicio eléctrico, sino como titular de derechos activos sobre sus propios datos. El RGPD le da acceso a sus datos de consumo, el derecho a oponerse al perfilado y la posibilidad de exigir la supresión de datos históricos. El Data Act le permite redirigir sus datos a plataformas de su elección. La DMIUE le garantiza información no discriminatoria sobre su consumo.

En la práctica, el ejercicio efectivo de estos derechos requiere que el ciudadano esté informado de su existencia y que cuente con mecanismos sencillos para ejercerlos. Este es un reto significativo en una región donde la brecha digital sigue siendo relevante: según los datos del INE, el 22% de los asturianos mayores de 65 años no utiliza internet, una proporción superior a la media nacional. La implementación del gemelo digital debe incluir obligatoriamente mecanismos de información y ejercicio de derechos accesibles para usuarios no digitalizados, líneas telefónicas, atención presencial, intermediación a través de servicios sociales.

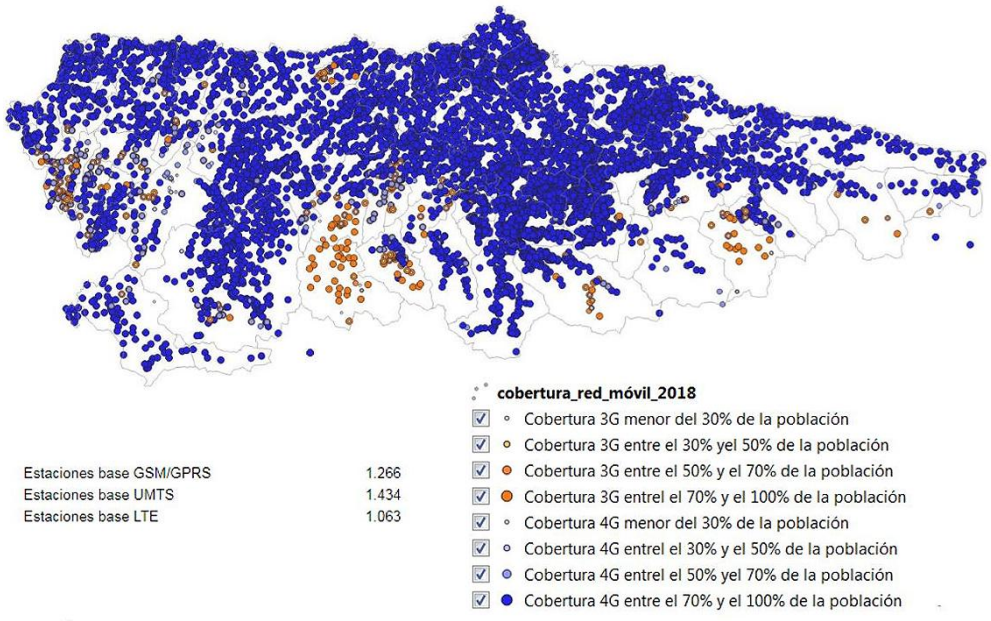

Ilustración 28. Cobertura de la red de internet asturiana[60]

La implementación del marco regulatorio de datos en el sector energético asturiano genera demanda de perfiles profesionales escasos: abogados especializados en RGPD y datos, ingenieros de seguridad con conocimiento del sector OT, delegados de protección de datos con experiencia en infraestructuras críticas y analistas de datos con dominio de las especificidades del sector eléctrico.

La normativa también impone obligaciones de formación continua al personal que trata datos personales (art. 29 RGPD y art. 32.4), lo que genera un mercado de formación corporativa que puede ser cubierto por proveedores de la región. En conjunto, el impacto neto sobre el empleo

[60] Fuente: Consejería de Ciencia, Innovación y Universidad del Gobierno del Principado de Asturias.

cualificado es positivo, aunque requiere políticas activas de reconversión laboral para los trabajadores del sector energético tradicional que deben adquirir nuevas competencias digitales.

2.4.13 IMPACTO AMBIENTAL DE LA REGULACIÓN.

El marco regulatorio del dato energético tiene una dimensión ambiental. El acceso y la apertura a los datos operativos de la red garantizada por el *Data Act* y la *DMIUE*, son condiciones necesarias para el funcionamiento de los mercados de flexibilidad. Esto permitirá integrar más energía renovable intermitente en el sistema. Sin esos datos o el acceso a los mismos, en tiempo real, los agregadores de flexibilidad no podrán cumplir con su función, ni será posible diseñar ofertas de respuesta de la demanda que desplacen el uso de generación fósil de respaldo.

En el contexto asturiano, donde la calidad del suministro eléctrico depende de importaciones eléctrica de otras regiones y de la operación de centrales de gas natural como respaldo ante la intermitencia de las renovables, la mejora de la gestión de la flexibilidad habilitada por el gemelo digital y por los datos abiertos puede tener un impacto ambiental medible en términos de toneladas de CO_2 evitadas. Los modelos del operador del sistema (REE) estiman que cada 1% de mejora en la integración de renovables equivale a una reducción de emisiones del sector eléctrico de entre 400.000 y 600.000 toneladas de CO_2 anuales a nivel nacional.

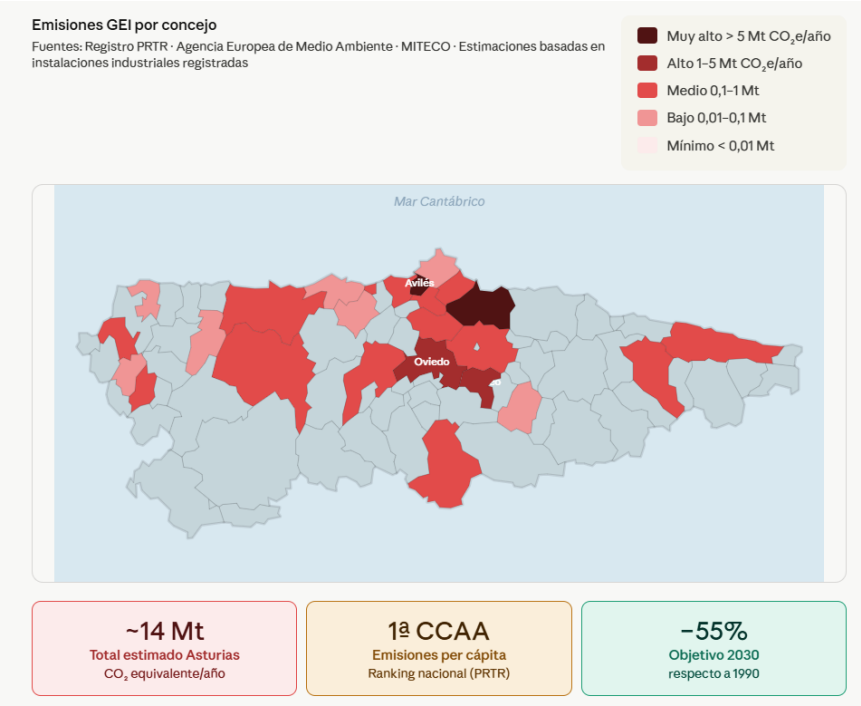

Ilustración 29. Emisiones[61] por concejos de Asturias

La aplicación de la regulación de datos tiene también una huella ambiental propia que no debe ignorarse. Los centros de datos necesarios para alojar el gemelo digital y sus sistemas de gestión consumen energía y agua. Las obligaciones de cifrado, auditoría y registro de accesos generan

[61] Fuente: Observatorio de la Sostenibilidad en España.

carga computacional adicional. La replicación de datos exigida por los planes de continuidad de negocio duplica el almacenamiento.

El Reglamento (UE) 2023/1791 de Eficiencia Energética impone a los centros de datos de más de 500 kW de potencia tienen la obligación de publicar indicadores de eficiencia (PUE, WUE) y de someterse a auditorías energéticas. Para los proyectos de gemelo digital asturianos que requieran infraestructura de cómputo significativa, la elección de un proveedor de servicios en la nube con centros de datos alimentados por energía renovable certificada no es solo una decisión de imagen corporativa, sino una forma de alinearse con los objetivos de descarbonización del Principado.

La actualización tecnológica periódica que impone el ciclo de vida de los componentes del gemelo digital (sensores, equipos de borde, servidores) genera residuos de aparatos eléctricos y electrónicos (RAEE). La normativa española de transposición de la Directiva RAEE (RD 110/2015) obliga a los productores y gestores de estos equipos a sistemas de recogida y reciclado. Para el proyecto asturiano, la incorporación de criterios de ecodiseño, durabilidad y mantenibilidad en los contratos de suministro de componentes del gemelo digital es una buena práctica que las guías de compra pública verde de la Comisión Europea recomiendan expresamente.

3. IA EN REDES ELÉCTRICAS INTELIGENTES.

3.1 ECOSISTEMA DE IA PARA REDES INTELIGENTES.

El ecosistema tecnológico que relaciona la IA a las Smart grids se ha desarrollado a lo largo de más de siete décadas, desde los primeros sistemas expertos basados en reglas de la década de 1970 hasta los actuales Gemelos Digitales Agénticos[62]. Esta evolución puede estructurarse en tres grandes tendencias tecnológicas superpuestas y complementarias:

- ***Primera (1970-2000):*** Sistemas expertos, lógica difusa y algoritmos genéticos. Aplicaciones principalmente en gestión de fallos, despacho económico y planificación de la expansión de la red.
- ***Segunda (2000-2018):*** *Machine Learning* clásico y *Deep Learning* incipiente. Predicción de carga, detección de anomalías, estimación de estado y diagnóstico de fallos con redes neuronales artificiales, SVM y algoritmos de conjunto.
- ***Tercera (2018-presente):*** *Deep Learning* avanzado, *Reinforcement Learning*, *Federated Learning* y Modelos de Lenguaje de Gran Escala. Gestión autónoma en tiempo real, optimización multivariante, preservación de la privacidad y razonamiento contextual en lenguaje natural.

[62] Se entiende al gemelo digital agéntico como un gemelo digital que integra una IA en su estructura; a diferencia del gemelo digital tradicional esta versión puede razonar, tomar decisiones y establecer planes de acción y ejecutarlos de forma autónoma.

Esta arquitectura tecnológica en capas se apoya en una infraestructura habilitadora que incluye el Internet de las Cosas Industrial (IIoT), las redes de comunicación 5G, los sistemas de computación en la frontera (*edge computing*) y las plataformas híbridas en la nube. Para Asturias, donde la heterogeneidad de activos energéticos es especialmente acusada —desde centrales hidráulicas de décadas de antigüedad hasta instalaciones fotovoltaicas de última generación—, la capacidad de estas tecnologías de integrarse es un factor crítico de su viabilidad real.

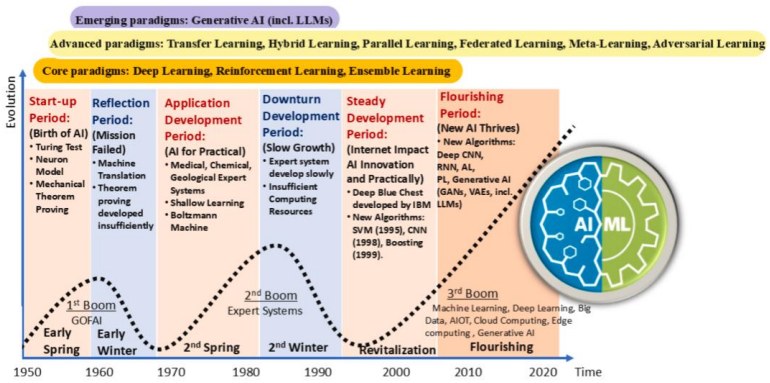

Ilustración 30. Evolución Histórica[63] de la IA y el Machine Learning.

3.2 MACHINE LEARNING.

El aprendizaje autónomo es el conjunto de técnicas que permiten a los sistemas mejorar su rendimiento mediante la experiencia; en el caso de las redes inteligentes se consideran tres tipos de aprendizaje:

- El aprendizaje supervisado opera con conjuntos de datos etiquetados donde el modelo aprende la correspondencia entre entradas y salidas. En la *smart grid*, esto se traduce en predicción de demanda eléctrica, detección de fraude en el consumo, clasificación de ciberataques y predicción de precios en el mercado mayorista. Los indicadores de rendimiento utilizados son MAPE (*Mean Absolute Percentage Error*) para predicción y para clasificación de anomalías o gestión de la demanda, que constituyen los KPIs directamente vinculados a objetivos operativos de la red.
- El aprendizaje no supervisado descubre patrones ocultos en datos sin etiquetar. En las redes eléctricas, técnicas como la *clusterización K-Means*[64] o los *autoencoders*[65] permiten la segmentación de consumidores por perfiles de carga, la detección de anomalías sin conocimiento previo de cómo se manifiestan, y la estimación de la topología de la red a partir de datos de medida. Para la red de distribución asturiana, donde la variabilidad topográfica genera perfiles de consumo muy heterogéneos entre

[63] Fuente: https://www.researchgate.net/

[64] Es un algoritmo basado en agrupar datos similares en diferentes grupos sin que nadie le diga al algoritmo las categorías.

[65] Es una red neuronal que aprende a representar los datos de forma más compacta sin perder demasiada información.

áreas industriales de interior y de costa y zonas rurales de montaña, esta capacidad de segmentación automática tiene un valor operativo considerable.

- El aprendizaje semi-supervisado aprovecha grandes volúmenes de datos sin etiquetar, junto a pequeños conjuntos etiquetados, lo que resulta especialmente útil en contextos donde el etiquetado es costoso o temporalmente imposible, como la detección de tipos de fallos que ocurren raramente en la red.

En el caso de Asturias, el *Machine Learning* presenta un impacto económico notable, dado que realizar una predicción de la demanda industrial de forma precisa permitiría a los grandes consumidores optimizar sus consumos energéticos y participar en mercados de flexibilidad. Se estima que una reducción de un 3% a 10% podría suponer unos ahorros anuales de entre 200.000€ y 800.000€ por instalación de gran consumo.

Dentro del impacto social, se puede mejorar la detección automática de fraude energético, beneficiando a los consumidores que soportan indirectamente el robo de la electricidad en su tarifa.

Dentro de su impacto ambiental se puede considerar la segmentación de consumidores por perfiles de carga permite diseñar tarifas y señales de precio que desplazan el consumo a horas de alta generación renovable, reduciendo directamente la necesidad de generación térmica de respaldo. Cada MWh desplazado desde ciclo combinado a renovable evita aproximadamente 0,37 toneladas de CO_2 en el mix eléctrico español.

3.3 DEEP LEARNING (DL).

El *Deep Learning* permite a los sistemas de inteligencia artificial aprender directamente de grandes cantidades de datos, identificando por sí mismos patrones y relaciones complejas que pueden resultar difíciles de detectar mediante métodos convencionales. Su capacidad para extraer patrones complejos de datos procedentes de sensores SCADA, contadores inteligentes y PMUs lo convierte en la tecnología dominante para la mayoría de las aplicaciones de predicción y diagnóstico en redes eléctricas modernas.

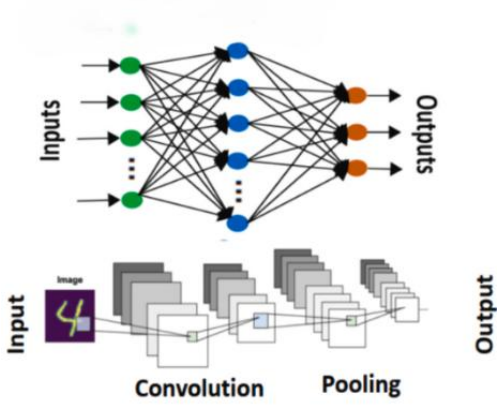

Ilustración 31.Deep Learning[66].

La predicción de la carga eléctrica es la aplicación más madura del *Deep Learning* en redes inteligentes. Los modelos pueden llegar a predicciones con márgenes de incluso 1 día con errores del 3% usando modelos LSTM. Para horizontes de planificación más largos, los Temporal Fusion Transformers (TFT) han demostrado la capacidad de predecir cargas a nivel de ciudad con errores del 1,5%, combinando atención temporal, selección de variables y manejo de covariables externas (temperatura, día de la semana, datos de mercado).

Para la red asturiana, la predicción de generación renovable tiene una dimensión de especial complejidad por tres factores concurrentes: la variabilidad meteorológica del Cantábrico, con cambios rápidos de irradiancia solar y velocidad del viento; la topografía abrupta, que genera microclimas significativamente diferentes entre instalaciones próximas; y la intermitencia que se superpone a la demanda de grandes consumidores industriales cuya operativa (arranque y parada de procesos) introduce variaciones de decenas de MW en la red. Los modelos híbridos CNN-LSTM[67] han demostrado ser especialmente robustos ante estas condiciones, separando las componentes de alta frecuencia (variabilidad meteorológica rápida) de las tendencias de baja frecuencia (patrones estacionales y diurnos).

Una de las aplicaciones de mayor retorno económico del *Deep Learning* en el sector energético es el mantenimiento predictivo. Los sistemas de generación eléctrica convencionales tienen costes de mantenimiento correctivo muy elevados cuando afectan a turbinas, generadores o transformadores de mayor potencia. Para cuantificar mediante un ejemplo el impacto de este tipo de medidas, la parada no planificada de una central de 100 MW durante 48 horas implica, a precios medios del mercado español, costes directos de oportunidad de entre 200.000€ y 400.000€, sin contar con los costes de reparación de urgencia y los impactos sobre la seguridad del suministro regional.

Los modelos de *Deep Learning* para diagnóstico de fallos procesan en paralelo señales de vibración, temperatura, presión, corriente y tensión, para identificar patrones precursores de averías antes de que se manifiesten. La experiencia industrial determina que el tiempo de

[66] Fuente: https://www.researchgate.net/
[67] Arquitecturas de aprendizaje profundo (Deep Learning) que combinan dos tipos de redes neuronales distintas para analizar datos que tienen características espaciales y temporales al mismo tiempo

parada no planificado se reduce un 35% mediante sistemas de gemelo digital basados en DL, con tasas de detección de fallos superiores al 98% en condiciones de laboratorio. La reducción de costes de mantenimiento se sitúa en rangos del 10% al 25% dependiendo del tipo de instalación y la madurez previa del programa de mantenimiento.

El aumento de la generación energética distribuida en la red de distribución asturiana genera perturbaciones de voltaje que los sistemas de control convencionales tienen dificultades para gestionar. Los modelos CNN-LSTM-Attention entrenados sobre datos de contadores inteligentes pueden estimar tensiones nodales y determinar soluciones específicas como (Envolventes Dinámicas de Operación, DOEs), que definen los límites de generación y consumo que cada punto de la red puede soportar en cada momento.

La incorporación de *Explainable AI* (XAI)[68] proporciona a los operadores de la red información interpretable sobre qué factores son los principales determinantes de las condiciones de voltaje en cada momento. Esto transforma la IA de una caja negra en una herramienta de apoyo a la decisión que aumenta la confianza del operador y facilita la validación regulatoria de los sistemas autónomos.

3.3.1 IMPACTO DEL DEEP LEARNING.

En el contexto asturiano el mantenimiento predictivo basado en Deep Learning sobre el parque hidráulico asturiano podría generar unos ahorros estimados de 3-8 millones de euros anuales en costes de mantenimiento; en el caso de la predicción eólica se pueden incrementar los ingresos de los parques asturianos reduciendo los costes de desviación en los mercados de balance.

Ilustración 32. Representación del Deep Learning[69].

Produciéndose un impacto directo sobre la calidad de vida en zonas rurales asturianas donde la orografía complica la red. La reducción del TIEPI (Tiempo de Interrupción Equivalente de

[68] Conjunto de procesos y métodos que permiten a los usuarios humanos comprender y confiar en los resultados y predicciones generados por los algoritmos de aprendizaje automático.
[69] Fuente: https://www.researchgate.net/

Potencia Instalada)[70] beneficia a todos los consumidores y reduce las compensaciones que la regulación obliga a pagar a los distribuidores.

Una integración más eficiente de las fuentes de energía renovables gracias a la predicción avanzada y al control de voltaje permite incrementar la cuota de energía renovable en el mix asturiano sin comprometer la estabilidad. La extensión de la vida útil de turbinas hidráulicas reduce la necesidad de fabricar nuevos equipos pesados, con la consiguiente reducción de emisiones embebidas en el ciclo de vida de los activos.

3.4 REINFORCEMENT LEARNING (RL).

El aprendizaje por refuerzo es el paradigma de IA más alineado con los desafíos operativos de las redes eléctricas inteligentes. A diferencia del aprendizaje supervisado, que requiere ejemplos de comportamiento óptimo previo, el RL aprende a través de la interacción directa con el entorno, recibiendo señales de recompensa o penalización en función de las acciones ejecutadas. Este paradigma es particularmente adecuado para la gestión de redes eléctricas porque el sistema es dinámico y no estacionario; las decisiones óptimas dependen del estado completo del sistema en cada momento, las consecuencias de las decisiones se manifiestan a lo largo del tiempo, y los objetivos son múltiples y en ocasiones en conflicto (coste, calidad de servicio, reservas de seguridad).

Ilustración 33. Reinforced Learning[71]

El RL formula la operación de la red observando el estado del sistema (precios de mercado, niveles de generación, demanda, frecuencia, voltajes), ejecutando acciones (*setpoints* de generación, señales de respuesta de la demanda, ajustes de almacenamiento), recibiendo beneficios del sistema (coste reducido, penalización por violaciones de límites de voltaje o frecuencia) y actualizando su política de actuación para maximizar el beneficio acumulado a largo plazo.

[70] Es el indicador utilizado en España y otros países regulados para medir la continuidad y calidad del suministro eléctrico. Representa el número de horas (o minutos) al año que un corte de luz habría afectado a toda la red si la pérdida de potencia se distribuyera uniformemente entre todas las instalaciones.
[71] Fuente: https://www.researchgate.net/

3.4.1 DEEP REINFORCED LEARNING (DRL) Y APLICACIONES CONCRETAS.

El *Deep Reinforcement Learning* combina la capacidad del *Deep Learning* para analizar grandes cantidades de datos con la capacidad del aprendizaje por refuerzo para aprender a tomar decisiones en situaciones complejas, como la gestión de una red eléctrica con miles de sensores.

Las aplicaciones de DRL más relevantes para la red asturiana son la gestión de la microrred y el despacho óptimo. Agentes DRL entrenados sobre datos históricos y simulaciones de gemelo digital pueden aprender políticas de despacho de generación distribuida que reducen el coste de operación, minimizando apuntamiento y la frecuencia de desviaciones. Estudios documentados muestran reducciones de coste del 15-25% en microrredes con alta penetración renovable respecto a métodos de optimización determinista.

La respuesta dinámica de la demanda industrial es otra aplicación crucial. En el contexto de las industrias electro intensivas asturianas que ya participan en los mercados de ajuste de Red Eléctrica mediante el SRAD[72], agentes DRL[73] pueden automatizar las decisiones de modulación de carga en respuesta a señales de precio en tiempo real, maximizando los ingresos por flexibilidad al tiempo que se respetan las restricciones de proceso productivo. La optimización del flujo de potencia óptimo (OPF)[74] es el problema más computacionalmente intenso de la operación de la red. El DRL puede ayudar a lograr soluciones cercanas al óptimo en tiempos de inferencia de milisegundos, habilitando el OPF en tiempo real que los métodos de optimización convencionales no pueden alcanzar.

3.4.2 MULTI-AGENT REINFORCED LEARNING.

La naturaleza distribuida de la red eléctrica moderna exige enfoques multi-agente donde los diferentes actores aprenden políticas coordinadas. El *Multi-Agent Reinforcement Learning (MARL)* proporciona el marco teórico y práctico para este escenario.

En el contexto asturiano, donde las Comunidades Energéticas (CE) y las instalaciones de autoconsumo crecen en número, están emergiendo como nuevos actores del sistema. El MARL puede habilitar la gestión autónoma y coordinada de los recursos, la negociación automática entre comunidades de energía y el operador de la red de distribución, y la participación coordinada de pequeños consumidores en los mercados de flexibilidad a través de agregadores.

Algunos estudios documentan que el MARL puede reducir los costes de operación de microrredes con múltiples agentes en un 15-25% y mejorar la estabilidad de la frecuencia durante episodios de alta penetración renovable.

[72] Servicio de Respuesta Activa a la Demanda dependiente de REE
[73] Agentes de Deeplearning
[74] Se determina cómo debería distribuirse la generación y el flujo de energía por la red para alcanzar un objetivo —por ejemplo, minimizar pérdidas, costes o congestiones— respetando las restricciones de tensión, corriente y capacidad de los equipos

3.4.3 IMPACTO DEL REINFORCED LEARNING.

Impacto Económico:

La automatización de la respuesta de la demanda mediante DRL puede duplicar o triplicar los ingresos por flexibilidad de las industrias electrointensivas asturianas en los mercados de ajuste (SRAD), al optimizar las ofertas en tiempo real en lugar de hacerlo manualmente. Los precios del SRAD alcanzaron 65 €/MWh en la subasta de noviembre de 2025, lo que ilustra la magnitud del incentivo. La reducción de costes de operación en la gestión de la red de distribución puede suponer ahorros anuales de varios millones de euros en el sistema eléctrico en Asturias.

Impacto Social:

La gestión MARL de comunidades de energía permite a ciudadanos y pequeñas empresas acceder a los beneficios de la flexibilidad energética sin necesidad de invertir en sistemas de gestión costosos. Democratiza el acceso a un recurso económico anteriormente reservado a grandes industrias, reduciendo la brecha entre pequeños y grandes consumidores.

Impacto Ecológico:

La optimización en tiempo real del flujo de potencia reduce las pérdidas técnicas en la red, que, en Asturias, con su orografía compleja y modelo de líneas de distribución, pueden superar el 5-8% de la energía transportada. Cada punto porcentual de reducción de pérdidas equivale a decenas de miles de MWh anuales que no necesitarían ser generados.

3.5 FEDERATED LEARNING (FL).

El despliegue de modelos de IA en redes eléctricas enfrenta una tensión fundamental: los mejores modelos requieren grandes volúmenes de datos de alta calidad, pero los datos más valiosos como las lecturas de contadores inteligentes, los perfiles de operación de los sistemas de almacenamiento o los datos de proceso de las industrias electrointensivas son altamente sensibles desde las perspectivas de la privacidad individual (RGPD), el secreto comercial e incluso la seguridad nacional (datos de infraestructuras críticas).

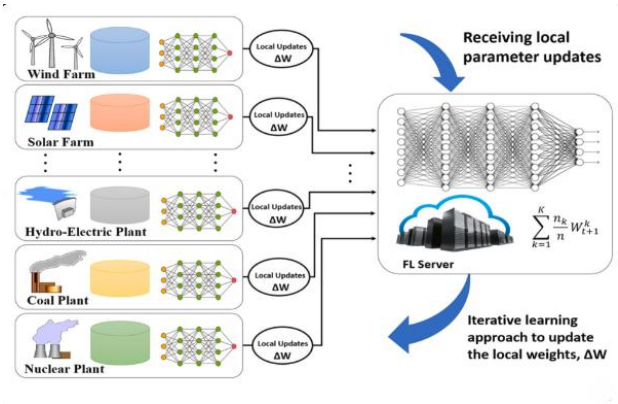

Ilustración 34. Federated Learning[75]

El *Federated Learning (FL)*[76] resuelve esta tensión mediante un cambio arquitectónico. En lugar de centralizar los datos para entrenar un modelo global, los datos permanecen en los dispositivos o servidores donde se generan, y solo se intercambian actualizaciones del modelo que no permiten reconstruir los datos originales. Un servidor federal agrega estas actualizaciones para construir un modelo global que refleja el conocimiento colectivo de todos los participantes sin que ningún actor tenga acceso a los datos de los demás.

3.5.1 ARQUITECTURAS Y VARIANTES.

Existen dos configuraciones fundamentales del *Federated Learning* con aplicaciones diferenciadas en el contexto energético asturiano. El *Federated Learning Horizontal (HFL)* es aplicable cuando los participantes tienen el mismo tipo de datos, pero sobre poblaciones diferentes, por ejemplo, los contadores inteligentes de los clientes y los de Distribución registran las mismas variables (kWh, perfil cuarto-horario,…) pero sobre usuarios distintos. Un modelo de predicción de demanda federado entre ambas distribuidoras mejoraría su capacidad de generalización geográfica sin violar las obligaciones de confidencialidad de los datos de clientes.

El *Federated Learning Vertical (VFL)* se aplica cuando diferentes actores tienen datos sobre los mismos usuarios, pero de tipos distintos (una comercializadora de energía tiene datos de contrato y facturación, la distribuidora tiene datos de medida en tiempo real, un agregador de flexibilidad tiene datos de respuesta del cliente,…). La combinación de estas perspectivas mediante VFL permitiría modelos de predicción de flexibilidad más precisos sin centralizar datos sensibles.

[75] Fuente: https://www.researchgate.net/

[76] Enfoque de Inteligencia Artificial que permite entrenar un modelo global de aprendizaje automático de forma descentralizada, manteniendo los datos guardados en los dispositivos locales donde se generaron, sin necesidad de subirlos nunca a un servidor central.

3.5.2 APLICACIONES EN LA RED ASTURIANA.

La red eléctrica asturiana presenta un escenario especialmente propicio para la aplicación del *Federated Learning* por la multiplicidad de actores con datos complementarios: Red Eléctrica de España como TSO, E-REDES o ELECTRANORTE como DSO, las Comunidades Energéticas, los grandes consumidores industriales del área central y los agregadores de flexibilidad. Las aplicaciones prioritarias incluirían la predicción federada de demanda a nivel regional, la detección federada de fraude en contadores inteligentes, el entrenamiento colaborativo de modelos de estimación de estado de la red, y la coordinación de recursos energéticos distribuidos en microrredes y comunidades energéticas.

3.5.3 IMPACTO DEL FEDERATED LEARNING.

Impacto Económico:

El FL permite a los actores del mercado energético asturiano colaborar en el desarrollo de modelos de IA más precisos sin ceder la ventaja competitiva que representan sus datos. Esto reduce las barreras de entrada a la IA para empresas pequeñas del sector que no tienen volúmenes de datos suficientes para entrenar modelos propios, democratizando el acceso a capacidades de predicción avanzada.

Impacto Social:

El FL es la tecnología que permite hacer compatibles los beneficios de la IA en la gestión de la red con los derechos de privacidad de los ciudadanos reconocidos en el RGPD. Sin FL, los modelos más potentes requieren ceder datos personales de consumo a terceros; con FL, la inteligencia puede mejorar sin que los datos salgan del perímetro del usuario.

Impacto Ambiental:

La mejora en la coordinación de la producción y equilibrado de la red permite incrementar la penetración de renovables en la red asturiana sin necesidad de grandes inversiones en infraestructura adicional. Además, el FL reduce la carga computacional respecto al entrenamiento centralizado al distribuir el procesamiento en los dispositivos de borde, reduciendo el consumo energético de los centros de datos.

3.6 LLM: GRANDES MODELOS DE LENGUAJE Y SU APLICACIÓN EN LA RED.

Los últimos desarrollos en IA se centran en aplicar modelos basados en un agente de IA existente como base de la arquitectura del sistema. Son entrenados en conjuntos de datos de tera-escala que incluyen texto científico, código, datos estructurados y registros operativos, desarrollando capacidades de razonamiento contextual, comprensión del lenguaje natural y generación de respuestas coherentes que superan a los modelos anteriores en tareas de flexibilidad y generalización.

La arquitectura de todos los LLMs modernos utiliza mecanismos que permiten capturar dependencias a largo plazo en secuencias de datos, ya sean palabras en texto, marcas temporales en series de consumo, o eventos en registros operativos de la red. Esta característica los hace superiores a las arquitecturas recurrentes para datos con dependencias de largo alcance, como los patrones estacionales anuales del consumo eléctrico o las correlaciones entre variables meteorológicas y generación renovable separadas por semanas.

3.6.1 ADAPTACIÓN AL DOMINIO ENERGÉTICO.

La adaptación de LLMs de propósito general al dominio energético se realiza mediante fine-tuning (el modelo pre-entrenado se especializa con datos específicos del sector, como registros SCADA, series temporales de medidores inteligentes, manuales de equipos, informes de incidencias, regulación sectorial). Sin necesidad de reentrenarlo desde cero hay técnicas que permiten que este proceso sea muy eficiente, modificando solo un subconjunto de los parámetros del modelo.

Otros modelos (modelo T5 afinado) se pueden usar para predicción de emisiones industriales de carbono a nivel provincial convirtiendo series temporales de consumo en formato textual y generando predicciones en lenguaje natural, superando métodos estadísticos clásicos.

El modelo BERT4ST (BERT for Spatio-Temporal), afinado con datos de velocidad de viento e irradiancia, supera consistentemente a modelos especializados en predicción de parques eólicos, demostrando que los LLMs preentrenados pueden aprender correlaciones espacio-temporales de la red sin conocimiento previo explícito del dominio físico.

El modelo TimeGPT, preentrenado sobre grandes conjuntos de series temporales multisectoriales, puede aplicarse a la predicción de carga eléctrica, siendo especialmente valioso en situaciones de escasez de datos históricos como ocurre con instalaciones nuevas o tipos de consumo emergentes.

3.6.2 INTELIGENCIA GENERATIVA PARA GESTIÓN DE RED Y CIBERSEGURIDAD.

La IA generativa, entendida como el conjunto de modelos capaces de generar datos sintéticos realistas, tiene aplicaciones de alto valor en contextos donde los datos reales son escasos o sensibles. Las Redes Generativas Adversariales (GANs) pueden crear datos simulados de generación eólica o solar para ampliar los datos disponibles y preparar los modelos para situaciones poco frecuentes, como fuertes rachas de viento o cambios rápidos en la radiación solar.

En el ámbito de la ciberseguridad, que cobra especial importancia para la infraestructura eléctrica crítica asturiana bajo el régimen NIS2, los LLMs y los modelos generativos pueden emplearse para generar escenarios de ataque sintéticos que entrenan a los sistemas de detección de intrusiones sin necesidad de haber experimentado los ataques reales, evaluar la robustez de los sistemas de IA ante ataques adversariales, y proporcionar asistencia en la interpretación de alertas de seguridad y en la elaboración de informes de incidentes.

3.6.3 LIMITACIONES DE LOS LLMS.

Los LLMs presentan limitaciones críticas que deben gestionarse para su aplicación en la infraestructura eléctrica. Las "alucinaciones", que es como se denomina a las respuestas plausibles pero incorrectas, dadas por uno de estos modelos, son la principal limitación y puede tener consecuencias graves si un operador de red actúa sobre una recomendación incorrecta del sistema. La literatura identifica varias estrategias de mitigación de este riesgo: la Generación Aumentada por Recuperación (RAG), que ancla las respuestas del LLM en fuentes de datos verificadas; los agentes críticos, que verifican las salidas del modelo antes de presentarlas al operador; y el razonamiento neuro-simbólico, que combina la capacidad generativa del LLM con reglas físicas y lógicas que deben satisfacerse.

Ilustración 35.Representación[77] de un LLM

La capacidad de cálculo es otro reto importante, ya que los modelos de inteligencia artificial más avanzados necesitan equipos potentes, como GPU, que pueden resultar costosos para las empresas distribuidoras. Para reducir estas necesidades se utilizan técnicas que permiten crear modelos pequeños que aprenden de otros modelos más grandes (se conoce como destilación), o que reduce la precisión de los cálculos para disminuir el tamaño y las necesidades de procesamiento del modelo (cuantización). Además, existen modelos de IA diseñados específicamente para funcionar con los equipos informáticos disponibles en las propias subestaciones eléctricas, sin necesidad de recurrir continuamente a grandes centros de procesamiento.

3.6.4 IMPACTO DE LOS LLMS.

Impacto Económico:

Los LLMs pueden reducir significativamente el coste de acceso a capacidades de análisis avanzado para empresas del sector energético de tamaño mediano que no pueden permitirse equipos de *data science* propios. Asimismo, la automatización de tareas de modelización energética de edificios (como la generación automática de modelos *EnergyPlus* mediante

[77] Fuente: https://medium.com/

agentes LLM) puede reducir los costes de auditoría energética, obligatoria para muchas instalaciones bajo la Directiva de Eficiencia Energética.

Impacto Social:

La interfaz conversacional que ofrecen los LLMs puede hacer accesible la información sobre el consumo energético propio y las opciones de ahorro a usuarios sin formación técnica, incluyendo poblaciones mayores o de baja renta que son especialmente vulnerables a la pobreza energética. El 22% de los asturianos mayores de 65 años no utiliza internet; los LLMs accesibles por voz o interfaces simplificadas pueden salvar esta brecha digital.

Impacto Ecológico:

La generación automática de informes de emisiones de carbono mediante LLMs facilita el cumplimiento de la Directiva CSRD y reduce la carga administrativa que frena la adopción de medidas de eficiencia en PYMES asturianas. Los LLMs también pueden analizar grandes volúmenes de documentación regulatoria sobre políticas energéticas y extraer información relevante para la planificación de inversiones en renovables en la región.

4. ARQUITECTURA PROPUESTA.

La arquitectura de un gemelo digital aplicada a las redes de distribución eléctrica en Asturias puede estructurarse en capas funcionales interconectadas que, tomadas en conjunto, permiten representar, supervisar y optimizar el comportamiento de la red en tiempo real. El modelo que se propone a continuación parte de los desarrollos conceptuales y tecnológicos que están siendo impulsados desde el ecosistema universitario asturiano, debiendo hacer especial referencia a los trabajos de PLEXIGRID. La propuesta se estructura en cuatro capas principales: la capa física, la capa de comunicaciones, la capa de modelado y simulación, y la capa de inteligencia y decisión basada en modelos de lenguaje de gran escala (LLM).

4.1 CAPA FÍSICA: ACTIVOS E INFRAESTRUCTURA DE LA RED ASTURIANA.

La capa física constituye el sustrato sobre el que opera el gemelo digital y comprende el conjunto de activos eléctricos reales de la red de distribución: subestaciones de transformación, líneas de media y baja tensión, centros de transformación, contadores inteligentes, inversores fotovoltaicos, sistemas de almacenamiento y puntos de recarga de vehículos eléctricos. En el caso de Asturias, la particular orografía del territorio y el elevado grado de dispersión de la edificación introducen condicionantes singulares que hacen especialmente necesaria una representación fiel de la red a nivel de baja tensión, habitualmente ausente en los sistemas de gestión convencionales.

Ilustración 36.Contadores Inteligentes[78]

La región cuenta con una penetración creciente de instalaciones de autoconsumo fotovoltaico vinculadas a comunidades energéticas en entornos rurales, con potencias inferiores a 100 kW, cuyo impacto sobre los flujos de potencia en baja tensión es difícil de gestionar con herramientas de monitorización tradicionales. La incorporación de estos activos al gemelo digital requiere su geolocalización precisa, la recogida de datos de generación y consumo en tiempo real a través de contadores inteligentes y el modelado eléctrico de la red que los conecta.

4.2 CAPA DE COMUNICACIONES: CONECTIVIDAD E INTEROPERABILIDAD.

La capa de comunicaciones es la responsable de garantizar el flujo continuo de datos entre los activos físicos y la plataforma de gemelo digital. En el contexto asturiano, la coexistencia de redes de comunicación heterogéneas — redes de fibra óptica en entornos urbanos, comunicaciones PLC (Power Line Communication) sobre la red eléctrica, redes móviles 4G/5G y, en zonas de menor cobertura, soluciones LPWAN[79] como LoRaWAN[80] — hace imprescindible una arquitectura de comunicaciones tolerante a la heterogeneidad y capaz de gestionar datos con diferentes granularidades temporales y niveles de latencia.

[78] Fuente: https://ganaenergia.com/
[79] Tecnologías de comunicación inalámbrica se basan en tecnologías de comunicación en rango amplio pero de baja potencia.
[80] Protocolo de red inalámbrica diseñada para IoT, permite realizar conexiones de larga distancia.

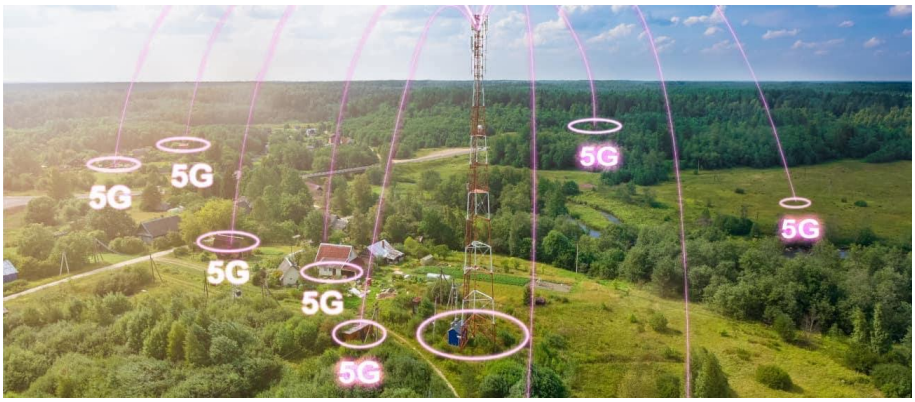

Ilustración 37.Representación[81] de una antena 5G

El estándar IEC 61850, ampliamente desarrollado en el apartado anterior, establece el marco de interoperabilidad para los equipos de la subestación y la red de media tensión, mientras que los protocolos DLMS/COSEM[82] y PRIME[83] son los de referencia para la comunicación con los contadores inteligentes en España. La integración de ambas familias de protocolos en una plataforma de gemelo digital exige capas de traducción semántica y modelos de datos unificados. En este ámbito, trabajos como los de PLEXIGRID se orientan a la obtención de datos procedentes de múltiples fuentes y formatos, construyendo una capa de datos unificada sobre la que opera el modelo digital de la red.

4.3 CAPA DE MODELADO Y SIMULACIÓN.

El núcleo del gemelo digital reside en la capa de modelado y simulación, donde los datos recogidos en tiempo real alimentan una representación matemática de la red eléctrica capaz de reproducir su comportamiento, anticipar situaciones de riesgo y evaluar alternativas de operación sin intervenir sobre el sistema real. Esta capa incluye, como mínimo, un motor de flujo de cargas que permite calcular tensiones, corrientes y pérdidas en cada nodo y rama de la red, así como modelos de predicción de generación renovable y demanda basados en series temporales e información meteorológica.

Para el caso asturiano, donde la integración de comunidades energéticas y la creciente electrificación de la movilidad están modificando los perfiles de carga en redes de baja tensión históricamente pasivas, esta capacidad de simulación anticipada tiene un valor operativo y económico difícilmente sustituible, al convertir esos perfiles de carga pasivos en elementos activos.

Otro elemento diferencial de esta capa es la capacidad de actualización continua del modelo a partir de los datos en tiempo real, lo que permite que el gemelo digital evolucione junto con la

[81] Fuente: https://www.telefonica.com/es/blog/telefonica-avanza-en-el-diseno-de-una-red-5g-verde/
[82] Device Language Message Specification/Companion Specification for Energy Metering son estándares asociados a la estructuración lectura y encriptado de los datos
[83] PoweRline Intelligent Metering Evolution, es una tecnología que opera en la capa física de la red empleando el cableado eléctrico existente para transmitir la información de los contadores y los nuevos sistemas de la red inteligente.

red física y mantenga su validez predictiva a lo largo del tiempo. Este proceso de calibración permanente, conocido como *state estimation*, distingue a los verdaderos gemelos digitales de los modelos estáticos de planificación convencionales.

4.4 CAPA DE DECISIÓN E INTEGRACIÓN DE LOS LLMS.

La capa superior de la arquitectura propuesta incorpora modelos de lenguaje de gran escala (LLM) como interfaz entre el gemelo digital y los operadores humanos, y como herramienta de razonamiento sobre los datos y resultados generados por las capas inferiores. Aunque su aplicación en el ámbito de la operación de redes eléctricas es aún emergente, los LLM ofrecen capacidades singulares que complementan de forma natural a los modelos analíticos tradicionales: la interpretación de datos no estructurados (informes de mantenimiento, registros de incidencias, normativa técnica), la generación de explicaciones comprensibles de situaciones de red complejas y el soporte a la toma de decisiones mediante razonamiento contextualizado.

En la práctica, un operador del centro de control de un distribuidor asturiano podría formular en lenguaje natural una consulta y recibir una respuesta generada por el LLM a partir de los resultados de simulación del gemelo digital, con la explicación de los factores determinantes y las posibles medidas correctoras. Esta capacidad de interacción conversacional reduce significativamente la barrera de acceso a las funcionalidades avanzadas del gemelo digital para personal técnico con distintos niveles de especialización.

La integración de LLMs en arquitecturas de gemelo digital para redes eléctricas plantea, no obstante, retos relevantes en materia de fiabilidad, alucinaciones y trazabilidad de las recomendaciones generadas. La tendencia más sólida en este ámbito apunta hacia arquitecturas RAG (*Retrieval-Augmented Generation*), en las que el LLM accede a los datos verificados del gemelo digital — y no solo a su conocimiento paramétrico — antes de formular cualquier respuesta, garantizando que las recomendaciones estén fundamentadas en el estado real de la red en cada momento.

4.5 IMPACTO ECONÓMICO.

La implantación de una arquitectura de gemelo digital en las redes de distribución asturianas generaría impactos económicos cuantificables en distintos niveles. Para los distribuidores, la reducción de pérdidas técnicas mediante la optimización continua de los flujos de potencia y la identificación temprana de elementos en sobrecarga puede suponer ahorros del orden del 3 % al 8 % de las pérdidas actuales, según estimaciones de proyectos comparables en redes europeas de distribución de características similares. La reducción del tiempo de reposición del suministro ante incidencias, gracias a la capacidad de localización precisa de fallos que ofrece el gemelo

digital, impacta directamente en los índices de calidad del suministro (TIEPI[84] y NIEPI[85]) y, por tanto, en las penalizaciones regulatorias a las que está sujeto el distribuidor.

Para el tejido industrial asturiano, la disponibilidad de una representación precisa del estado de la red en tiempo real habilita la participación efectiva en los mercados de flexibilidad descritos en el apartado anterior, con una mayor fiabilidad en el cumplimiento de los compromisos adquiridos, por tanto, una menor exposición a penalizaciones por incumplimiento. Las comunidades energéticas rurales, por su parte, podrían beneficiarse de una gestión optimizada de sus excedentes fotovoltaicos, al conocer con mayor precisión la capacidad de absorción de la red local en cada momento y adaptar sus estrategias de almacenamiento y vertido en consecuencia.

4.6 IMPACTO SOCIAL.

El impacto social de la implantación de gemelos digitales en la red de distribución asturiana se manifiesta en primer lugar a través de la mejora de la calidad del suministro eléctrico, con especial relevancia en los entornos rurales y de montaña donde la red presenta mayores índices de incidencia y donde la dependencia de servicios esenciales — calefacción eléctrica, equipos médicos domiciliarios, sistemas de comunicación — hace especialmente costosas las interrupciones del suministro. La capacidad predictiva del gemelo digital para anticipar sobrecargas y fallos permite una actuación proactiva del distribuidor que reduce tanto la frecuencia como la duración de las interrupciones.

4.7 IMPACTO AMBIENTAL.

La contribución ambiental de los gemelos digitales aplicados a las redes eléctricas opera a través de dos mecanismos principales. El primero es la reducción de pérdidas en la red, que implica directamente una menor generación necesaria para satisfacer una demanda dada y, por tanto, una reducción de emisiones asociadas a la generación eléctrica. Aunque el mix eléctrico asturiano está en proceso de descarbonización acelerada, la reducción de pérdidas tiene un impacto ambiental positivo tanto en el período de transición como una vez alcanzada la plena integración renovable, al liberar capacidad de red para la evacuación de generación limpia adicional.

El segundo mecanismo es la habilitación de una mayor integración de energías renovables distribuidas sin comprometer la estabilidad de la red. La capacidad del gemelo digital para simular en tiempo real el impacto de nuevas instalaciones fotovoltaicas o de aerogeneradores de pequeña potencia sobre la tensión y la carga de los transformadores locales permite a los distribuidores autorizar conexiones que, con los criterios conservadores actuales, serían rechazadas por ausencia de información suficiente. Esta función de facilitador de la integración renovable es quizás la contribución ambiental más relevante de la tecnología en el contexto de

[84] Tiempo medio en horas o minutos que un cliente esta sin suministro eléctrico al año en una zona determinada.
[85] Es el número promedio de veces que el servicio eléctrico se interrumpe para un cliente durante el año.

la transición energética asturiana, donde el potencial de generación distribuida pendiente de conexión es aún muy significativo.

La posibilidad de certificar los ahorros energéticos derivados de la optimización de la red mediante el mecanismo de Certificados de Ahorro Energético (CAEs), respaldada por la trazabilidad que ofrece el gemelo digital, añade una dimensión económica al impacto ambiental y puede contribuir a financiar parcialmente la implantación y mantenimiento de la plataforma, generando un modelo de sostenibilidad tecnológica alineado con los incentivos regulatorios vigentes.

5. LIMITACIONES DE LAS REDES INTELIGENTES.

Las redes inteligentes y los gemelos digitales ofrecen ventajas sustanciales en eficiencia, supervisión y capacidad de respuesta, pero presentan limitaciones técnicas, regulatorias y operativas que conviene identificar con claridad.

5.1 LIMITACIONES TÉCNICAS.

Un proyecto dedicado a implementar una red inteligente estará sujeto a las siguientes limitaciones técnicas:

- ***Ampliación de la superficie de ciberataques:*** La digitalización implica multiplicar los puntos de conexión, sensores y sistemas de comunicación expuestos, invirtiendo la lógica tradicional de seguridad de redes antes físicamente aisladas y hoy crecientemente interconectadas.
- ***Dependencia de la calidad e integridad de los datos:*** Un gemelo digital es tan fiable como los datos que lo alimentan. Datos incompletos, retrasados o manipulados —de forma accidental o deliberada— pueden conducir a decisiones operativas erróneas sin que existan señales evidentes de alarma.
- ***Heterogeneidad tecnológica y deuda técnica:*** La coexistencia de equipos legados con protocolos sin cifrado y tecnología digital moderna obliga a introducir capas de conversión que constituyen, en sí mismas, nuevas vulnerabilidades, y dificulta la aplicación homogénea de actualizaciones de seguridad.
- ***Limitaciones de latencia y tiempo real*:** Las capas de protección (cifrado, segmentación, detección de intrusiones) pueden introducir retardos incompatibles con operaciones que requieren respuesta en milisegundos, como la protección de subestaciones o el control de frecuencia, obligando a un equilibrio constante entre seguridad y rendimiento.
- ***Complejidad y fiabilidad del modelado:*** Un gemelo digital de una red eléctrica completa es un sistema de modelado extremadamente complejo, que debe sincronizarse en tiempo casi real con un sistema físico en constante cambio. Errores de calibración, desviaciones acumuladas entre el modelo y la realidad, o la dificultad de validar el comportamiento del gemelo frente a escenarios extremos poco frecuentes (eventos

meteorológicos severos, fallos en cascada) limitan la confianza que puede depositarse en sus predicciones en los casos más críticos.

5.2 RETOS RELACIONADOS CON LA GENERACIÓN DISTRIBUIDA.

La generación distribuida (instalaciones fotovoltaicas residenciales e industriales, pequeños aerogeneradores, sistemas de autoconsumo, puntos de recarga de vehículos eléctricos con capacidad de inyección a la red), introduce una limitación estructural específica para las redes inteligentes y sus gemelos digitales. La red eléctrica fue diseñada originalmente bajo un modelo unidireccional, con flujos de energía predecibles desde grandes centrales hacia los puntos de consumo. La generación distribuida invierte parcialmente esta lógica, generando flujos bidireccionales y una variabilidad mucho mayor en los nodos de baja tensión, donde tradicionalmente existía menos instrumentación y menor capacidad de monitorización.

Esto plantea varios problemas concretos. En primer lugar, un problema de visibilidad: muchas instalaciones de generación distribuida, especialmente las de pequeña escala, no están suficientemente monitorizadas en tiempo real, lo que genera puntos ciegos en el gemelo digital que dificultan representar con precisión el estado real de la red en los tramos de distribución de baja tensión. En segundo lugar, un problema de seguridad ampliada: cada instalación distribuida con capacidad de comunicación remota (inversores inteligentes, sistemas de gestión de baterías) constituye un nuevo punto potencial de acceso a la red, gestionado a menudo por el propio usuario final o por terceros sin los mismos estándares de seguridad que el operador de la red, lo que traslada parte del riesgo cibernético fuera del perímetro de control directo del DSO. En tercer lugar, un problema de estabilidad técnica: la intermitencia de muchas fuentes distribuidas (solar, eólica a pequeña escala) introduce fluctuaciones que el gemelo digital debe anticipar y gestionar para evitar problemas de tensión, frecuencia o sobrecarga en tramos de red que no fueron diseñados originalmente para flujos bidireccionales de esta magnitud.

5.3 RETOS DEL EQUILIBRIO DE LA RED Y SU SENSIBILIDAD.

Una red eléctrica funciona bien cuando la cantidad de electricidad que se genera coincide en todo momento con la cantidad que se consume. Este equilibrio se mide a través de la frecuencia de la red, en el caso de Europa se fija en 50 Hz y en el caso de la red americana son 60 Hz. La tarea de mantenerla estable se centra en evitar las desviaciones de frecuencia en el caso que se varíen los valores de la frecuencia en exceso se activan automáticamente sistemas de protección que desconectan generadores o zonas de consumo para evitar daños mayores en los equipos. En las redes tradicionales, este equilibrio era relativamente fácil de mantener porque la electricidad se generaba en pocas centrales grandes (térmicas, nucleares, hidráulicas), que utilizan turbinas pesadas girando de forma continua, aportando una inercia al sistema. Esa masa en movimiento actúa como una especie de "colchón físico": si se produce un fallo repentino, la inercia de esas turbinas amortigua el golpe y da tiempo a que los operadores reaccionen antes de que la frecuencia se descontrole.

El problema es que la generación distribuida no funciona así. Estas fuentes se conectan a la red a través de inversores electrónicos, que no tienen elementos físicos girando y por lo tanto no

aportan esa inercia. Cuanta más generación de este tipo entra en el sistema y menos peso tienen las centrales tradicionales, menos inercia tiene la red en su conjunto. En la práctica, esto significa que cuando ocurre un imprevisto (caídas de línea, se desconecta una central grande, sube mucho la demanda de golpe) la frecuencia de la red puede moverse mucho más rápido y mucho más bruscamente que antes. Y como se mueve más rápido, los operadores y los sistemas automáticos tienen menos tiempo para reaccionar antes de que se disparen las protecciones, lo que aumenta el riesgo de que un problema pequeño y localizado termine convirtiéndose en un apagón que afecta a una zona mucho más amplia.

A esto se añade que la generación renovable es, por su propia naturaleza, más difícil de predecir: la generación solar y eólica varía constantemente según las condiciones meteorológicas, mucho más que la producción de una central convencional. Esto obliga a los operadores a estar corrigiendo el equilibrio de la red de forma mucho más frecuente y mucho más fina que antes. Y aquí entra en juego el gemelo digital: si la información que recibe sobre lo que está pasando en la red (especialmente en las zonas de baja tensión, donde está la mayoría de la generación distribuida) llega incompleta, retrasada o manipulada, el operador pierde justo la capacidad de anticipación que más necesita en un sistema que, al tener menos inercia, ya de por sí le da menos margen de reacción.

Dicho de forma sencilla: las redes eléctricas modernas son más limpias y eficientes, pero también menos controlables— reaccionan más rápido a los problemas, tanto en sentido positivo como negativo, y eso reduce el margen de error disponible para corregir un fallo antes de que se convierta en un corte de suministro. Esto conecta directamente con la ciberseguridad del gemelo digital: si un ataque consigue dejar sin información temporalmente al operador justo en el momento en que se produce una perturbación física en la red, el tiempo disponible para evitar un apagón es menor que en un sistema eléctrico tradicional, menos digitalizado y con más inercia. Por eso, proteger el gemelo digital frente a ciberataques no es solo una cuestión de cumplimiento normativo o de protección de datos: es, cada vez más, una condición necesaria para que la propia red eléctrica se mantenga físicamente estable.

En el caso de Asturias, esta situación tiene una relevancia especial por la combinación de un parque eólico ya consolidado, un crecimiento esperado de la energía solar y el autoconsumo, y la presencia de grandes consumidores industriales, cuya desconexión repentina —ya sea provocada deliberadamente o como consecuencia de un fallo en cascada— tendría un impacto desproporcionado sobre el equilibrio de toda la red regional.

5.4 RETOS RELACIONADO CON LA CONGESTIÓN.

Cada tramo de la red de distribución tiene una capacidad física máxima de transporte de electricidad, determinada por el grosor de los cables, la capacidad de los transformadores y otros elementos de la infraestructura. Cuando la generación distribuida conectada a un mismo tramo produce en un momento más electricidad de la que ese tramo puede absorber o transportar de forma segura, el operador de red no tiene otra opción que limitar artificialmente esa inyección de energía, una práctica conocida como "*curtailment*" o recorte de generación. Esto supone un problema en dos sentidos. Por un lado, es una ineficiencia económica evidente:

energía renovable que podría haberse aprovechado se desperdicia, y los productores —que en muchos casos son particulares o pequeñas empresas que han invertido en sus propias instalaciones— ven reducidos sus ingresos sin haber tenido ningún fallo técnico, simplemente porque la red no tiene capacidad suficiente en ese momento y lugar. Por otro lado, supone un reto añadido para el gemelo digital, que debe calcular en tiempo casi real cuanto margen de maniobra queda disponible en cada tramo de la red, combinando datos de generación, consumo y límites técnicos de cada elemento, para poder anticipar dónde y cuándo será necesario aplicar estos recortes antes de que se conviertan en un problema de seguridad del propio sistema. Cuanto más crece la generación distribuida sin una inversión paralela en refuerzo de la red, más frecuente y más extenso se vuelve este problema.

5.5 CIBERSEGURIDAD Y SEGURIDAD FISICA COMO RIESGOS CONVERGENTES.

Tradicionalmente, la ciberseguridad y la seguridad física de las instalaciones eléctricas se han tratado como dos mundos relativamente separados: uno protege los datos y los sistemas informáticos, el otro protege los equipos y las instalaciones físicas. Sin embargo, en un sistema tan interconectado como el que describe este documento, ambos mundos se retroalimentan mutuamente, y no siempre en una sola dirección.

Es evidente que un ciberataque puede provocar un problema físico. Pero el camino inverso también existe: un apagón o cualquier otra perturbación física de la red puede, a su vez, debilitar las propias defensas de ciberseguridad.

Por ejemplo, si un corte de suministro afecta a un centro de control o a una subestación, los sistemas de respaldo eléctrico (baterías, generadores de emergencia) que mantienen operativos los cortafuegos, los sistemas de detección de intrusiones o las cámaras de videovigilancia tienen una autonomía limitada; si el apagón se prolonga más de lo previsto, esos sistemas de seguridad pueden empezar a fallar justo en el momento en que más se necesitan, dejando a las instalaciones más expuestas frente a un segundo ataque o frente a un acceso físico no autorizado.

Este fenómeno se conoce como riesgo cíber-físico convergente, y su característica más peligrosa es precisamente que crea un círculo de retroalimentación negativa: un problema inicial, ya sea digital o físico, debilita las defensas del otro dominio, lo que facilita un segundo incidente, que a su vez puede agravar aún más la situación original.

Por este motivo, los planes de gestión de crisis y de continuidad de negocio mencionados en este documento no pueden diseñarse pensando en escenarios puramente cibernéticos o puramente físicos por separado, sino que deben contemplar explícitamente esta posible combinación.

5.6 ESCALABILIDAD DEL GEMELO DIGITAL.

Un gemelo digital no es un programa estático, sino un sistema que necesita recibir, procesar y actualizar constantemente los datos procedentes de miles (y, a medida que crece la generación distribuida, potencialmente cientos de miles) de puntos de la red: medidores inteligentes,

sensores, inversores, sistemas de protección. Cada nuevo punto de generación distribuida; cada nuevo punto de recarga de vehículo eléctrico con capacidad de inyección a la red; cada nuevo sensor instalado para ganar visibilidad sobre la baja tensión, añaden una fuente más de datos que el gemelo digital debe incorporar y procesar, idealmente en tiempo casi real para que su representación de la red siga siendo útil. Esto plantea un problema de escalabilidad: la infraestructura de cómputo (servidores, capacidad de proceso) y de comunicaciones (ancho de banda de las redes que transportan estos datos) que es suficiente hoy puede no serlo en pocos años si el crecimiento de la generación distribuida y de los dispositivos conectados continúa al ritmo previsto. Si el sistema no se dimensiona con un margen de crecimiento adecuado desde el principio, pueden aparecer cuellos de botella técnicos —retrasos en la actualización del modelo, saturación de las comunicaciones, necesidad de ampliaciones de infraestructura no presupuestadas— que reduzcan la utilidad del gemelo digital precisamente en el momento en que la red más necesita esa visibilidad, por ser más compleja y tener más elementos que coordinar.

5.7 FALSOS POSITIVOS Y FATIGA POR ALERTAS.

Cuantos más sensores, medidores y puntos de monitorización se incorporan a una red inteligente, mayor es la cantidad de información que el sistema de detección de anomalías debe procesar, y con ella, mayor es también el volumen de alertas que genera.

El problema es que no todas estas alertas corresponden a incidentes reales: una variación de tensión perfectamente normal, un pico de consumo estacional, o un simple error de calibración de un sensor pueden disparar avisos que, vistos de forma aislada, parecen indicar un problema grave.

Cuando el número de estas alertas, que en su mayoría suelen ser falsos positivos, crece de forma sostenida, los operadores humanos deben revisarlas y decidir si requieren acción lo que genera que se vean sometidos a lo que se conoce como "fatiga por alertas": un fenómeno bien documentado en ciberseguridad y en otros campos de monitorización crítica (como la medicina intensiva), por el cual la exposición constante a avisos de bajo valor informativo reduce progresivamente la capacidad de atención y de respuesta ante cualquier alerta, incluidas las legítimas.

El resultado paradójico es que un sistema diseñado para mejorar la seguridad y la capacidad de reacción puede, si no está bien calibrado, terminar generando el efecto contrario: operadores que normalizan el ruido, que tardan más en reaccionar, o que llegan a desactivar o ignorar ciertas categorías de alertas para poder gestionar su carga de trabajo, precisamente el tipo de comportamiento que un atacante sofisticado podría aprovechar para que una intrusión real pase desapercibida entre el ruido de fondo. Mitigar este problema exige invertir en sistemas de correlación y priorización de alertas más inteligentes —y no solo en añadir más sensores—, así como en un dimensionamiento adecuado del equipo humano encargado de revisarlas.

5.8 DEPENDENCIA DE LA SINCRONIZACIÓN TEMPORAL.

Muchas de las funciones más críticas de una red eléctrica inteligente dependen de que todos los dispositivos involucrados compartan exactamente la misma referencia de tiempo, con una precisión que se mide en microsegundos. Esto es esencial, por ejemplo, para la protección de líneas (que compara mediciones tomadas en dos extremos distintos de una misma línea para detectar fallos) o para que el gemelo digital pueda reconstruir correctamente el orden en que ocurrieron los eventos durante un incidente.

Esta sincronización se obtiene habitualmente mediante señales de GPS o mediante protocolos como el PTP (*Precision Time Protocol*, o Protocolo de Tiempo de Precisión). El problema es que esta dependencia introduce, a su vez, un punto único de fragilidad: si la señal de GPS se pierde —por ejemplo, por un fallo del receptor, por interferencias atmosféricas, o por un ataque deliberado de interferencia o suplantación de la señal GPS (lo que se conoce como *jamming* o *spoofing*)—, o si el protocolo PTP es manipulado, los distintos dispositivos de la red pueden empezar a registrar los eventos con marcas de tiempo ligeramente distintas entre sí. Esto puede tiene consecuencias reelvantes: un sistema de protección diferencial mal sincronizado puede no detectar un fallo real, o peor, puede generar una desconexión innecesaria al interpretar erróneamente una diferencia de tiempo como un fallo físico.

Además, en el análisis forense posterior a un incidente —ya sea un fallo técnico o un ciberataque—, una sincronización horaria defectuosa puede dificultar enormemente reconstruir con precisión la secuencia exacta de lo ocurrido, complicando tanto la respuesta inmediata como la investigación y el reporte posterior a las autoridades supervisoras.

5.9 VIDA ÚTIL DESIGUAL DE LOS COMPONENTES.

Los grandes activos físicos de una red eléctrica, como son los transformadores, líneas de transporte y subestaciones, se diseñan y se amortizan pensando en ciclos de vida de varias décadas, a menudo entre 25 y 40 años o más. El hardware y el software digital se instala para monitorizar y proteger esos mismos activos que sigue; en cambio, tienen un ciclo de vida tecnológico mucho más corto: un servidor, un sistema operativo o una plataforma de ciberseguridad puede quedar obsoleto, sin soporte del fabricante, o tecnológicamente superado en cinco o diez años, es decir en muchos casos antes de que el activo físico que protege llegue a la mitad de su vida útil prevista.

Esto genera un desajuste estructural y recurrente. A lo largo de la vida de un mismo transformador o de una misma subestación será necesario sustituir o actualizar varias veces el conjunto de sistemas digitales asociados —sensores, pasarelas de comunicación, sistemas SCADA, plataformas de ciberseguridad—, lo que implica un coste recurrente que debe planificarse desde el principio del proyecto y no tratarse como un gasto excepcional. Además, este desajuste temporal complica la propia gestión de la ciberseguridad: durante los periodos de transición entre una generación de sistemas digitales y la siguiente, es habitual que coexistan equipos de distintas épocas tecnológicas sobre una misma instalación física, lo que reproduce y agrava precisamente el problema de heterogeneidad y deuda técnica descrito anteriormente en

este documento, y obliga a mantener planes de actualización tecnológica planificados con la misma seriedad con que se planifica el mantenimiento de los activos físicos.

5.10 EXCESO DE PARADAS POR SOBRE-SENSIBILIDAD.

Una de las paradojas menos intuitivas de la digitalización de la red es que un sistema más sensible y con mayor capacidad de detección puede hacer un sistema menos robusto. Los sistemas de protección analógicos tradicionales se diseñaron con umbrales de actuación relativamente simples y conservadores: reaccionan ante un número limitado de magnitudes físicas (sobrecorriente, sobretensión, desviación de frecuencia) y solo cuando estas superan márgenes claramente definidos. Esta simplicidad, aunque limita su capacidad de detección, también los hace menos propensos a activarse innecesariamente, precisamente porque no interpretan más información que aquella para la que fueron diseñados.

Los sistemas digitales modernos, en cambio, monitorizan un número mucho mayor de variables, con mayor resolución y mayor frecuencia de muestreo, y a menudo emplean lógicas de protección más sofisticadas que combinan varias señales para tomar decisiones. Esta mayor capacidad de detección tiene un coste: el sistema puede llegar a interpretar como anómalas situaciones que, en la práctica, no representaban ningún riesgo real para la red, pero que un sistema analógico simplemente no habría registrado como relevantes.

El resultado es que los sistemas digitales pueden desconectar líneas, generadores o tramos de red ante eventos transitorios o fluctuaciones menores que, en una red más simple, no habrían provocado ninguna actuación. Esto se traduce en un número de paradas o desconexiones más frecuente, no porque la red sea objetivamente menos segura, sino porque el sistema de protección es más sensible y, en ocasiones, sobre reacciona ante perturbaciones que no requerían realmente una intervención.

Este fenómeno tiene dos consecuencias prácticas. La primera es puramente operativa: cada desconexión injustificada tiene un coste —económico, de calidad de suministro, y de confianza de los usuarios y de las industrias conectadas a la red—, incluso cuando la causa raíz no era un fallo real sino una interpretación excesivamente cautelosa de los datos disponibles. La segunda conecta directamente con el problema de "fatiga por alertas" descrito anteriormente.

Calibrar correctamente estos umbrales —de forma que el sistema aproveche su mayor capacidad de detección sin caer en una sobre reacción sistemática— es, por tanto, un reto técnico de primer orden en el diseño de cualquier red inteligente y de su gemelo digital, y debe entenderse como un proceso de ajuste continuo, no como una configuración que se establece una sola vez al desplegar el sistema. Lograr este equilibrio exige validar los nuevos algoritmos de protección frente a un histórico amplio de eventos reales de la red, para asegurarse de que la mayor sensibilidad se traduce en mejor detección de fallos genuinos, y no simplemente en más desconexiones de eventos sin consecuencia real.

6. CONCLUSIONES

Se puede afirmar que los gemelos digitales aplicados a las redes de distribución eléctrica constituyen una solución técnicamente madura y económicamente justificable, cuya implantación en el contexto asturiano responde a una necesidad operativa cada vez más acuciante.

La transición energética en curso —caracterizada por la incorporación masiva de generación renovable distribuida, la electrificación de la movilidad y la aparición de comunidades energéticas rurales ente otros procesos— está transformando de forma estructural el comportamiento de unas redes diseñadas originalmente para un modelo de generación centralizada y demanda pasiva. La orografía asturiana, la dispersión de su edificación y la coexistencia de un tejido industrial electrointensivo con un entorno rural en plena descarbonización convierten a la región en un caso de uso especialmente representativo de los retos que afrontarán las redes de distribución europeas en la próxima década.

Frente a estos retos, la arquitectura de gemelo digital propuesta —articulada en cuatro capas, desde la representación física de los activos hasta la interfaz conversacional basada en modelos de lenguaje de gran escala— ofrece una respuesta que va más allá de la monitorización convencional. La incorporación de técnicas de inteligencia artificial (*Machine Learning, Deep Learning, Reinforcement Learning, Federated Learning y LLMs*) permite avanzar desde la mera descripción del estado de la red hacia la anticipación de su evolución y, en última instancia, hacia la prescripción de acciones óptimas de operación. El *Federated Learning* merece una mención particular, al ofrecer una vía para desarrollar modelos de IA de calidad sin comprometer las exigencias de privacidad del RGPD ni la confidencialidad comercial de los actores del mercado, una condición indispensable para la viabilidad regulatoria y social del conjunto del sistema. Los impactos económicos, sociales y ambientales estimados —reducciones de pérdidas técnicas del 3-8 %, mejora de los índices de calidad del suministro, mayor integración de renovables distribuidas y generación de empleo cualificado — refuerzan el atractivo de esta tecnología como palanca de modernización del sistema eléctrico regional.

No obstante, la digitalización de la red, precisamente por ampliar la información disponible y de puntos de conexión, introduce una nueva categoría de riesgos que las redes tradicionales no afrontaban: una mayor “superficie” expuesta a ciberataques, una dependencia crítica de la calidad e integridad de los datos que alimentan el gemelo digital, y una heterogeneidad tecnológica —fruto de la convivencia entre equipos legados y sistemas modernos— que genera tanto deuda técnica como nuevas vulnerabilidades.

A esto se suma una paradoja estructural identificada: los sistemas más sensibles y con mayor capacidad de detección no son necesariamente más robustos, ya que pueden generar un exceso de desconexiones por sobre sensibilidad o provocar fatiga de alertas en los operadores humanos, debilitando en la práctica la respuesta ante incidentes reales. La progresiva pérdida de inercia del sistema eléctrico asociada a la generación distribuida basada en inversores electrónicos, combinada con los problemas de congestión, visibilidad y sincronización temporal descritos, hace que las redes inteligentes sean, en cierto sentido, sistemas más eficientes, pero

también más sensibles ante perturbaciones, con un margen de reacción menor que el de las redes convencionales. Estas limitaciones exigen un diseño e implantación que incorporen desde el origen una perspectiva de resiliencia cíber-física, y no solo de eficiencia operativa.

El marco normativo —IEC 61850, la Directiva NIS2, el Data Act, el RGPD y la legislación sectorial eléctrica— lejos de constituir un obstáculo, proporciona precisamente el marco de referencia necesario para construir una arquitectura técnica y organizativa robusta, auditada y confiable frente a estos riesgos. El cumplimiento de estándares no debe entenderse únicamente como una obligación legal, sino como una condición para la interoperabilidad con otros actores del sistema y para la calidad y confiabilidad en las recomendaciones generadas por el gemelo digital ante reguladores, auditores e inversores. El análisis económico muestra además que el coste de cumplimiento normativo y de las medidas de ciberseguridad asociadas, aunque significativo, resulta comparable o incluso inferior al coste potencial de un incidente cibernético grave no contenido, lo que convierte la inversión en seguridad en una decisión económicamente racional y no solo en un requisito impuesto desde fuera.

Desde la perspectiva del ecosistema asturiano, la existencia de empresas tecnológicas de referencia representa un activo estratégico de primer orden, que permite desarrollar, validar y escalar esta tecnología en el propio territorio, con datos reales de la red asturiana y en colaboración con los distribuidores presentes en la región. Esta capacidad local sitúa a Asturias en una posición diferencial respecto a otras comunidades autónomas dependientes de soluciones importadas, con implicaciones directas sobre la generación de empleo cualificado, la retención de talento y la atracción de inversión en un sector estratégico para la transición justa de la región.

En síntesis, la implantación de gemelos digitales en las redes de distribución asturianas no debe entenderse como una mejora tecnológica incremental, sino como una condición habilitante para que Asturias afronte con más garantías aún el proceso de descarbonización de su sistema energético, sin comprometer la competitividad de su tejido industrial ni la calidad del suministro a sus ciudadanos. Sin embargo, esta misma transformación exige asumir, de la misma forma que se asumen sus beneficios, las nuevas vulnerabilidades técnicas, regulatorias y de resiliencia física que introduce la digitalización de la red. La madurez tecnológica de la solución, la urgencia de los retos operativos, la disponibilidad de capacidad local de desarrollo y un marco normativo adecuado que mitiga buena parte de los riesgos identificados, ofrecen una buena oportunidad de desarrollo.

7. BIBLIOGRAFÍA

7.1 LEGISLACIÓN EUROPEA

- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2).
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (CER).
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento de Ciberseguridad / Cybersecurity Act).
- Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo sobre requisitos horizontales de ciberseguridad para los productos con elementos digitales (Cyber Resilience Act — CRA).
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de IA / AI Act). Diario Oficial de la Unión Europea.
- Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (Data Act). Diario Oficial de la Unión Europea.

7.2 LEGISLACIÓN ESTATAL ESPAÑOLA

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 12/2022, de 5 de julio, por el que se adoptan medidas urgentes en el ámbito de la ciberseguridad y de la seguridad de las infraestructuras críticas (transposición parcial NIS2).
- Ley 24/2013, de 26 de diciembre, del Sector Eléctrico (arts. 4 y 40 — obligaciones de seguridad del operador del sistema y distribuidores).

7.3 NORMAS TÉCNICAS INTERNACIONALES

- IEC 62443 (serie completa). Security for industrial automation and control systems. International Electrotechnical Commission.
- IEC 62443-3-2:2020 — Security risk assessment for system design.
- IEC 62443-2-4:2015+AMD1:2017 — Security program requirements for IACS service providers.

- ISO/IEC 27001:2022 — Information security management systems.
- ISO/IEC 27019:2017 — Information security controls for the energy utility industry.
- ISO/IEC 27005:2022 — Information security risk management.
- IEC 61850 (2013). Communication networks and systems in substations. International Electrotechnical Commission.
- NERC CIP (Critical Infrastructure Protection Standards) — Referencia internacional para sistemas de control eléctrico.

7.4 DOCUMENTOS DE REFERENCIA INSTITUCIONAL

- ENISA (2023). Threat Landscape for the Energy Sector 2023. European Union Agency for Cybersecurity.
- ENISA (2022). Guidelines on Security of IoT – Secure Supply Chain for IoT.
- CNPIC (2023). Guía de Buenas Prácticas para la Protección de las Infraestructuras Críticas del Sector Energético. Ministerio del Interior.
- CCN-CERT (2023). CCN-STIC 885 A – Seguridad en Sistemas de Control Industrial. Centro Criptológico Nacional.
- CCN-CERT (2022). CCN-STIC 480 — Ciberseguridad en redes eléctricas. Centro Criptológico Nacional.
- INCIBE (2023). Guía de Ciberseguridad para Operadores de Servicios Esenciales. Instituto Nacional de Ciberseguridad.
- ICS-CERT / CISA (2023). ICS Security Guidance for Critical Energy Infrastructure. Cybersecurity and Infrastructure Security Agency (EE.UU., referencia internacional).
- ETIP SNET (2022). Ciberseguridad en Redes Energéticas Inteligentes: Recomendaciones para Operadores Europeos. Comisión Europea, JRC.
- Red Eléctrica de España (2024). Informe de Servicios de Ajuste del Sistema Eléctrico 2024. REE/Redeia.
- Red Eléctrica de España (2024). El sistema eléctrico español: Informe anual. REE, Madrid.
- IDAE (2022). Plan Nacional Integrado de Energía y Clima (PNIEC) 2021-2030. Ministerio para la Transición Ecológica y el Reto Demográfico.
- AENOR / CNMC (2023). Plan de Despliegue de Contadores Inteligentes en España: Balance y perspectivas. Madrid.
- Principado de Asturias (2021). Estrategia Asturiana de Transición Energética EATE 2030. Consejería de Industria.
- Principado de Asturias (2021). Agenda para la Industria Asturiana 2021-2025. Consejería de Industria, Empleo y Promoción Económica.

7.5 SMARTGRIDS Y APLICACIONES IA

- Antonesi, G., Cioara, T., Anghel, I., Michalakopoulos, V., Sarmas, E., & Toderean, L. (2025). A systematic review of transformers and large language models in the energy sector: towards agentic digital twins. Applied Energy, 401, 126670.

- Banad, Y. M., Sharif, S. S., & Rezaei, Z. (2025). Artificial intelligence and machine learning for smart grids: from foundational paradigms to emerging technologies with digital twin and large language model-driven intelligence. Energy Conversion and Management: X, 28, 101329.
- Heluany, J. B., & Gkioulos, V. (2024). A review on digital twins for power generation and distribution. International Journal of Information Security, 23, 1171–1195.
- Noura, H. N., Yaacoub, J. P. A., Salman, O., & Chehab, A. (2025). Advanced Machine Learning in Smart grids: An Overview. Internet of Things and Cyber-Physical Systems.
- Shahverdi, N., Saffari, A., & Amiri, B. (2025). A systematic review of artificial intelligence and machine learning in energy sustainability. Energy Reports, 13, 5551–5578.

7.6 GEMELOS DIGITALES

- Aghazadeh Ardebili, A., Zappatore, M., Attia Ramadan, A.I.H., Longo, A. y Ficarella, A. (2024). Digital Twins of smart energy systems: a systematic literature review on enablers, design, management and computational challenges. Energy Informatics, 7(94).
- Mchirgui, N., Quadar, N., Kraiem, H. y Lakhssassi, A. (2024). The Applications and Challenges of Digital Twin Technology in Smart grids: A Comprehensive Review. Applied Sciences, 14(23), 10933.
- Digital Twin Consortium (2021). The definition of a digital twin.
- Tao, F., Zhang, M. y Nee, A. (2019). Digital twin driven smart manufacturing. Academic Press.
- Khan, M.M.S., Giraldo, J.A. y Parvania, M. (2023). Real-Time Cyber Attack Localization in Distribution Systems Using Digital Twin Reference Model. IEEE Transactions on Power Delivery, 38, 3238–3249.
- Onile, A.E., Petlenkov, E., Levron, Y. y Belikov, J. (2024). Smartgrid-Based Hybrid Digital Twins Framework for Demand Side Recommendation Service Provision in Distributed Power Systems. Future Generation Computer Systems, 156, 142–156.
- Coppolino, L., Nardone, R., Petruolo, A. y Romano, L. (2023). Building Cyber-Resilient Smart grids with Digital Twins and Data Spaces. Applied Sciences, 13, 13060.
- Salvi, A., Spagnoletti, P. y Noori, N.S. (2022). Cyber-Resilience of Critical Cyber Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem. Computers & Security, 112, 102507.
- Rasheed, A., San, O. y Kvamsdal, T. (2020). Digital twin: values, challenges and enablers from a modeling perspective. IEEE Access, 8, 21980–22012.
- Massel, L. y Massel, A. (2020). Development of digital twins and digital shadows of energy objects and systems using scientific tools for energy research. E3S Web Conference, 209.
- Kumar, P. et al. (2023). Digital Twin-Driven SDN for Smart grid: A Deep Learning Integrated Blockchain for Cybersecurity. Solar Energy, 263, 111921.
- Steindl, G. et al. (2020). Generic digital twin architecture for industrial energy systems. Applied Sciences Basel, 10(24), 8903.