Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Ángel Tomás Ledo Iglesias
Investigador en formación en la Escuela Internacional de Doctorado de la UNED, en el programa "Análisis de problemas sociales"

IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL JUNTO A LAS YA NO TAN NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, EN RELACIÓN A LA SEGURIDAD DE INFRAESTRUCTURAS ESTRATÉGICAS

-Caso particular del sistema eléctrico-

IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL JUNTO A LAS YA NO TAN NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, EN RELACIÓN A LA SEGURIDAD DE INFRAESTRUCTURAS ESTRATÉGICAS

-Caso particular del sistema eléctrico-

Resumen: En la actualidad hay dos elementos que se erigen como pilares tecnológicos de la civilización. Por una parte, las fuentes y generación de energía, por otra parte, la información. Ambos elementos, energía e información junto a las complejas tecnologías para su generación, gestión, distribución y consumo no son ajenos a la seguridad.

Los nuevos algoritmos y paradigmas en relación a la Inteligencia Artificial (IA) unido a la alta capacidad de computación conseguida, ha provocado una irrupción de la IA en muchos de los órdenes de la vida. Apoyando y asistiendo en la toma de decisiones, cuando no sustituyendo en muchos casos ya, la decisión humana por la decisión de la máquina.

Esta nueva realidad se hace patente e irrenunciable en la gestión de los sistemas y arquitecturas tecnológicas más complejas, algunas prestan los servicios esenciales al ciudadano.

Este estudio pretende abordar distintas visiones como son la visión normativa, técnica y el tecnológica, sobre la irrupción de la IA y las ya no tan nuevas Tecnologías de la Información y la Comunicación (TIC), en uno de los principales sectores estratégicos, el energético, concretamente el sector eléctrico.

Abstract: Currently two elements stand as technological pillars of civilization. On the one hand, the sources and generation of energy, on the other hand, the information. Both elements, energy and information together with the complex technologies for its generation, management, distribution and consumption are not unrelated to security.

The new algorithms and paradigms in relation to Artificial Intelligence (AI) together with the high computing capacity achieved, have caused an irruption of AI in many areas of life. Supporting and assisting in decision-making, when not substituting in many cases already, the human decision for the decision of the machine.

This new reality becomes evident and inalienable in the management of the most complex technological systems and architectures, some of which provide essential services to the citizen.

This study aims to address different visions such as the normative, technical and technological vision, on the irruption of AI and the not so new Information and Communication Technologies (ICT), in one of the main strategic sectors, energy, specifically the electricity sector.

Palabras clave: Inteligencia artificial, infraestructuras críticas, servicios esenciales, sector eléctrico, ciberseguridad, seguridad física, resiliencia.

Keywords: Artificial intelligence, critical infrastructures, essential services, electricity sector, cybersecurity, physical security, resilience.

1.- INTRODUCCIÓN

La civilización actual no es concebible sin la información y ésta, en gran medida, no es concebible sin la electricidad. Es más, sin la electricidad las distintas cadenas de suministro de bienes y servicios que se disfrutan no serían posibles.

Si hubiera un fallo eléctrico a gran escala y una duración en el tiempo de tan solo una semana, provocaría un fallo sistémico en cascada en el funcionamiento de la cadena de suministros de múltiples sectores y por ende en la prestación de servicios y productos esenciales. La seguridad pública se vería seriamente comprometida. (Ledo Iglesias, 2019)

No se tendría acceso a formas de pago electrónico, éste estaría fuera de servicio desde el primer momento, el medio de pago en efectivo se agotaría rápidamente para gran parte de la población. No se podría notificar las incidencias, los accidentes en tiempo real para su atención. Los sistemas de información y telecomunicación al principio funcionarían de forma muy precaria y limitada alimentados por generadores eléctricos que estos se alimentarían de combustibles sólidos, difícilmente proveer y de mantener tantos días al nivel que demandaría un centro urbano de medio tamaño. Impensable para grandes urbes e infraestructuras como los puertos, aeropuertos, estaciones, centros de producción, entre otros.

El acceso a los alimentos, el agua, la sanidad, a la administración, la sanidad e incluso a otras fuentes de energía. En definitiva, todos los servicios esenciales se verían seriamente comprometidos, cuando no anulados. Ante este escenario la situación se tornaría difícilmente sostenible para los poderes públicos en términos de seguridad pública.

Se puede intuir, de lo anteriormente expuesto, que la generación, distribución y acceso o consumo de la electricidad se ha convertido en un proceso de vital importancia. Todo este proceso se desarrolla en el ámbito del sector eléctrico.

Los sistemas que permiten la cadena de suministro desde la producción hasta el consumo de electricidad, se sustenta en complejas arquitecturas tecnológicas. Esta

complejidad gestionada y dirigida por el componente humano, paulatinamente ha ido evolucionando hacia una gestión con menos intervención humana, hasta la mera gestión y supervisión sin su anuencia.

A tenor de la importancia del sector eléctrico, la provisión de seguridad tanto física como lógica al mismo, en sus elementos e infraestructuras, en los procesos y en los servicios asociados se muestra de una importancia capital.

Es en esta seguridad y en la transformación digital de la operación del sistema eléctrico donde la inteligencia artificial (IA) irrumpe creando un nuevo escenario y disruptivo. Tal es así que seguramente constituirá un factor importante en la incipiente 4ª revolución industrial.

2.- EL SISTEMA ELÉCTRICO, INFRAESTRUCTURA ESTRATÉGICA

La Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, se traspone al ordenamiento jurídico español por medio de la Ley 8, 2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC) y ésta a su vez se ve desarrollada por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (RPIC).

Cabe mencionar que la Directiva 2008/114/CE, ha sido sustituida y derogada por la Directiva (UE) 2022/2557, del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas, que ha entrado en vigor el pasado día 16 de enero y será aplicable desde el día 18 de octubre de 2024, debiendo cumplirse, por tanto, no más tarde del día 17 de octubre de 2024.

En la ley LPIC, a lo largo de la redacción del artículo 2, se desarrolla las definiciones a efectos de dicha Ley, estableciendo que se deberá entender:

"Infraestructura estratégica: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales", Artículo 2.d de la LPIC[1].

Considerando servicio esencial "el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas." Artículo 2.a de la LPIC.

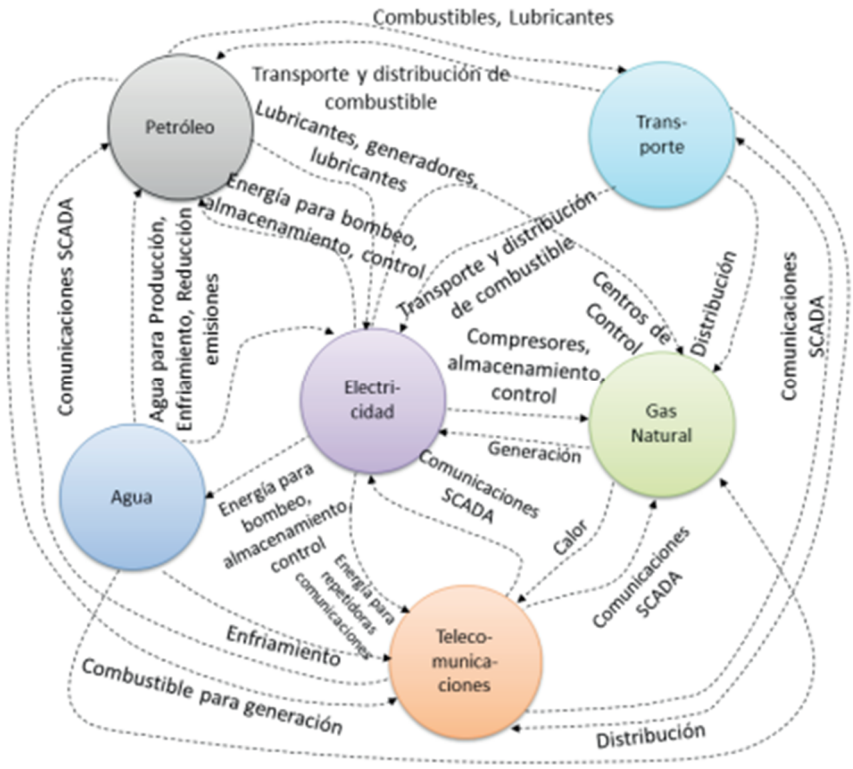
Avanzando en el concepto de infraestructura estratégica hacia el de infraestructura crítica, como aquellas "infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales" (Ledo Iglesias & Martínez, 2020)

[1] Accesible a través de la Página del Boletín Oficial del Estado (BOE) en el enlace https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

Identificados y relacionados entre sí los conceptos y naturalezas de la consideración de servicio esencial, infraestructura estratégica e infraestructura crítica. Puede entenderse que no todo los elementos e instalaciones del sector eléctrico son una infraestructura crítica; algunas lo serán porque su funcionamiento sea indispensable y no sustituible, otras podrán ser sustituidas por la entrada en servicio o suplir la prestación del servicio por otras.

Igualmente es claramente identificable, que el conjunto de elementos, sistemas e instalaciones que operan en el sector eléctrico, se constituirán muchas de ellas como infraestructuras estratégicas, por el servicio que prestan, ya tratado anteriormente que para su funcionamiento interactúa y depende de otras infraestructuras estratégicas e incluso infraestructuras críticas, como puede inferirse claramente de la imagen 1.

Imagen 1. Interdependencia del sector eléctrico de otras infraestructuras críticas



Fuente (Jaime Correa-Henao & Yusta-Loyo, 2013)

Es preciso aclarar, por rigor terminológico y no conducir a errores conceptuales, que en el ámbito de la LPIC, que define en su artículo 2.b, al "sector estratégico como cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma."

"El sistema energético español, se asienta sobre tres grandes sectores: electricidad, gas natural y petróleo" (Estrategia de Seguridad Energética Nacional, 2015, pág. 14)

3.- EVOLUCIÓN DE LA CADENA DE SUMINISTRO DEL SECTOR ELÉCTRICO HACIA UN MODELO DE REDE ELÉCTRICA INTELIGENTE O SMART GRID

El sistema eléctrico es una de los sistemas más complejos construidos por el hombre, en el que los elementos, subsistemas e infraestructuras dedicados realizan la producción, el transporte, la distribución, el almacenamiento y la comercialización de la energía eléctrica hasta los puntos finales de consumo.

En estos procesos son desarrollados por las denominadas Tecnologías de Operación (OT, por sus siglas en inglés) y para gestionar la eficacia y en gran medida eficiencia de su funcionamiento se ha ido haciendo más uso de las Tecnologías de la Información (IT, por sus siglas en inglés). Esta sinergia de los dominios de OT e IT, no es baladí.

Tradicionalmente, hasta comienzos del presente siglo, el modelo de cadena de suministro del sistema eléctrico era un modelo estable y bien definido, en el que la energía eléctrica se producía en unos centros de producción, se transportaba la energía eléctrica desde esos puntos de producción hacia unos puntos intermedios de distribución como son las centrales y estaciones de alta tensión, a otros puntos como las subestaciones de media y baja tensión y de ahí hacia los puntos de consumo.

Era claro los operadores que actuaban en cada parte del proceso, había unos operadores que producían la energía eléctrica, otro operador el transporte y distribución, en el caso español es la empresa Red Eléctrica de España; finalmente una serie de operadores que comercializaban la misma a unos consumidores.

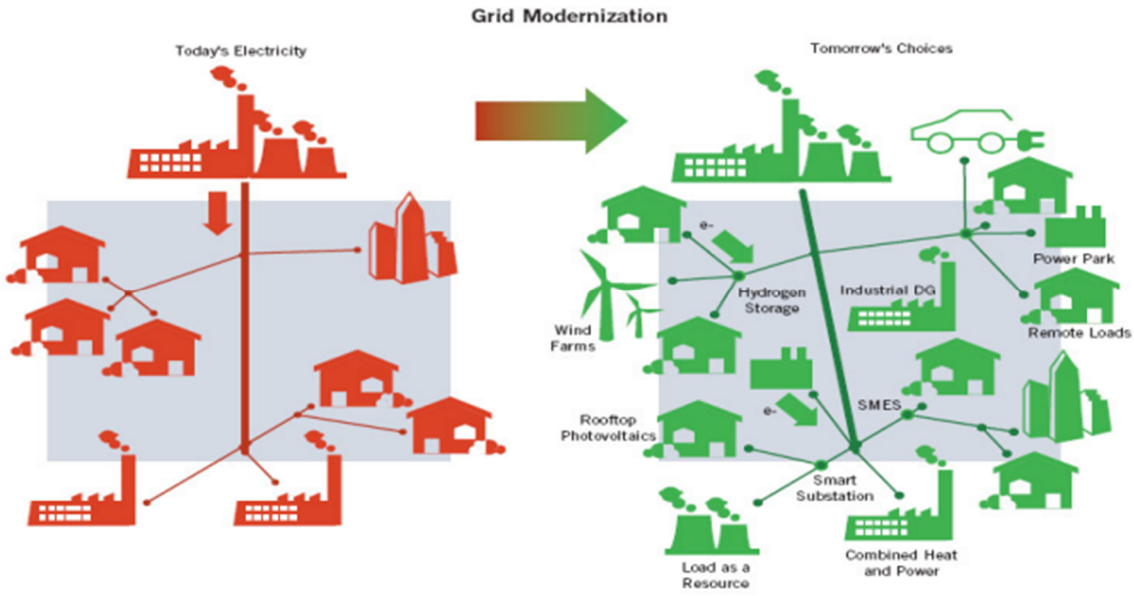
En la actualidad, con la evolución de las fuentes y tecnologías de generación de energía eléctrica, surge la posibilidad que muchos de los hasta entonces consumidores puedan producir energía eléctrica, tanto para su autoconsumo como para inyectar los excedentes en el sistema eléctrico para ponerlo a disposición del resto de operadores.

Para (Alonso et al., 2021) “Las nuevas redes eléctricas inteligentes son complejos sistemas ciberfísicos en los que interaccionan los tradicionales sistemas físicos de generación, distribución y transporte de la energía eléctrica, con las Tecnologías de la Información y Comunicación (TIC) empleadas para la captación de medidas, comunicación y procesado de la información en tiempo real. La integración de la nueva infraestructura cibernética con la infraestructura eléctrica tradicional abre un nuevo abanico de posibilidades, pero a la vez aparecen una serie de problemáticas en materia de seguridad.”

Se evoluciona desde un modelo de puntos de producción centralizado hacia un modelo en el que los puntos de producción y consumo pueden cambiar dinámicamente, adoptando ambos roles al mismo tiempo o en un momento dado uno u otro rol, bien de productor, bien de consumidor, ver Imagen 2. Sin planificación o programación previa, de forma totalmente dinámica y espontánea.

Salvaguardar la estabilidad y seguridad del sistema eléctrico en estas nuevas circunstancias, así como la gestión de la propia producción y consumo se ha convertido en un requisito irrenunciable.

Imagen 2. Evolución del modelo productivo-consumo eléctrico clásico a una red eléctrica inteligente o Smart Grid.



Fuente (Kienle & De Schryver, 2012)

El modelo eficaz de producción eléctrica persigue que siempre que haya una demanda energética, haya electricidad para poder satisfacerla. Ahora bien, el modelo productivo eficaz y eficiente debe perseguir que siempre que haya una necesidad energética se satisfaga, pero no en perjuicio de una sobreproducción energética que haya que desperdiciar. Este anhelo no es baladí y es casi imposible de cumplir dado la cantidad de circunstancias e imponderables a tener en cuenta. Desde que no haya viento y no funcionen parte de los parques eólicos o que no haya suficientes horas de sol para que las granjas fotovoltaicas produzcan la energía en las cantidades necesarias a la concurrencia de eventos multitudinarios como conciertos, partidos e incluso movimientos sociales que proponen acciones multitudinarias como no encender las luces o reducir el consumo un día determinado a unas horas determinadas, etc.

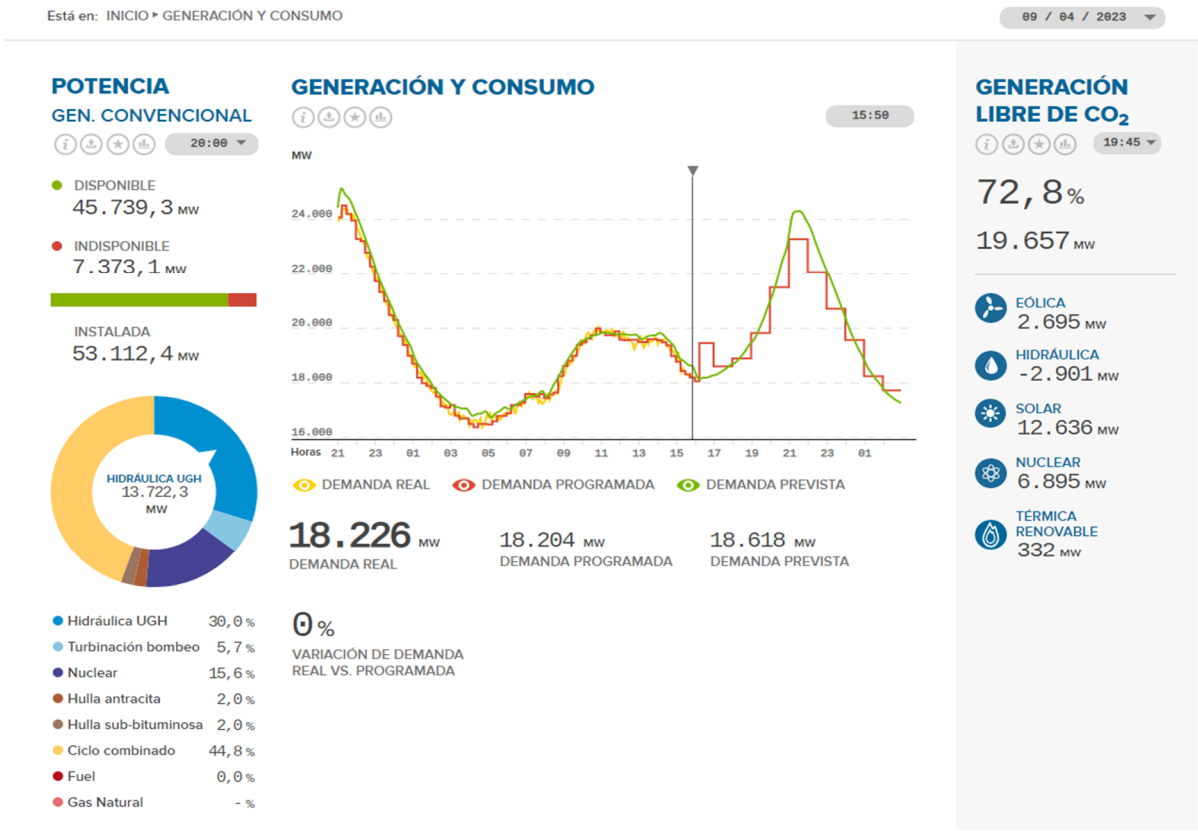
La capacidad estimada en la red española de poder almacenar la energía excedentemente producida se estima en torno al 15%.

Hacer coincidir el consumo eléctrico esperado, la energía eléctrica producida (y con qué fuentes renovables, nuclear, etc.) y el consumo real, es una labor que no podría realizarse de no tener una alta sensorización de la infraestructura eléctrica, una alta capacidad de cálculo y procesamiento unido a técnicas de Inteligencia Artificial. Esto es necesario para poder medir, analizar y reaccionar en tiempo real para producir la energía necesaria utilizando los medios de producción y transporte de la forma más económica y sostenible, desde el punto de vista medioambiental, posible.

Esta correlación de medición del consumo y peticiones de electricidad en tiempo real, su análisis y confrontación con las estimaciones realizadas, junto a la capacidad reactiva para la producción y transporte de la electricidad puede consultarse en tiempo

real en la página Web de Red Eléctrica de España[2] (REE), un resultado referido al día 9 de abril de 2023, es visualizado en la imagen 3.

Imagen 3 Consulta producción, consumo eléctrico estimación y real.



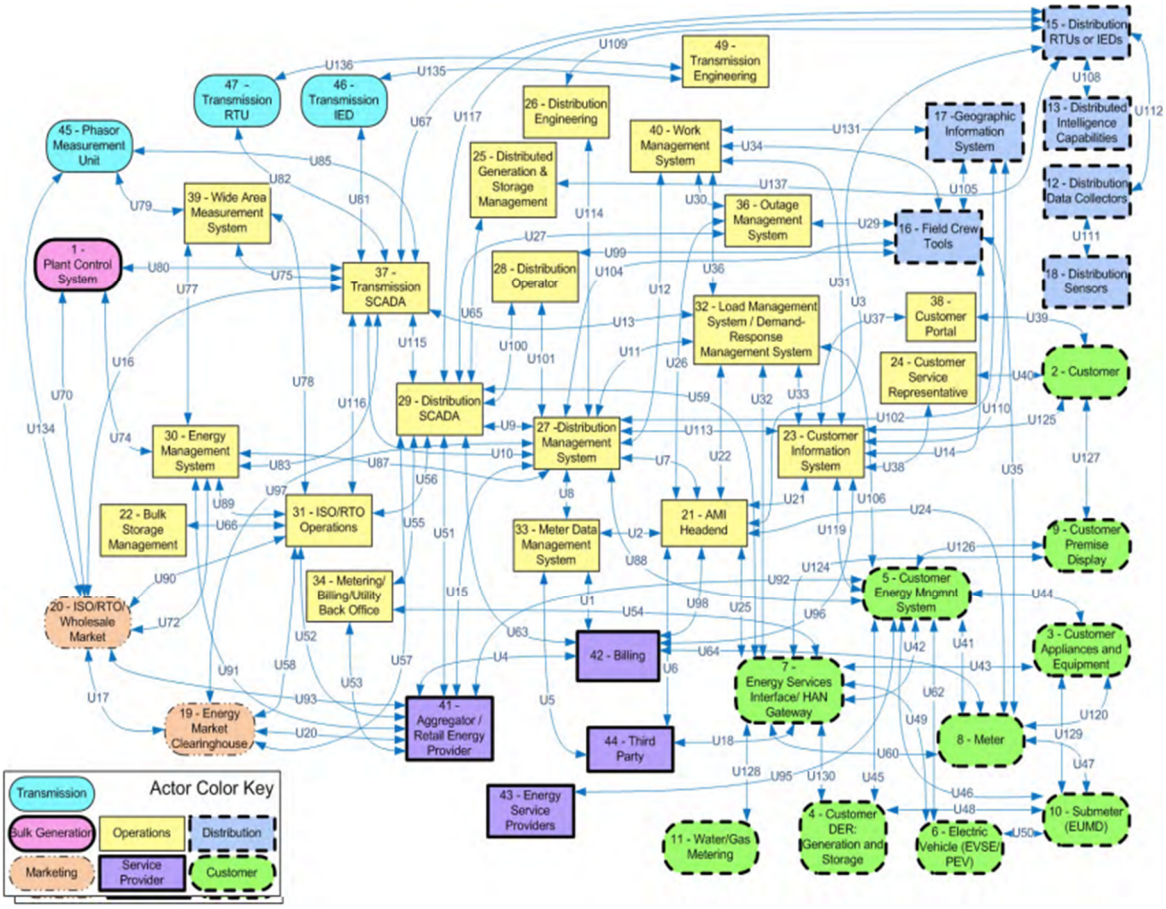
Fuente (REE)

4.- INTELIGENCIA ARTIFICIAL, ESTADO DEL ARTE, CAPACIDADES Y REGULACIÓN EUROPEA Y NACIONAL.

Ya se ha comentado la complejidad del sistema eléctrico. No es una elección, es una necesidad el disponer de una segmentación y automatización tanto en la medición de la producción y parámetros de control de los elementos ciberfísicos que interactúan en el sistema. Una representación gráfica de las distintas tecnologías implicadas, que interactúan entre sí, mostrando la complejidad de la definición lógica del sistema, puede apreciarse en la imagen 4.

[2] https://demanda.ree.es/visiona/peninsula/nacional/total última consulta producida el día 13 de abril de 2023.

Imagen 4 Modelo de referencia de la interacción lógica de sistemas en una red inteligente.



Fuente (NISTIR 7628[3], pág. 17)

4.1.- Estado del arte de la IA

Para poder adquirir la ingente cantidad de información generada, almacenarla, procesarla y gestionarla se ha estado realizando a través de incipientes tecnologías de la revolución industrial 4.0, como el Data Mining (DM, o minado de datos en español que hace referencia al conjunto de técnicas y tecnologías orientadas a la exploración de información en grandes repositorios de datos, no necesariamente estructurados o almacenados en bases de datos relacionales) o el Bussiness Intelligence (BI), también conocida como la inteligencia de negocios, utiliza herramientas de minería de datos, visualización e infraestructuras de datos y herramientas, orientadas a la ayuda a la toma de decisiones . Si bien, ya no es suficiente por los nuevos paradigmas que surgen, en los que ya no solamente se persigue encontrar patrones u obtener respuestas a cuestiones concretas, debiendo hacer uso de técnicas como Big Data (BD). Utilizándose este término anglosajón, por lo estandarizado en el uso de la bibliografía técnica, si bien se corresponde con las expresiones en español "macrodatos", "datos masivos" o "datos a gran escala", el

[3] Recuperable desde la página Web https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf , recuperado por última vez el día 13 de abril de 2023.

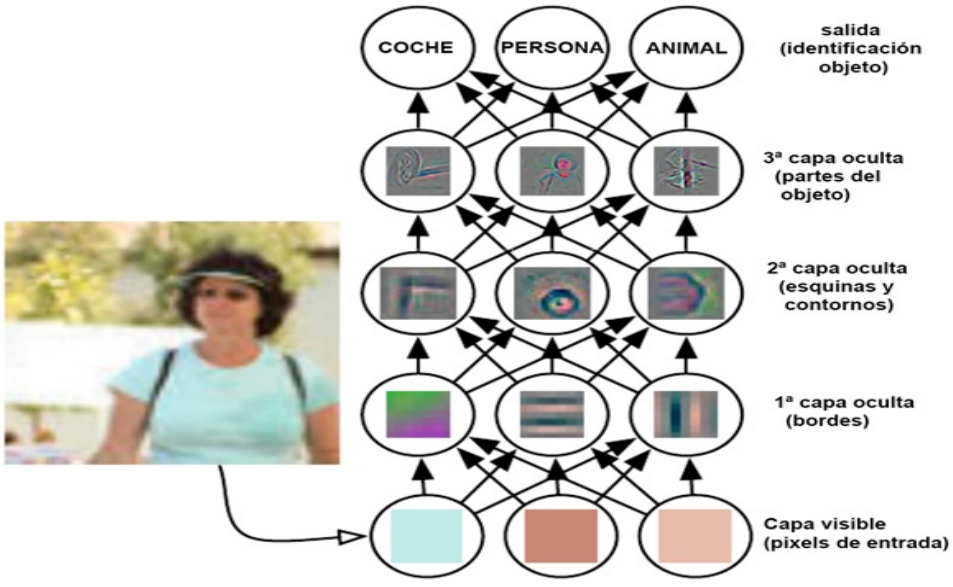
mismo hace referencia a un gran conjunto de datos complejos y a las tecnologías específicas en el ámbito de las TICs para su tratamiento.

Se precisa poder ir más allá en la mera automatización de acciones de respuesta ante unos eventos determinados, donde una causa ya contemplada, identificada se ha digitalizado el procedimiento y acción de respuesta ante la misma. Así ante una misma causa, la acción será la misma, pero no realimentará el sistema ante nuevas causas o las podrá relacionar con otras distintas.

La IA, es la disciplina perteneciente al ámbito de la ingeniería informática y de las ciencias computacionales que permite crear algoritmos que emularían las acciones que realizaría la mente humana con un aprendizaje y razonamiento lógico. Para esto es preciso que el sistema pudiera aprender por sí mismo, mediante disciplinas como el aprendizaje profundo o Deep Learning, (DL, por sus siglas en inglés) para lo que se utilizan redes neuronales y el aprendizaje máquina o Machine Learning (ML, por sus siglas en inglés) en el que se busca la identificación de patrones de datos. De esta manera la IA es capaz de emular acciones y toma de decisiones como lo haría un humano.

El DL es capaz, a través de las redes neuronales, de realizar acciones utilizadas en tecnologías en el ámbito de la seguridad, tanto física como lógica. Así es utilizado para reconocimiento biométrico (decadactilar, iris, venas, facial, voz), de caracteres, textos, imágenes, objetos, entre otros. Un ejemplo de funcionamiento del proceso de discriminación de objetos por una red neuronal sería el mostrado en la imagen 5.

Imagen 5. Proceso de discriminación de objetos utilizando una red neuronal.

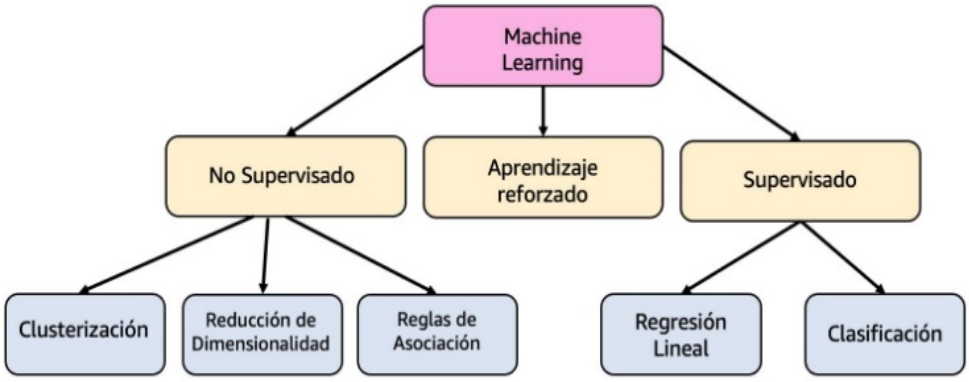


Fuente (Goodfellow et al., 2016)

Con el aprendizaje automático, dentro del ML, aparecen distintos paradigmas que permitirán procesar la información transformando ésta en conocimiento. Para esto el ML, utiliza algoritmos que se pueden clasificar en tres grandes grupos:

- El aprendizaje no supervisado. En este caso no se conocen los valores de las variables y las etiquetas de entrada ni de salida. El modelo es entrenado utilizando técnicas como la clusterización, reglas de asociación y reducción de dimensionalidad.
- El aprendizaje supervisado. Se entrena al modelo mediante la utilización entradas de variables y etiquetas conocidas, puede aprender de los errores cometidos, funcionando bien por clasificación o por regresión lineal. Analiza qué relación existen entre los datos de entrada (inputs) y los datos de salida (outputs), enseñando a los algoritmos el resultado deseado para una determinada entrada. Permitiendo encontrar resultados incluso para valores no mostrados antes al algoritmo. El proceso requiere de un entrenamiento prolongado, exhaustivo y sobre todo cuantioso. Cuantos más ejemplos de uso y discriminación de datos se aporten al modelo, mejor y más rápido será su aprendizaje.
- El aprendizaje por refuerzo. Este tipo de aprendizaje se basa en una serie de castigos, recompensas que recibe el agente de ML por las acciones que realiza en la interacción con su entorno. Aprendiendo el agente por exploración con su entorno y los premios que recibe por sus acciones con el entorno. (Li et al., 2021)

Imagen 6. Técnicas de aprendizaje de ML



Fuente Amazon Web Services, (aws)[4]

Hay tareas que los humanos realizan de forma instintiva, sin tener conciencia del por qué es, pero es capaz de reconocer intuitivamente las relaciones entre objetos y tomar decisiones y acciones consecuentes. La IA, mediante el ML, al final encuentra los patrones de relaciones y es capaz de aplicarlos, no intuitivamente, sino porque ha encontrado patrones. Estos pueden ser absolutos y probabilísticos, pero son útiles en la mayoría de las ocasiones, haciendo que la IA cada vez sea más fiable.

El aprendizaje supervisado utiliza la regresión para predecir un valor continúo y la clasificación para predecir una clase o una categoría. El aprendizaje por refuerzo enseña a la IA qué acciones debe escoger un agente software en un determinado entorno, para obtener o maximizar el premio acumulado. Por el contrario, el aprendizaje supervisado, persigue la producción de conocimiento tan sólo con los datos suministrados, los "inputs", sin condicionar o explicar a la IA el resultado esperable. En este caso, la IA trabaja buscando similitudes entre los inputs para poder encontrar patrones y crear predicciones

[4] Imagen recuperada de https://aws.amazon.com/es/blogs/aws-spanish/introduccion-artificial-intelligence-y-machine-learning-para-desarrollares-de-aplicaciones/ último acceso, el día 13 de abril de 2023.

futuras. Los inputs no deben estar etiquetados, requiere de una cantidad muy grande de inputs para poder sacar conclusiones.

Actualmente el uso del método de aprendizaje no supervisado está infrautilizando en relación al supervisado. Si bien, con la mejora de los algoritmos y la evolución de la capacidad de cálculo y su abaratamiento; permite inferir que dado el coste de tener un humano continuamente etiquetando la información para alimentar el modelo de IA con el paradigma supervisado, se vea superado en un futuro, tendiendo al modelo de aprendizaje no supervisado. (Salimans et al., 2016)

El aprendizaje no supervisado se sirve de distintas técnicas para su aprendizaje como es el clustering, la asociación, la detección de anomalías, la minería de secuencia, la reducción de dimensión o el sistema basado en recomendaciones (Baviera, 2017)

Para conseguir resultados de modelos predictivos, en la actualidad tanto la programación como el entrenamiento de estos modelos están basados, fundamentalmente, en algoritmos ya existentes que se van reajustando utilizando el paradigma del aprendizaje automático supervisado. Algunos de los modelos utilizados son "Naive Bayes[5]", "árboles de decisión" también conocidos por DT (por sus siglas en inglés, Decision Tree) que es una técnica de clasificación, su potencial y utilización es muy grande en contextos muy dispares, en común todos ellos tienen, la necesidad de predecir los datos de salida en base a los datos de entrada. Una mejora de este último modelo son los "bosques aleatorios" y las "redes neuronales"[6].

4.2.- Aplicabilidad de la IA a la gestión de la red

La transformación y la digitalización en el sector eléctrico, no es un fenómeno reciente. Los elementos y los componentes de control y gestión son muy costosos y tienen un ciclo de vida prolongado, hay sistemas de control industrial que pueden estar perfectamente activos más de veinte años. Su sustitución y su automatización es un proceso continuo en este sector, si bien son miles los sensores y dispositivos que están funcionando y funcionando bien, muchos de ellos muy orientados al entorno OT, como se ha explicado anteriormente.

Por esto, el grado de penetración de las distintas tecnologías, entre ellas la incorporación de la transformación digital convergiendo los entornos IT y OT para su gestión, se ha está realizando por importancia de las redes. Se ha avanzado mucho en las redes de alta y media tensión, no habiéndose avanzado tanto en las redes de "última milla".

La aplicación de la IA en el sector eléctrico está aportando una mejora en los medios de gestión tradicionales, máxime con la digitalización de la red y está aportando la integración inteligente basado en factores muy distintos, logrando la convergencia eficiente de sistemas antiguos con sistemas nuevos, optimizando la gestión. Un ejemplo ya visto es la integración de los distintos factores contemplados para realizar la predicción

[5] Basados en la teoría Bayesiana para el cálculo de probabilidades de pertenencia de los datos a los grupos asignados según sus etiquetas.

[6] Según sea la infraestructura puede ser de interés utilizar redes neuronales clásicas basadas en distintas capas, redes neuronales convolucionales, o las redes neuronales recurrentes (Alom, Md et al, 2019).

de carga del sistema visto en tiempo real, convirtiéndose en un sistema crítico, como se ha mostrado en la imagen 3.

En ese ejemplo se podía apreciar, las distintas fuentes de energía, contribuyendo a la eficiencia energética y a la sostenibilidad. Otro ejemplo es el proyecto EA2, del Instituto de Ingeniería del Conocimiento (IIC, de la Universidad Autónoma de Madrid), orientado a dar soporte de decisión en la producción de energía eólica, pudiendo predecir la previsión climatológica con un rango de 12 a 48 horas.

Cada vez más se irá instaurando la IA en la gestión y explotación de la red eléctrica para poder permitir una mejor predicción del consumo y producción de energía, permitir una descentralización del control, poder gestionar más factores de control y estado del Sistema Eléctrico de Potencia (SEP), permitir una mayor adaptabilidad, robustez y fiabilidad del sistema.

En la actualidad la arquitectura de los distintos centros de producción, transporte y transformación, incluye muchos elementos de medidas y de control, incorporando los dispositivos electrónicos inteligentes (IEDs, por sus siglas en inglés), muy utilizados en toda la infraestructura eléctrica y muy especialmente en las subestaciones eléctricas, que vinculados entre sí por medio de la red local y de forma global por la interconexión del sistema. Esto ha sido posible, gracias al avance e incorporación de las redes informáticas en este entorno de operación. Antaño funcionaban de forma independiente en cada instalación, pero cada vez más se han incorporado a la estructura global, haciendo uso de la IT, para su gestión, teniendo terminales de control remota digitales (RTUs, por sus siglas en inglés). Esto ha provocado que la cantidad de información entre mediciones, comandos y alarmas, a gestionar sea enorme. Teniendo que almacenar los datos en medio de almacenamiento pasivo, y utilizar las ya mencionadas técnicas de Big Data e IA para su tratamiento.

De especial importancia ha sido la introducción de agentes inteligentes en los elementos de control y monitorización. Entendiéndose como tales, aquellas unidades computacionales situados en los elementos de control del sistema eléctrico que están provistos de autonomía, desarrollando sus tareas sin intervención humana, teniendo su propio control interno y la capacidad de actuación en el medio desplegado. Trabajan de forma conjunta y coordinada, reportando, información e inteligencia al sistema de la IA para una gestión más desatendida y eficiente. El reto de estos agentes inteligentes estriba en el modelado de a toma de decisiones y en el diseño de la arquitectura en cómo van a trabajar con el entorno y entre sí, confiriendo una reactividad y una pro-actividad eficaz en la utilización de los sistemas multiagente (SMAs,)

Las características básicas de la plataforma multiagente están definidas por la Foundation for Intelligent Physical Agents (FIPA, por sus siglas en inglés), actualmente, incorporado como el undécimo comité de estándar del IEEE (Instituto de Ingeniería Eléctrica y Electrónica, por sus siglas en inglés), en el año 2005[7].

[7] Más información puede ser visualizada en su página Web oficial en el siguiente enlace http://www.fipa.org/ , última visita el día 14 de abril de 2023.

Los SMAs, son muy utilizados fundamentalmente para la gestión del entorno del mercado eléctrico, el control en tiempo real, integración de fuentes y generadores de energía y la operatividad global en la red.

4.3.- Aplicabilidad al mantenimiento

La utilización de la IA en el mantenimiento de los sistemas, puede aportar una mayor estabilidad en la red, menores tiempos de fuera de servicio y una mejora en toda la cadena logística del sistema.

Se puede realizar simulaciones predictivas de fallo de componentes para enseñar a los modelos qué acciones tomar. Para Miguel Angel Fernández Céspedes, manager experto en el Sector Energías Renovables de Stratesys,

"la aplicación de la IA mejora la eficiencia en el sector de las energías renovables, reduciendo el coste de mantenimiento en sus instalaciones. Por ejemplo, especifica que tecnologías como Machine Learning y Deep Learning permiten "recopilar información a través de las redes de sensores ubicados en las instalaciones, con el fin de anticipar averías y alargar la vida útil de las mismas. Se aumenta la vida útil de los equipos, puesto que se anticipan posibles averías y se reducen los traslados del personal de mantenimiento a las plantas. Y el hecho de saber, y anticipar, las averías más recurrentes y las piezas que sufren mayor desgaste, hace que haya menos estrés de repuestos y se reduce el stock de aquellos menos necesarios"[8]

Algunos ejemplos de estas implementaciones utilizando IA en el mantenimiento reactivo y preventivo son el proyecto "Pastora"[9] o el Acuerdo entre Siemens Gamesa Renewable Energry con la IA y la nube de Microsoft, para el mantenimiento preventivo y correctivo de las palas de los rotores de los aerogeneradores de parques eólicos[10], pudiendo recomponer todas las fotografías que realizaba un dron con el aerogenerador parado y realizar un visionado del estado del mismo en 24 minutos, identificando distintos tipos de fallos de distinta gravedad, que será supervisado por el equipo técnico y eventualmente escalado a un ingeniero para su tratamiento.

Un ejemplo notable de la aplicación de la IA, para la ayuda del mantenimiento de la infraestructura de operación en el sistema eléctrico es el proyecto BD40PEM[11], de la Universidad Politécnica de Cataluña, dotado con casi 10 millones de euros, en el marco del proyecto H2020 de la Unión Europea, cuya fecha de finalización está fijada para el día 30 de junio del presente año 2023. Entre sus logros está la detección de errores de

[8] Obtenido como cita en el artículo de la página Web https://aserta.com.es/inteligencia-artificial-en-el-sector-energetico/ recuperado el día 14 de abril de 2023.

[9] Proyecto capitaneado por Endesa, para el control y el mantenimiento preventivo de la red de distribución, extraído de la Web del proyecto https://www.endesa.com/es/proyectos/todos-los-proyectos/transicion-energetica/redes-inteligentes/pastora-inteligencia-artificial-red-distribucion , recuperado el día 14 de abril de 2023.

[10] https://news.microsoft.com/es-es/2019/04/05/siemens-gamesa-renewable-energy-crea-un-futuro-mas-sostenible-con-la-energia-eolica-la-ia-y-la-nube-de-microsoft/ , recuperado el día 14 de abril de 2023.

[11] BD40PEM, Big Data for Open innovation Energy Marketplace. La información de este Proyecto puede ser consultada en la página Web del mismo en la Unión Europea, en el siguiente enlace https://cordis.europa.eu/project/id/872525/es , fecha de última recuperación 14 de abril de 2023.

medida, análisis de topología y monitorización de redes de baja tensión, así como la realización de mantenimiento predictivo.

4.4.- Aplicabilidad en la seguridad física de acceso a la infraestructura del SEP.

Se ha tratado ya la importancia e irrupción de la IA en la seguridad de los elementos de control y operación (OT) del SEP. Ahora bien, la irrupción de la IA en los sistemas de seguridad física y de control de acceso, sin que sea un uso particular en el sistema eléctrico, más bien se ha incorporado como algo transversal a cualquier infraestructura, se ha convertido en un hecho muy notable. En la actualidad la gestión de la seguridad física y protección de las numerosas instalaciones tanto de generación, transporte, distribución y transformación de la energía eléctrica, ha venido en poder homogenizar realizar la gestión de dicha seguridad, de una forma mucho más eficiente. Ha permitido poder incluir distintos operadores de seguridad privada, que pueden desplegar una mayor cantidad de detectores de intrusión y sabotaje en las mismas, facilitando la neutralización de las distintas amenazas contra las instalaciones. Especialmente acentuadas en los últimos tiempos con el robo de cobre, que aparte de suponer un perjuicio económico, provoca no pocos problemas de seguridad en la operación y suministro de electricidad.

Así la utilización de la IA en los sistemas de seguridad física, como es el control de acceso físico mediante biometría (reconocimiento facial, vehículos, personas en listas blancas, personas en listas negras, etc.) o en la propia gestión y reconocimiento de las alarmas que procesan los distintos subsistemas de seguridad, para maximizar la probabilidad de detección de los mismos (Pd) y a su vez minimizar al máximo las falsas alarmas recibidas (índice FAR), utilizando para ello el ML en forma supervisada, son claros ejemplos de los beneficios que ha supuesto en la gestión y operación de los sistemas de seguridad en las instalaciones del sector eléctrico.

Con la digitalización de los sistemas de video vigilancia, su interconexión y el almacenamiento masivo de la imagen en formato digital y codificado en medios de almacenamiento masivo, ha permitido junto a los avances en IA y en computación, avanzar en los algoritmos de análisis, reconocimiento y aprendizaje. Así, se puede realizar reconocimientos de objetos, personas, animales. Estas capacidades no se han limitado al ámbito de la seguridad física y su monitorización, ha evolucionado para integrar la información de los sistemas de seguridad con otros como los de recursos humanos, facturación, logística, prevención de riesgos laborales, gestión de activos, etc. Aportando un alto valor en toda la cadena de suministro de distintos sistemas al aprender y tomar decisiones en tiempo real y de carácter predictivo.

4.5.- Aportación de la IA a la ciberseguridad de los sistemas IT y OT del sistema eléctrico.

En este trabajo se entiende por ciberseguridad como el conjunto de políticas, medidas, herramientas y procedimientos a garantizar la información y los sistemas en los que se almacenan, procesan y transmite la información. De forma determinada en relación a cinco dimensiones como son la confidencialidad, la disponibilidad, la integridad, la trazabilidad y la autenticidad de la información.

Se ha tratado ya el proceso de digitalización del sector eléctrico y como convergen, sobre todo a partir de la cuarta revolución industrial las infraestructuras IT y OT, en todos los sectores y el sector eléctrico no es anejo a este cambio disruptivo. Si los sistemas de

OT, estaban relativamente protegidos, por un aislamiento de los sistemas, la especificidad de sus sistemas, por un uso de protocolos propietarios del fabricante en su gran mayoría. La irrupción de la telecomunicación y gestión, unido a la necesaria estandarización de los sistemas OT, hizo que su sinergia con la IT fuera de una gran productividad y evolución tecnológica.

No todo han sido parabienes, la parte negativa de esta sinergia es que también se hereda las amenazas, vulnerabilidades y riesgos asociados a las IT, de las que tradicionalmente las OT, por lo anteriormente expuesto se venía abstrayendo. Con la interacción y sinergia de las IT y las OT, esta relativa seguridad desparece. Desaparece además de una forma traumática porque si bien las IT, han lidiado con los problemas de ciberseguridad, también es mucho más maduro, las estrategias, políticas, métodos, procedimientos y herramientas orientadas a la ciberseguridad.

Los sistemas OT, no tienen ese nivel madurativo, asociado a que el parque de dispositivos de medición y control es muy numeroso, heterogéneo, con sus propios protocolos y características no tan estandarizadas y con un ciclo de vida que se puede prolongar a varias décadas, en algunos casos.

Los sistemas cyber-físicos, basado en elementos de control, como los ya mencionados agentes inteligentes, SMAs, también tienen otros elementos más de control y supervisión como son los sistemas de control industrial (ICS, Industrial Control System, por sus siglas en inglés). Estos sistemas engloban a sistemas implantados en áreas ampliadas como los sistemas de supervisión, control y adquisición de datos (SCADA, por sus siglas en inglés), y los sistemas de control de distribuidos (DCS, por sus siglas en inglés). Estos sistemas existían ya hace 20 años, pero no estaban preparados para trabajar de forma telemática y remota o interconectando redes de centros. En la actualidad estos sistemas han evolucionado no solo para contemplar las mediciones y el control OT, sino que son capaces de trabajar con elementos de control inteligentes propios de la tecnología IT, como son los sistemas cortafuegos (Firewire, en inglés), sistemas de detección de intrusiones (IDS, por sus siglas en inglés), sistemas de prevención de intrusiones (IPS, por sus siglas en inglés) o sistemas de información y gestión de eventos (SIEM, por sus siglas en inglés).

En este escenario en el que se genera una ingente cantidad de información que provienen de todos los sistemas de medición y control tanto de IT como de OT, irrumpe las tecnologías de IA como son los Big Data, el Machine Learning y el Deep Learning, convirtiendo a los sistemas en sistemas expertos, con capacidad de reaccionar en tiempo real, aprender de los distintos incidentes y patrones que suceden para prevenir y adoptar autónomamente nuevas medidas que ayudan a proteger tanto a los sistemas IT como los sistemas OT de los ataques de ciberseguridad. Amenazas tan importantes como son el ransomware o las APTs, puede comprometer muy seriamente los sistemas, en el objeto de estudio, los sistemas del sector eléctrico.

Ya ha ocurrido con éxito, ciberataques en el sector eléctrico y haciendo patente la interrelación de los sistemas ciberfísicos y cómo un ataque meramente informático utilizando fundamentalmente las IT han afectado, llegando a anular el funcionamiento de las infraestructuras OT.

Casos como el ataque sufrido por la planta nuclear de Natanz en Irán, en abril de 2011 mediante el malware Stuxnet[12], que retrasaron el programa nuclear iraní en más de cinco años.

Los ataques sufridos en la red eléctrica de Ucrania en diciembre de 2015, en el que se vieron afectadas más de 225.000 personas como muestra el informe SANS de marzo de 2016 y en el año 2017 con el malware BlackEnergy[13] o el ciberataque que sufrió la red eléctrica de Portugal, a través del operador EdP[14] (Energías de Portugal, S.A.), en el que se ex filtraron 10 TB de información.

En el ámbito del sector eléctrico una guía(Jeffrey A. Marron, Avi M. Gopstein, Nadya Bartol, Larry Feldman, 2019) para implementar un sistema de ciberseguridad en las redes inteligentes, impulsada por el NIST del Gobierno de los Estados Unidos. En el ámbito nacional destacan, la guía de seguridad en protocolos industriales- Smart Grid[15], publicada por el Instituto Nacional de Ciberseguridad (INCIBE), junto a las guías publicadas por el Centro Criptológico Nacional (CCN).

La implementación de IA en ciberseguridad se está realizando en distintos ámbitos, como para la detección automática de amenazas que gracias al aprendizaje automático los sistemas aprenden y se adaptan a las nuevas amenazas pudiendo predecir ataques futuros con variaciones, realizando análisis predictivo, ejecutando acciones de detección, respuesta y recuperación. También son ampliamente utilizadas para apoyo a la decisión, tras adquirir y analizar miles de señales de los sistemas de detección como los IDS. La IA, evoluciona y aprende continuamente, disminuye los tiempos de respuesta y detecta las amenazas con mayor anterioridad, aportando un tiempo extra para la prevención, detección y respuesta ante los ciberincidentes.

Productos como PowerMarc para la protección del servicio de correo electrónico de correos no deseados o tecnologías basadas en IA de IBM, para la adopción de ciberseguridad como son IBM Security QRadar[16] o IBM Advisor with Watson[17] , aportan soluciones integrales basadas en IA, en el ámbito corporativo para la ciberseguridad. La clasificación y cumplimiento de la privacidad de datos, el perfilado de seguridad del comportamiento de usuarios, el perfilado de seguridad en el rendimiento de los sistemas, son otras aplicaciones de la IA y el ML en materia de ciberseguridad.

[12] Información detallada sobre este malware, puede ser consultada en la página Web del Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia, en el siguiente enlace https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/23-noticias/1222-el-gusano-stuxnet-que-afecta-a-sistemas-scada-causa-revuelo-internacional.html último acceso el día 14 de abril de 2023.

[13] https://www.incibe-cert.es/blog/nuevo-ciberataque-red-electrica-ucrania último acceso el día 14 de abril de 2023.

[14] Noticia publicada en algunos medios de seguridad como el diario digital "CincoDías", en el siguiente enlace https://cincodias.elpais.com/cincodias/2020/04/14/companias/1586887179_127560.html último acceso el día 14 de abril de 2023.

[15] Accesible desde el enlace https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_protocolos_smart_grid_2017_v2.pdf último acceso 14 de abril de 2023.

[16] https://www.ibm.com/es-es/products/qradar-siem/addons último acceso el día 14 de abril de 2023.

[17] https://www.ibm.com/es-es/products/qradar-siem/addons#3071036, último acceso el día 14 de abril de 2023.

4.6.- Normalización de la IA.

La IA lleva décadas de historia y evolución desde su aparición, es en estos momentos, en el que se está llegando a la IA cognitiva cuando parece mostrar un inusitado potencial, que si bien se preveía no se tomaba conciencia de su advenimiento. La irrupción de la evolución de la IA cognitiva ha alterado los umbrales de la sociedad creando una fuerte sensación de inestabilidad en relación a su impacto en el actual modelo social, creando una gran incertidumbre en relación a sus verdaderas capacidades y su afectación a los derechos fundamentales de privacidad de datos, morales y jurídicos.

En este sentido la Unión Europea (UE), publicó, a modo de recomendaciones sin efectos normativos, el "Libro Blanco sobre la inteligencia artificial- un enfoque europeo orientado a la excelencia y la confianza", la COM/2020/65 final[18]. Un documento que, si bien contempla los beneficios que aportará la IA en todos los órdenes de la vida de los ciudadanos, reconoce una serie de riesgos potenciales como la opacidad en la toma de decisiones, la intromisión en las vidas privadas o su uso con fines delictivos. Se reconoce una oportunidad para Europa de convertirse en una potencia en esta rama tecnológica, instando a una actuación coordinada para tal fin y para la mejora de la calidad de vida de los ciudadanos. Viene a completar el marco de la Estrategia Europea de Datos, en el que la Comisión ha propuesto más de 4000 millones de euros en el marco del Programa Europa Digital para respaldar la misma.

A raíz del Libro Blanco sobre la IA, se encuentra en este momento una propuesta de Reglamento por el que se establecen normas armonizadas sobre IA, es conocida como la "AI Act"[19], en el que se definen a los sistemas IA, se identifican prácticas prohibidas de IA, los riesgos asociados a usos específicos de la IA, clasificando en cuatro los niveles de riesgos distintos: riesgo inaceptable, riesgo alto, riesgo limitado y riesgo mínimo.

A nivel nacional se ha desarrollado a partir del eje número 4 "Economía del Datos e inteligencia artificial" de la Agenda España Digital 2026[20], la Estrategia Nacional de Inteligencia Artificial[21], en la que se establecen unos objetivos estratégicos a alcanzar por medio de seis ejes estratégicos, que contemplan aspectos como la investigación y el desarrollo tecnológico e innovación en IA. El fomento de capacidades digitales para potencial el talento nacional en IA, el desarrollo de plataformas de datos e infraestructuras tecnológicas que den soporte a la IA, la integración de la IA en las cadenas de valor del tejido económico del país, potenciar el uso de la IA en la administración pública y en las misiones estratégicas nacionales. Por último, se contempla un marco ético y normativo que refuerce los derechos individuales y colectivos, a efectos de garantizar la inclusión y el bienestar social. (Estrategia Nacional de Inteligencia Artificial.2020)

---

[18] Accesible a través del enlace https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0065, último acceso el día 14 de abril de 2023.

[19] La propuesta y sus anexos pueden ser consultados en el enlace https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence último acceso el día 14 de abril de 2023.

[20] Accesible en el enlace https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf último acceso el día 14 de abril de 2023.

[21] Accesible a través del enlace https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf último acceso el día 14 de abril de 2023.

En este sentido, es significativo mencionar la publicación del Decreto Ley autonómico de Extremadura en relación a la IA, (Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. 2023) como norma de rango autonómico. Con objetivos como es el establecimiento de una IA ética, confiable y respetuosa con los derechos fundamentales, elevar la capacitación técnica en IA, fomentar la implantación de la IA en las empresas de la región, entre otros. En su disposición adicional primera, establece la elaboración y aprobación de una Estrategia Extremeña de Inteligencia Artificial.

5.- CONCLUSIONES Y LÍNEAS FUTURAS DE INVESTIGACIÓN

A lo largo del presente artículo, se ha podido identificar el sistema eléctrico como uno de los sistemas más complejos sino el más complejo ideado y construido por el hombre. Se ha expuesto la importancia del sector eléctrico como componente vital de la sociedad actual, concluyendo que el sector eléctrico, forma parte de las infraestructuras estratégicas del país y algunas en particular como infraestructuras críticas, viendo como su afectación produciría una afectación en cascada en infraestructuras estratégicas de la casi totalidad de los sectores estratégicos.

Se ha ahondado en la transformación digital y la confluencia de las IT y OT en los sistemas eléctricos, mostrando la evolución del modelo productivo-transporte-consumo tradicional de la energía eléctrica hacia los sistemas de redes inteligentes de potencia, las denominadas Smart Grids.

La evolución en la cantidad de detectores generando señales y datos, junto a los avances en las capacidades de las redes informáticas y la capacidad de cálculo, ha favorecido la integración de la sinergia e interoperabilidad cada vez mayor entre la IT y OT, surgiendo la IA como una parte irrenunciable de la solución a la gestión, mantenimiento y gobernanza del sistema eléctrico. Ahondando en la aplicabilidad de la IA en estos procesos.

Igualmente se ha podido identificar la relación de la IA con los sistemas de ciberseguridad, sus implicaciones y posibilidades de implementación y explotación en relación al sector eléctrico.

Finalmente, se ha identificado las principales normas e iniciativas normativas tanto a nivel europeo, nacional, con un caso particular de desarrollo y propuesta normativa en el ámbito autonómico, como ha sido el desarrollo del Decreto Ley 3/2023, de la Junta de Extremadura. En el que se puede identificar las preocupaciones y esperanzas que la Unión y el Estado tienen sobre la IA y su irrupción e impacto en la vida de los ciudadanos e instituciones.

El futuro Reglamento de la inteligencia artificial (conocida como la “IA Act”) junto al Reglamento Europeo de Protección de Datos (RGPD), se ciernen como futuros estándares de facto en el ámbito global en materia de gobernanza de la IA.

A tenor de los primeros pasos expuestos en este trabajo, surgen diversas líneas de investigación futura, tanto normativas, éticas, técnicas, tecnológicas y sociales sobre la IA y más concretamente en el sector eléctrico. Se propone la investigación en materia de ciberseguridad en entornos ciberfísicos y la adopción de análisis de riesgos multivariable

en el mismo, la investigación en materia administrativa, civil y penal de la defraudación y mala praxis en el uso de la IA tanto para la prestación del servicio eléctrico como la defraudación y otros efectos perniciosos en el sistema.

BIBLIOGRAFÍA

- Alonso, M., Turanzas, J., Amaris, H., & Ledo, A. T. (2021). Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. *Sensors, 21*(17), 5826.
- aws.*Innovar con el uso de machine learning.* Amazon Web Service (aws). Retrieved 14/04/2023, from https://aws.amazon.com/es/ai/
- Baviera, T. (2017). Técnicas para el análisis del sentimiento en Twitter: Aprendizaje Automático Supervisado y SentiStrength. *Dígitos, 1*(3), 33-50.
- Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. Decreto LeyU.S.C. (2023). https://www.boe.es/buscar/act.php?id=BOE-A-2023-8795&p=20230310&tn=6
- *Estrategia Nacional de Inteligencia Artificial.* (2020). (). https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.
- Jaime Correa-Henao, G., & Yusta-Loyo, J. M. (2013). *Seguridad Energética y Protección de Infraestructuras Críticas.*ssn: 2145-4086
- Jeffrey A. Marron, Avi M. Gopstein, Nadya Bartol, Larry Feldman. (2019). *NIST-Cybersecurity Framework Smart Grid.* (). https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf
- Kienle, F., & De Schryver, C. (2012). 100% green computing at the wrong location?
- Ledo Iglesias, A. T.Analysis of Social and Legal Issues on Critical Infrastructures in Spain. Paper presented at the *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG),* 375-377.
- Ledo Iglesias, A. T., & Martínez, M. A. (2020). El sistema eléctrico español como infraestructura crítica: su protección ante ciberincidentes. *Cuadernos De La Guardia Civil: Revista De Seguridad Pública,* (61), 97-126.
- Li, X., Shi, J., & Chen, Z. (2021). Task-Driven Semantic Coding via Reinforcement Learning. *IEEE Transactions on Image Processing : A Publication of the IEEE Signal Processing Society, 30*, 6307-6320. 10.1109/TIP.2021.3091909
- Salimans, T., Goodfellow, I., Zaremba, W., Cheung, V., Radford, A., & Chen, X. (2016). Improved techniques for training gans. *Advances in Neural Information Processing Systems, 29*