EL SISTEMA ELÉCTRICO ESPAÑOL COMO INFRAESTRUCTURA CRÍTICA SU PROTECCIÓN ANTE CIBERINCIDENTES

ÁNGEL TOMÁS LEDO IGLESIAS

TENIENTE, CENTRO UNIVERSITARIO DE LA GUARDIA CIVIL. DOCTORANDO DEL PROGRAMA DE DOCTORADO "ANÁLISIS DE PROBLEMAS SOCIALES" DE LA UNED

MÓNICA ALONSO MARTÍNEZ

DEPARTAMENTO DE INGENIERÍA ELÉCTRICA, UNIVERSIDAD CARLOS III DE MADRID

RESUMEN

La sociedad actual depende hoy en día, entre otros, de dos servicios fundamentales. Por una parte, de los servicios que proveen de electricidad y por otra de los servicios que proveen la información digital. Estos servicios esenciales son provistos por una infraestructura amplia y compleja. Parte de esa infraestructura es considerada como infraestructura crítica[1] (en adelante, IC). El fallo o caída del servicio prestado por una IC, por dependencias funcionales unas de otras, puede provocar un efecto en cascada que devenga en la caída de más infraestructuras que proporcionen otros servicios esenciales a los ciudadanos.

El estudio de la estructura del sistema eléctrico español como uno de los doce sectores estratégicos, que tiene sus propias infraestructuras críticas, la normativa referida a las IC y al sector eléctrico español, los agentes implicados en su operación y protección como son los propios operadores del sistema, la Guardia Civil o el Centro Nacional de Protección de Infraestructuras y Ciberseguridad, entre otros agentes, así como las diferentes tipologías de ataques y los posibles agentes agresores que actúan en el ciberespacio son el objetivo principal del presente artículo.

Palabras clave: Ciberincidentes, Sistema Eléctrico Español, Infraestructuras Críticas, Smart Grids, SCADA/ICS.

ABSTRACT

Society depends today, among others, on two essential services. On the one hand, the services that provide electricity and, on the other hand, the services that provide digital information. These essential services are provided by a long and complex infrastructure. Part of that infrastructure is considered critical infrastructure (hereinafter, CI). The failure or fall of the service provided by a CI, by functional dependencies ones of each other, these can cause a cascade effect that results in the fall of more infrastructures that provide other essential services to citizens.

1 Las Infraestructuras críticas son 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" (Art. 2. de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas).

The study of the Spain's electricity structure system as one of the twelve strategic sectors, which has its own critical infrastructures, the regulations regarding IC's and the Spanish electricity sector, the agents involved in its operation and protection, such as the operators of the system, the Civil Guard or the National Center for Infrastructure Protection and Cybersecurity, among other agents. As well as the different typologies of attacks and the possible aggressors that operate in cyberspace are the main objective of this article.

Keywords: Cyber Incidents, Spanish Electric System, Critical Infrastructures, Smart Grids, SCADA/ICS.

1. INTRODUCCIÓN

Los terribles atentados terroristas del 11S de 2001 en Nueva York y el del 11M, de 2004 en Madrid, supusieron un revulsivo para todas las sociedades, haciendo que se sintieran más vulnerables y más conscientes de la necesidad de proteger aquellos servicios que les resultaban más esenciales y básicos para la vida y su bienestar.

Hoy en día, las sociedades dependen de la energía para su desarrollo y de su bienestar de la energía, entre las cuales se encuentra la energía eléctrica. Sin este tipo de energía las funciones esenciales serían simplemente imposibles e inexistentes.

Para preservar las infraestructuras que proveen los servicios que satisfacen las necesidades esenciales, los distintos países han realizado y continúan realizando grandes esfuerzos desde todos los frentes que les son competentes, comenzando por la regulación y el desarrollo de normas jurídicas.

Ya en la *Constitución Española de 1978* (en adelante, CE), en su preámbulo, se recoge el deseo de la Nación española de establecer la seguridad y promover el bien de cuantos la integran en uso de su soberanía. En su artículo 17 proclama que toda persona tiene derecho a su libertad y su seguridad. Estableciendo como competencias exclusivas del Estado sobre distintas materias en su artículo 149, entre otras, la legislación, la ordenación y la concesión de recursos y aprovechamientos hidráulicos cuando las aguas discurran por más de una Comunidad Autónoma, y la autorización de las instalaciones eléctricas cuando su aprovechamiento afecte a otra Comunidad o el transporte de energía salga de su ámbito territorial (*CE, artículo 149.22ª*.), la legislación básica sobre protección del medio ambiente (*CE, artículo 149.23ª*.), las bases del régimen minero y energético (CE, artículo 149.25ª.) o la Seguridad pública (CE artículo 149.29ª.)

En este sentido se expresa la Estrategia de Seguridad Nacional de 2017 (en adelante ESN), al afirmar que *"La energía es un elemento fundamental para la prosperidad, el bienestar de la sociedad y la propia soberanía y continuidad del Estado". (Departamento de Seguridad Nacional, 2017).*

Es en ese documento, la ESN, donde se plasman los desafíos y amenazas[2] a los que se enfrenta España como nación, los ámbitos de actuación en los que las mismas se desdoblan, estableciendo unas líneas de acción y objetivos que desarrollan

2 Se entenderá por amenaza al evento, persona, artificio o circunstancia que pueda dañar o destruir la información, los datos, los servicios, sistemas o a las personas.

esas líneas de acción para garantizar el bienestar, la propia soberanía y la continuidad del Estado.

También, en este documento se vislumbran una serie de amenazas a la seguridad nacional, entre las que se encuentran el terrorismo, el crimen organizado o el espionaje.

Las amenazas, que se desarrollan en unos ámbitos comunes como es el ciberespacio, en el que se pueden reconocer vulnerabilidades donde las amenazas anteriormente descritas, las ciberamenazas o el uso de forma ilegítima del ciberespacio pueden tener lugar.

Es en este dominio, el ciberespacio, en el que algunas conductas antijurídicas como el robo de información, los daños en la información, los daños a los sistemas de información y comunicación, la privación de los servicios prestados por estos sistemas con técnicas como el DoS[3] o el DDoS[4], el chantaje utilizando técnicas como el *ransomware*[5] se ciernen como posibles ciberataques a infraestructuras, entre ellas las infraestructuras críticas y de estas las referentes al sector estratégico de la energía eléctrica. Otro de los sectores estratégicos relacionados con el anterior, en el que se producen esas conductas antijurídicas, es el de las tecnologías de la información y la comunicación (en adelante, TIC).

Así la ESN, reconoce en espacios comunes globales, amenazas y desafíos globales como son la vulnerabilidad del ciberespacio, la vulnerabilidad energética, los efectos derivados del cambio climático o las amenazas sobre las IC.

Para hacer frente a estas amenazas y desafíos, se establecen unos objetivos y unas líneas de actuación. Entre estas estarían como líneas de actuación incrementar la ciberseguridad, la lucha contra el terrorismo, la seguridad energética, la protección de las IC o la preservación del medio ambiente.

El proceso de transformación digital se revela como un gran catalizador para el desarrollo tecnológico y la preservación del medio ambiente, donde se muestra como una acción fundamental, el garantizar el suministro energético. Surgiendo la necesidad de proteger la seguridad de las instalaciones e infraestructuras que permiten su producción, gestión, transporte y distribución.

Proveer esta seguridad es una responsabilidad compartida entre los agentes que operan las infraestructuras y las administraciones públicas, frente a aquellos agentes que pretendan dañar las infraestructuras del sector energético y los servicios prestados por el mismo, guiados por diversos motivos como puedan ser los motivos económicos, los ideológicos o los políticos.

Por otra parte, se ha establecido una convergencia entre el mundo físico y el mundo virtual soportado por las TIC, que permite gestionar y operar de forma remota, y

3 DoS es un tipo de ataque informático. Significa Denegación de Servicio por sus siglas en inglés (Denied of Servicie, DoS).

4 DDoS es un tipo de ataque informático evolucionado del anterior, en el que se utiliza multitud de dispositivos de forma distribuida para realizar el ataque contra un sistema concreto. Significa Distribuid Denied of Servicie, DDoS.

5 El ransomware es un tipo de ataque informático en el que se realiza, por parte del atacante, un cifrado total o parcial de la información del sistema de la víctima y se pide un rescate a cambio de obtener una clave que permitiría su descifrado.

muchas veces desatendida, los dispositivos y máquinas reales. De forma que lo que ocurre en el mundo físico tiene un alto impacto en la gestión y operatividad gestionada en el entorno virtual y viceversa.

Todo esto sucede de una forma transparente para el ciudadano. De la misma forma, en entornos industriales se ha pasado del control y supervisión manual por operarios a sistemas de control industrial, conocidos por sus siglas en inglés (ICS, *Industrial Control System*). Estos sistemas engloban a métodos de control implantados en áreas ampliadas como son los sistemas inteligentes de control y adquisición de datos (*Supervisory Control and Data Acquisition*, SCADA) y los sistemas de control distribuidos, conocidos por sus siglas en inglés (DCS, *Distributed Control System*)

Estos sistemas de control industrial no estaban diseñados para funcionar con seguridad en las redes de datos de propósito general, como puede ser Internet, con un gran ciclo de vida que puede superar normalmente, según la actividad, los 15 años de vida útil. Estos sistemas han estado históricamente implantados de forma aislada, pero en la actualidad cada vez más lo están. Y se despliegan utilizando la infraestructura de Internet para poder gestionar de forma remota los distintos sistemas distribuidos geográficamente, con el consecuente riesgo que esto supone para la seguridad lógica de los mismos, la seguridad lógica de los sistemas a los que se conectan, así como de las propias redes de información a las que se acoplen.

Tradicionalmente se trabajaba en la seguridad desde el ámbito de la seguridad física, pero esto ya no es posible, teniendo que adoptar un concepto de seguridad integral, en el que se enmarca también la protección desde el ámbito de la seguridad lógica, especialmente en los sistemas dedicados al control industrial.

La amenaza de ataques a sistemas e información operados en el sector eléctrico y en el ciberentorno es real, ya ha ocurrido. Ciberincidentes como el sufrido contra la planta nuclear de Natanz en Irán, con el malware[6] "*Stuxnet*". El ataque sufrido por la empresa de distribución de energía eléctrica Kyivoblenergo de Ucrania, el 23 de diciembre de 2015, en el que se vieron afectadas más de 225.000 personas como muestra el informe del instituto SANS (*SANS, marzo 2016*[7]) o el más reciente ciberincidente sufrido a primeros de abril de 2020 por la compañía EdP (Energías de Portugal, S.A)[8], en el que se estima que se han visto comprometidos 10 TB[9] de información, por el que han pedido a la compañía un rescate de diez millones de euros, son una muestra de ello.

2. EL SISTEMA ELÉCTRICO COMO INFRAESTRUCTURA CRÍTICA

Los sistemas eléctricos son una de las máquinas más complejas desarrollados por el hombre y de ellos depende la mayor parte de la actividad física y económica del mundo. Es por tanto necesario considerar a las redes eléctricas como instalaciones críticas que es necesario proteger, y así ha sido recogido dentro del 2017, *Join*

6 Malware, proviene del acrónimo malicious software, software malicioso. Se considera como tal, todo aquel software capaz de dañar a la información o a los sistemas de información de forma lógica.

7 Recuperado de: https://bit.ly/3kGNGCB. Fecha. 22 de mayo de 2020

8 EdP es uno de los principales grupos de producción y distribución de energía en Europa y el principal de Portugal, con una facturación de 12.000 millones de euros en 2012.

9 TB, es el acrónimo de Tera Bytes, es una unidad de medida de información. En concreto 1 TB equivale a 1024 Mega Bytes o a 1.048.576 Mega Bytes de información.

Communication on Cibersecurity. Teniendo en cuenta la nueva digitalización a la que se enfrenta el sector eléctrico, la UE en su paquete "*Clean Energy for all Europeans"* (*JOIN/2017/0450*) ha adoptado ocho medidas encaminadas a la creación de un entorno favorable para la transición hacia el mundo digital dentro del sector eléctrico, en el que cobra especial relevancia la ciberseguridad de dichos sistemas.

2.1. EL SISTEMA ELÉCTRICO COMO INFRAESTRUCTURA CRÍTICA. NORMATIVA

Después de los ya mencionados atentados del 11S[10] y 11M[11], y ante la importancia de mantener los servicios esenciales, la continuidad de la prestación de los mismos y las infraestructuras que lo sostienen, los Estados reaccionaron con distintas medidas e iniciativas para su consecución, siendo una de las primeras medidas la regulación normativa. Se verá un breve itinerario de las distintas regulaciones tanto de la Unión Europea como la española.

2.1.1. Marco regulatorio de la Unión Europea en relación a las IC

En 2004, y en respuesta a los ataques terroristas del 11M y 11S, surge en el seno de la Unión Europea la necesidad de incrementar la seguridad en lo que se consideraban las IC. En junio de 2004, el Consejo Europeo solicita la elaboración de una estrategia global para mejorar la protección de infraestructuras críticas.

La Comisión, en respuesta a esa solicitud, el 20 de octubre de 2004 adopta la *Comunicación COM/2004/0698*, sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, en la que se formulan propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que afecten a las IC.

Con la comunicación *COM/2004/0701*, *"Lucha contra el terrorismo: preparación y gestión de las consecuencias"*, la Comisión creará un sistema europeo de alerta temprana denominado "ARGUS", para conectar todos los sistemas de emergencia especializados.

Ese mismo año se promulga la **Comunicación COM/2004/0702, "Protección de las infraestructuras críticas en la lucha contra el terrorismo"**. En la misma se identifica qué son las infraestructuras críticas y un sistema que defina la criticidad de las mismas, se establece la creación de un inventario y criterios de clasificación de estas infraestructuras. Por la misma Comunicación, se crea la Agencia Europea de Seguridad de las Redes y la Información (*European Network and Information Security Agency*, ENISA) y finalmente se propone la creación del Programa Europeo para la Protección de Infraestructuras Críticas PEPIC, o por sus siglas en inglés (*European Programme for Critical Infrastructure Protection*, EPCIP). Se establecen medidas concretas como la identificación de las Infraestructuras Críticas Europeas (ICE), sin perjuicio de que los estados miembros trabajen sus Infraestructuras Críticas Nacionales (ICN), y que estos establezcan un Organismo de Coordinación Nacional de Protección

10 Atentado terrorista por atacantes yihadistas que sucedió en la ciudad de Nueva York, el día 11 de septiembre de 2001.

11 Atentado terrorista por atacantes yihadistas que sucedió en la ciudad de Madrid, el día 11 de marzo de 2004.

de Infraestructuras Críticas (OCNP-PIC). Se incide en la necesidad de trabajar en los Planes de Seguridad de Operador (PSO), proponiendo un modelo.

El 8 de diciembre de 2008, se promulga la Directiva Europea 2008/114/CE, en vigor desde el 12 de enero de 2009 que debía ser incorporada a los ordenamientos jurídicos de los estados miembros con anterioridad al 12 de marzo de 2011. Esta directiva establece un procedimiento de identificación de ICE, así como un criterio común para evaluar las infraestructuras. Se definen en su artículo 2 varios conceptos como son:

- Infraestructuras críticas.
- Infraestructuras críticas europeas.
- Análisis de riesgo.
- Información sensible sobre protección de infraestructuras críticas.
- Protección.
- Propietarios u operadores de infraestructuras críticas europeas.

Así, define Infraestructura Crítica como "*El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones*" (Directiva Europea 2008/114/CE)

En su artículo 3 establece que cada estado miembro identificará las ICEs y las ICNs para proponerlas a la comisión y que, a su vez, la Comisión podrá proponer la existencia de infraestructuras para valorarlas como infraestructuras críticas europeas. Se establecen unos criterios horizontales para valorar la criticidad de las infraestructuras que habrán de incluir el número de víctimas, el impacto económico y el impacto público.

En su artículo 4, entre otras indicaciones, señala que el proceso de identificación y designación de ICE se completará antes del 12 de enero de 2011, estableciéndose que su revisión deberá hacerse de forma periódica.

En 2013, se publica la Estrategia de Ciberseguridad de la Unión Europea (*Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*, CSEU-SSC). Este documento comprende los aspectos del mercado interior, justicia y política exterior relacionados con el ciberespacio.

Pero el verdadero impulso en materia de ciberseguridad viene de la mano de la promulgación de la *Directiva 1148/2016/UE*, de 6 de julio de 2016, más conocida como la *Directiva NIS*, la "Directiva del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión", publicada el 19 de julio de 2016, que entró en vigor el 9 de agosto de 2016. Traspuesta a nuestro ordenamiento jurídico, a través del *Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y los Sistemas de Información*.

En este Real Decreto-ley, se establece en su artículo 36 una tipificación de faltas calificadas como faltas leves, graves y muy graves, por las que se pueden establecer

unas sanciones que podrían ir desde una mera amonestación hasta una sanción de 1.000.000 de euros para faltas muy graves.

2.1.2. Marco regulatorio español en relación a las IC y al sector eléctrico

En España, *la Directiva 2008/114/CE*, se ha traspuesto al ordenamiento jurídico a través de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, de una forma completa y aportando otras medidas complementarias. Esta ley es comúnmente conocida como *Ley de Protección de Infraestructuras Críticas (*en adelante, LPIC), desarrollada por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el *Reglamento de protección de las infraestructuras críticas* (en adelante RDPIC).

En la LPIC, se incluye la definición oficial en España de qué es un servicio esencial, una infraestructura crítica y una infraestructura estratégica, siendo que:

- Servicio esencial: *"Es 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*".
- Infraestructuras Críticas: *"Son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*".
- Infraestructuras Estratégicas: *Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales" (Ley PIC, 2011).*

Tanto en la LPIC como en el RDPIC, se establece que la responsabilidad de la seguridad de las infraestructuras críticas será compartida por el Gobierno, a través de los organismos competentes[12], los operadores críticos que operen o exploten las mismas (ya sean operadores públicos o privados) y terceras partes que se hubieran incorporado por delegación de los anteriores.

La LPIC y su desarrollo reglamentario con el RDPIC establecen un esquema de planificación de la protección de las IC, articulado en un mecanismo de carácter interdepartamental formado por órganos y entidades tanto de carácter privado como de las Administraciones Públicas. Estos son de carácter estratégico y responsabilidad

12 Según el RDPIC, los organismos competentes son:
- La **Secretaría de Estado** de Seguridad del Ministerio del Interior.
- El **Centro Nacional** para la Protección de las Infraestructuras Críticas.
- Los **Ministerios** y organismos integrados en el Sistema.
- Las **Comunidades Autónomas y** las Ciudades con Estatuto de Autonomía.
- Las **Delegaciones del Gobierno** en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
- Las **Corporaciones Locales** mediante la asociación de Entidades Locales de mayor implantación a nivel nacional.
- La **Comisión Nacional** para la Protección de las Infraestructuras Críticas.
- El **Grupo de Trabajo Interdepartamental** para la Protección de las Infraestructuras Críticas.

exclusiva del Estado, del que emanan el Plan Nacional de Protección de IC (PNPIC) y los Planes Estratégicos Sectoriales (PES).

Por otra parte, a un nivel más limitado en alcance y organizativo de responsabilidad, estarían los titulares de la IC, del que emanará los Planes de Seguridad del Operador (PSO) y los Planes de Protección Específicos (PPE).

Finalmente, estaría el escalón de planificación con un carácter operativo por las Delegaciones de Gobierno, a través de las Fuerzas y Cuerpos de Seguridad que realizarán los Planes de Apoyo Operativo (PAO).

Hay otras normas de distinto rango jurídico que vienen a dar apoyo, respuesta y soluciones al complejo tratamiento de la protección de infraestructuras críticas, como son las seguidamente relacionadas:

- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador (PSO) y de los Planes de Protección Específicos (PPE).

- Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017 (en adelante, ENS 2017).

- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019 (en adelante, ENCS 2019), aprobada por el Consejo de Seguridad Nacional.

- Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave.

- Orden PCI/179/2019, de 22 de febrero, por la que se publica la Estrategia Nacional contra el Terrorismo 2019, aprobado por el Consejo de Seguridad Nacional.

- Estrategia de Seguridad Energética Nacional, publicado por el Departamento de Seguridad Nacional en 2015, en la que se estable como características del sistema eléctrico español su robustez y fortaleza al estar mallado y parcialmente interconectado, tanto con Francia como con Portugal.

Así en España el sector estratégico de la energía comprende tanto la producción, transporte como la distribución de la energía, ya sea eléctrica, de hidrocarburos o de gas natural.

Se denota que, si bien, tanto la LPIC como el RDPIC no tienen un régimen sancionador, por no contemplar las debidas medidas de seguridad por parte de los operadores, esto sí queda reflejado en la transposición de la *Directiva 1148/2016/UE*, de 6 de julio de 2016, más conocida como la Directiva NIS, a través del *Real Decreto-ley 12/2018,* de 7 de septiembre, de Seguridad de las Redes y los Sistemas de Información.

Según datos publicados por el Departamento de Seguridad Nacional, hasta diciembre de 2018, en el ámbito del sector energético español se habían consolidado los PSO de quince operadores críticos y los PPE de sesenta y siete instalaciones críticas (*Departamento de Seguridad Nacional, 2019*).

SECTOR	SUBSECTOR	PLAN DE SEGURIDAD DEL OPERADOR	PLAN DE PROTECCIÓN ESPECÍFICO
Energía	Eléctrico	15	67
	Petróleo	5	17
	Gas	5	33
Financiero		15	25
Nuclear		4	6
Transporte	Aéreo	2	7
	Marítimo	18	6
	Ferroviario	3	1
	Carreteras	2	2
Agua		26	15
Espacio		3	0
Químico		8	7
TIC		6	0
Alimentación		0	0
Transporte		0	0
Administración		0	0
Instalaciones de investigación		0	0

Fuente: Ministerio del Interior

Ilustración 1. Planes de Seguridad de Operador y Planes de Protección Específicos del sector eléctrico español, 2018. (Fuente, DSN)[13].

2.1.3. Marco regulatorio europeo y español en relación al sector eléctrico

En cuanto a la normativa específica del sector eléctrico español, abundante en esta materia, se encuentra consolidada y actualizada[14] a fecha 27 de abril de 2020, cuando se cerró este artículo. En la ilustración 2, se pueden ver los principales desarrollos normativos tanto nacionales como europeos desde 1997 a 2017.

En gran medida estos desarrollos normativos han ido encaminados a la liberalización en el ámbito de la competencia y el mercado de la energía eléctrica. Por otra parte, este desarrollo normativo ha ido orientado a contemplar las medidas técnicas de instalación, transporte y operación de las líneas de distribución eléctrica.

13 Recuperado del informe anual 2019, del Departamento de Seguridad Nacional. Fecha: 22 de mayo de 2020.

14 Código electrónico de la Energía Eléctrica, publicado por el BOE (Boletín Oficial del Estado) y recuperable en el enlace: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=014_Codigo_de_la_Energia_Electrica&tipo=C&modo=2

Podría destacarse:

- *La Directiva 2003/54/CE* del Parlamento Europeo y del Consejo, de 26 de junio de 2003, sobre normas comunes para el mercado interior que deroga la anterior Directiva 96/92/CE de declaraciones sobre las actividades de desmantelamiento y de gestión de residuos y que ha sido traspuesta a nuestro ordenamiento jurídico, a través de la Ley 17/2007.

- *Ley 17/2013*, de 29 de octubre, para la garantía de suministro e incremento de la competencia en los sistemas insulares y extra-peninsulares, en la que se establece que Red Eléctrica de España (en adelante, REE), en su calidad de operador del sistema, sea el titular de todas las nuevas instalaciones de bombeo, siempre y cuando se determine que dichas instalaciones tengan como finalidad principal la garantía del suministro, la seguridad del sistema y la integración de energías renovables no gestionables.

- *Ley 24/2013*, de 26 de diciembre, del Sector Eléctrico, que es la principal norma reguladora de las actividades de transporte de energía eléctrica.

- *Reglamento 2019/943*, del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de electricidad.

Desde el punto de vista técnico, cabe destacar:

- El Reglamento publicado por el *Real Decreto 223/2008*, sobre condiciones técnicas y garantías de la calidad en líneas de Alta Tensión.

- *Real Decreto 134/2010*, por el que se establece el procedimiento de resolución de restricciones para garantía de suministro.

- *Real Decreto-ley 9/2013* por el que se establecen medidas urgentes para garantizar la estabilidad financiera del sistema eléctrico en el sistema eléctrico y en el sector financiero.

- *Real Decreto-ley 413/2014* por el que se regula la actividad de producción de energía eléctrica a partir de las fuentes de energía renovables, cogeneración y residuos.

- Circular de la Comisión nacional de los Mercados y la Competencia (en adelante, CNMC), *Circular 7/2019*, de 5 de diciembre, por la que se aprueban las instalaciones tipo y los valores unitarios de referencia de operación y mantenimiento por elemento de inmovilizado que se emplearán en el cálculo de la retribución de las empresas titulares de instalaciones de transporte de energía eléctrica y que establecen el actual marco regulatorio retributivo para la actividad de transporte de energía eléctrica en España.

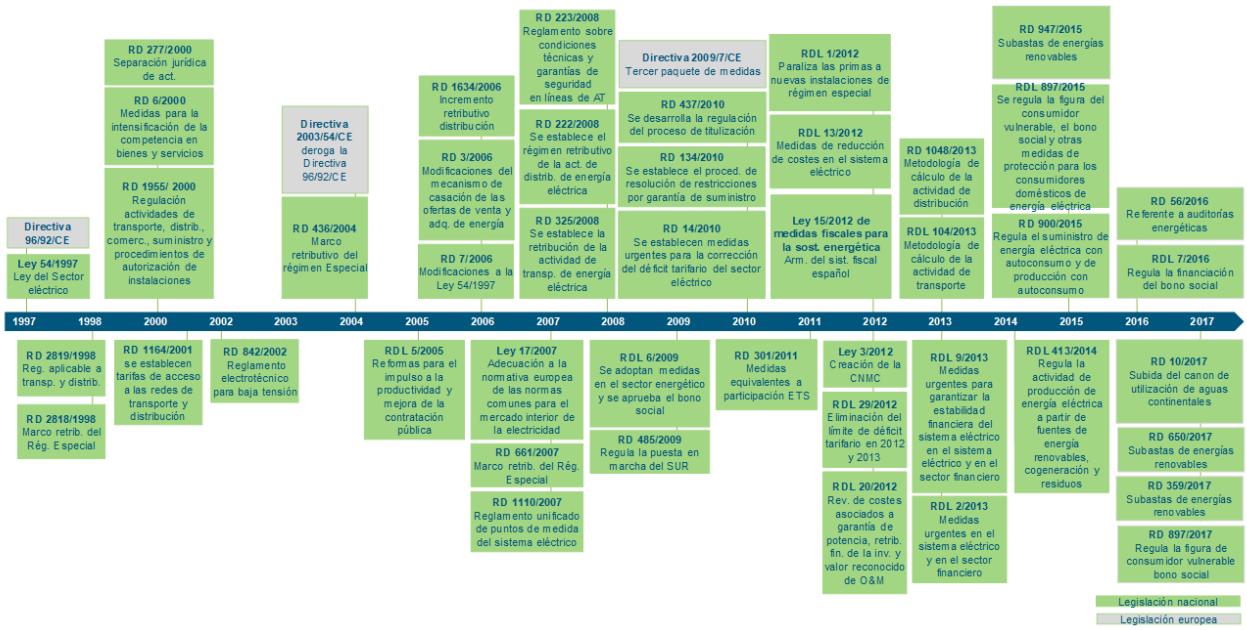

Ilustración 2. Legislación básica del Sector Eléctrico Español[15].

2.2. ESTRUCTURA DEL SISTEMA ELÉCTRICO, DESDE EL GENERADOR AL CONSUMIDOR

El objetivo de un sistema eléctrico es abastecer la demanda eléctrica de las cargas presentes a lo largo de un territorio. Puesto que no es posible almacenar a gran escala la energía eléctrica, es necesario que se cumpla en todo momento un equilibrio entre la demanda y la generación.

Esta condición, junto con la necesidad de mantener continuidad en los circuitos que transportan la energía eléctrica, hacen que el sistema eléctrico forme parte del sector estratégico de la energía, parte de ellas se encuentran catalogadas como IC.

Las tres funciones principales de un sistema eléctrico son la generación, el transporte y la distribución de la energía eléctrica, desde las plantas generadoras hasta los consumidores finales, como puede observarse en la Ilustración 3.

Para llevar a cabo estas funciones el sistema eléctrico está compuesto por numerosos componentes: unidades de generación; líneas de transporte y distribución; transformadores; sistemas de monitorización, protección y control; operadores de red, encargados de mantener el equilibrio entre demanda y generación; y circuitos eléctricos de los consumidores finales.

15 Recuperado de http://www.energiaysociedad.es/manenergia/2-2-el-marco-normativo-espanol/, Fecha: 22 de mayo de 2020.

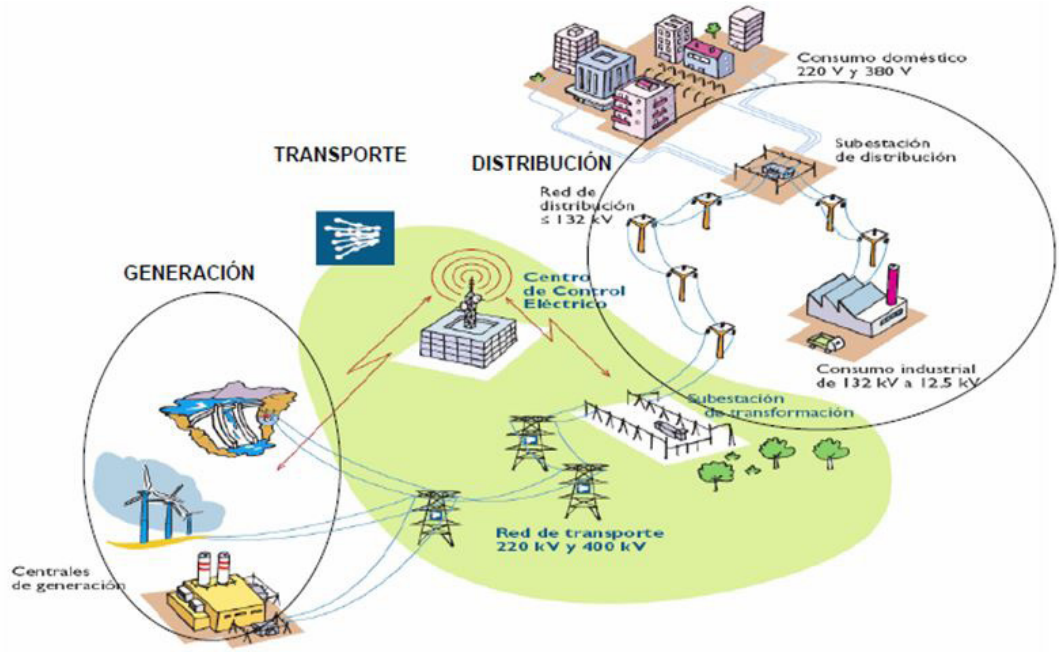

Ilustración 3. Esquema básico del sistema eléctrico español[16].

La generación de electricidad en España, junto con la distribución, es una actividad regulada, encargada de la producción de energía eléctrica. Las unidades de generación transforman energía primaria (agua, carbón, luz, viento, etc) en energía eléctrica, y en el territorio español conviven tecnologías convencionales (hidráulica, nuclear y térmica) con las instalaciones renovables (eólica, solar, biomasa, etc.).

Para hacer llegar la energía eléctrica desde los centros de generación al consumidor final es necesario disponer de una red de transporte y distribución de energía eléctrica. En España se pueden distinguir dos segmentos en función de las tensiones de trabajo: la red de transporte en alta tensión (220 kV y 380 kV) y la red de distribución en media y baja tensión (tensiones inferiores a 132 kV).

La red de transporte es la encargada de transportar la energía eléctrica desde las grandes centrales de generación, a lo largo de la geografía española, hasta las redes de distribución, así como de mantener los intercambios de energía internacionales.

Red Eléctrica de España[17] es la empresa encargada de las labores de mantenimiento, operación y gestión de la red eléctrica de transporte española en exclusividad desde el año 2007 (Ley 17/2007), dado el carácter esencial del transporte de energía eléctrica que es una actividad regulada, ejercida en régimen de monopolio.

Por otra parte, la red de distribución transporta la energía eléctrica de la red de transporte hasta el consumidor final, a través de diferentes niveles de tensión, es por tanto una red de aproximación de la electricidad al consumidor. La distribución de energía eléctrica es una actividad no regulada que llevan a cabo diferentes compañías a lo largo del territorio español.

16 Recuperado de https://codigopublico.com/a-fondo/la-energia-que-nos-mueve-2/ Fecha: 22 de mayo de 2020.

17 REE (Red Eléctrica de España) es una empresa de titularidad pública nacida en enero de 1985. https://www.ree.es/es/conocenos/ree-en-2-minutos Fecha: 23 de mayo de 2020.

El paso de un nivel de tensión a otro se realiza mediante transformadores, localizados en subestaciones, siendo uno de los elementos críticos de los sistemas eléctricos.

En función de los niveles de tensión con los que trabaja el transformador se pueden distinguir:

- subestaciones elevadoras, encargadas de elevar la tensión a la salida de los generadores para adecuarla a los niveles de tensión de la red de transporte de energía eléctrica;
- subestaciones de distribución, actúan de eslabón entre el sistema de transporte y el de distribución;
- los centros de transformación, que reducen la tensión a los niveles de los consumidores finales de baja tensión.

En la ilustración 4 puede verse el esquema de actividades realizadas en el sistema eléctrico español, junto a los principales operadores y algunos de menor entidad.

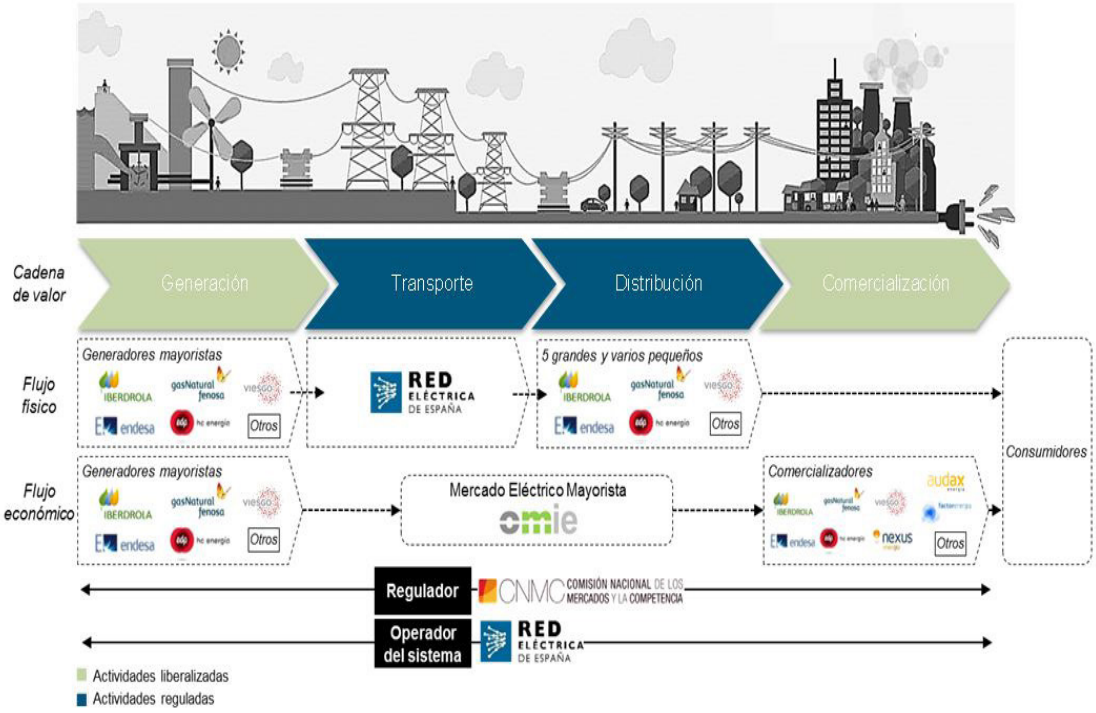

Ilustración 4. Actividades en el sistema eléctrico español[18].

Según el informe de cierre del año 2019, de Red Eléctrica de España[19], la red de transporte del sistema eléctrico español está compuesta por 44.457 km de líneas eléctricas y 33.700 km de fibra óptica.

18 Recuperado de https://codigopublico.com/a-fondo/la-energia-que-nos-mueve-2/ Fecha: 22 de mayo de 2020.

19 Recuperado, desde la página Web de REE https://www.ree.es/es/datos/publicaciones/informe-anual-sistema/sistema-electrico-espanol-prevision-cierre-2019 Fecha: 23 de mayo de 2020.

En cuanto a la potencia instalada, en el año 2019 se incrementó a nivel nacional en 108,6 TWh[20] llegando a los 261,02 TWh en el territorio nacional. En relación a los intercambios internacionales con Francia y Portugal, a lo largo de 2019 se importaron 18,8 TWh y se exportaron 12,2 TWh, resultando un saldo importador de 6,6 TWh. Finalmente, y atendiendo a los requerimientos en materia de cobertura de la demanda con fuente de energía renovable, en 2019 el 58,6% de la producción nacional fue libre de dióxido de carbono.

En la tabla 1 puede apreciarse la potencia eléctrica instalada en el sistema eléctrico español, durante los últimos cinco años.

RED ELÉCTRICA DE ESPAÑA

Potencia instalada nacional (MW)

	2016	2017	2018	2019	2020
Hidráulica convencional y mixta	17.030	17.028	17.046	17.085	17.085
Bombeo puro	3.329	3.329	3.329	3.329	3.329
Nuclear	7.573	7.117	7.117	7.117	7.117
Carbón	10.004	10.004	10.030	9.683	9.456
Fuel + Gas	2.490	2.490	2.490	2.447	2.447
Ciclo combinado	26.670	26.670	26.284	26.284	26.284
Hidroeólica	11	11	11	11	11
Resto hidráulica (1)	-	-	-	-	-
Eólica	23.001	23.082	23.545	25.799	25.902
Solar fotovoltaica	4.683	4.685	4.712	8.913	9.146
Solar térmica	2.304	2.304	2.304	2.304	2.304
Térmica renovable/Otras renovables (2)	870	872	877	1.076	1.076
Térmica no renovable/Cogeneración y resto/Cogeneración (3)	5.965	5.801	5.727	5.677	5.672
Residuos no renovables(4)	496	496	490	490	490
Residuos renovables(4)	160	160	160	160	160
Total	**104.588**	**104.050**	**104.123**	**110.376**	**110.480**

(1) Incluye todas aquellas unidades menores de 50 MW que no pertenecen a ninguna unidad de gestión hidráulica (UGH). A partir de 2015 están incluidas en hidráulica convencional y mixta.
(2) Otras renovables incluyen biogás, biomasa, hidráulica marina y geotérmica. Los valores de potencia incluyen residuos hasta el 31/12/2014.
(3) Los valores de potencia incluyen residuos hasta el 31/12/2014.
(4) Potencia incluída en térmica renovable y térmica no renovable/cogeneración y resto/cogeneración hasta el 31/12/2014.
Fuente: Comisión Nacional de los Mercados y la Competencia (CNMC) hasta 2014 en: resto hidráulica, eólica, solar fotovoltaica, solar térmica, térmica renovable/otras renovables, térmica no renovable/cogeneración y resto/cogeneración y residuos.
Datos a 31 de diciembre.
(*) Para el año 2020 datos a abril de 2020.

Tabla 1. Potencia eléctrica instalada en España, periodo 2016-2020, por tipo de fuente de generación (Fuente REE).

El sistema eléctrico español, como ya se ha comentado, se pretende robusto y fuerte por diversas causas. Principalmente por el mallado de su red, siendo muy densa, permitiendo distribuir el flujo de potencia por caminos alternativos en caso de caída de líneas, seguidamente por su interconexión parcial, tanto a Francia como a Portugal, pero también por la diversidad de fuentes generadoras de electricidad utilizadas.

A esta variedad de fuentes ha contribuido, sin duda, el proceso de descarbonización y la implementación de fuentes de generación renovables y menor dependencia del carbón y del petróleo.

20 TWh: Tera Watios por hora.

3. EL NUEVO MODELO DE SISTEMA ELÉCTRICO: LAS SMART GRIDS

3.1. SMART GRIDS

Como consecuencia de las medidas encaminadas a la descarbonización de los sistemas de potencia y la descentralización de la generación, así como el aumento de la participación de los consumidores finales en la producción y gestión de su propia demanda y generación, los sistemas eléctricos de potencia están sufriendo grandes cambios en las últimas décadas.

Las nuevas redes eléctricas inteligentes o Smart grids son complejos sistemas ciber-físicos en los que interaccionan los tradicionales sistemas físicos de generación y transporte de la energía eléctrica, con las nuevas tecnologías digitales empleadas para la captación de medidas, comunicación y procesado de la información que facilitan la gestión de la red eléctrica. Así, las Smart grids integran las acciones de los generadores, de los consumidores y *prosumers* (consumidores con capacidad de generación) conectados a ellas, así como de los sistemas de transporte y distribución, constituyendo un entorno interconectado en una red inteligente que permite ser más eficiente en la producción, el consumo y el transporte de energía eléctrica. Además, las Smart grids permiten alcanzar los objetivos fijados por la Unión Europea en materia de cambio climático: reducir el consumo energético, ampliar la cobertura de la demanda eléctrica con fuentes de generación renovable, y finalmente mejorar la eficiencia energética.

La Ilustración 6 muestra la evolución de las redes eléctricas tradicionales hacia las Smart grids y su exposición a las amenazas de las redes de estándares de tecnologías de la información o IT (por sus siglas en inglés, *Information Technology*).

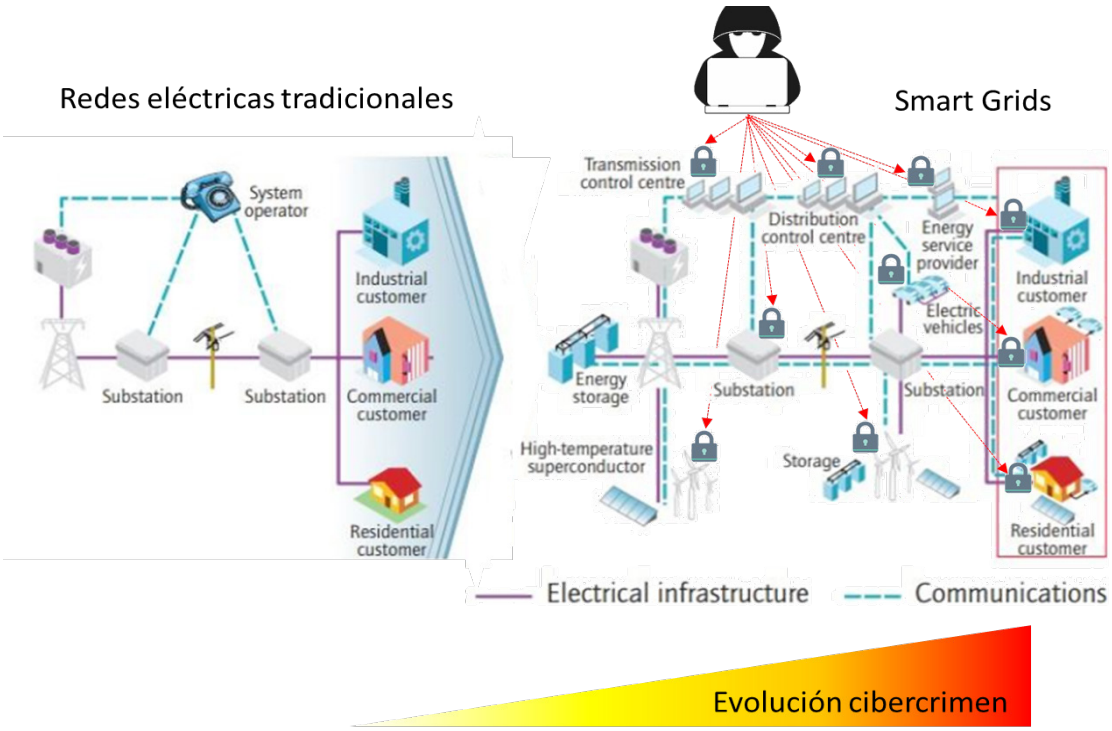

Ilustración 5. Evolución de las redes eléctricas tradicionales a Smart Grids[21].

21 Recuperado de https://www.iea.org/reports/world-energy-outlook-2011 Fecha: 22 de mayo de 2020.

Uno de los elementos clave en la operación de las Smart grids es la arquitectura de comunicaciones, que se emplea para recoger datos sobre el estado de la red. Así como enviar comandos de actuación a los diferentes elementos controlables del sistema eléctrico como generadores, consumidores con capacidad para gestionar su demanda o elementos de control del flujo de potencia en las subestaciones.

La integración de la nueva infraestructura cibernética con la infraestructura física tradicional del sistema eléctrico abre un nuevo abanico de posibles problemáticas en materia de ciberseguridad.

Es en este punto donde confluyen la arquitectura de IT[22] con la de las tecnologías de operación industrial, también conocidas por OT (por sus siglas en inglés, *Operation Technology*), no estando estos últimos, normalmente, preparados para trabajar en condiciones de seguridad en redes estándares de IT. La diferencia conceptual entre ambas es la seguridad.

En el ámbito de las IT se da prioridad a la confidencialidad de la información, a continuación, a la integridad de la misma y, por último, a la disponibilidad.

Por su parte, el ámbito de las OT es mucho más restrictivo en cuanto al tiempo de proceso y el número de dispositivos que han de interactuar intercambiando información. Por esto las redes OT dan prioridad a la disponibilidad, dejando en segundo plano la integridad y por último la confidencialidad.

Lo anteriormente expuesto, unido al largo ciclo de vida que tienen algunos elementos empleados en el sector energético (como pueden ser las grandes centrales térmicas, hidráulicas o nucleares en producción desde hace más de 30 años, hace que al querer integrar estas máquinas, carentes en su diseño de las funcionalidades de seguridad básicas para operar interconectados con redes IT, queden expuestas a amenazas de ciberseguridad muy importantes, que pueden explotar las vulnerabilidades de estos sistemas por agentes que quieran atacarlos.

Ataques puntuales a ciertos elementos del sistema eléctrico pueden acarrear problemas de estabilidad en la red, un fallo en cascada en el sistema o, incluso, llegar a un apagón o, por como es más conocido en la industria por su vocablo en inglés, "*blackout*".

Especialmente sensibles en cuanto a la ciberseguridad son los elementos de procesamiento y comunicación de información dispuestos en la infraestructura avanzada de medida, conocida por sus siglas en inglés (AMI, *Advanced Metering Infraestructure*).

22 Las redes IT son las utilizadas en el ámbito comercial y empresarial, por su parte las OT son tipos de redes utilizadas en el ámbito de la industria.

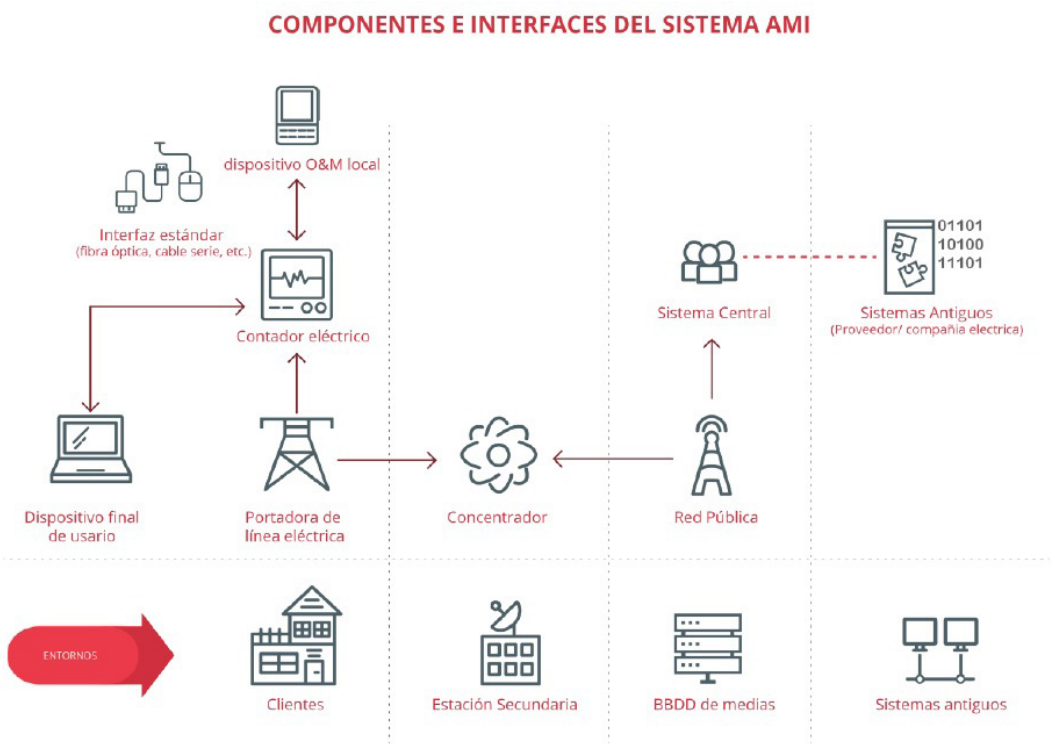

Ilustración 6. Componentes principales de una Infraestructura Avanzada de Medida. Fuente INCIBE[23] [24].

El sector eléctrico es un entorno especial por su implantación de sistemas de medición, control y actuación industrial. En buena parte por las fuertes inversiones realizadas en el sector para su adecuación a la evolución hacia el Smart grid. En este sentido el INCIBE refiere:

> *"Gracias a la unión y estandarización establecida entre distribuidores de energía, fabricantes y desarrolladores, la existencia de protocolos relacionados con las redes inteligentes no es tan profusa como en otros entornos de la industria. De entre los protocolos salidos de esta unión y estandarización se analizan aquellos cuyo uso es más común en el territorio español y aquellos que son usados ampliamente a lo largo del territorio europeo"* (INCIBE, 2012)[25].

Los protocolos de comunicación OT más utilizados en el sector energético español y europeo son *PRIME*[26], *Meters and More*[27], DLMS/COSEM[28], G3-PLC y OSGP[29].

23 INCIBE, Instituto Nacional de Ciberseguridad, España.

24 Obtenido de la Guía de Protocolos de Seguridad Industrial, INCIBE en https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiHpP351s_pAhVy5-AKHQPcDp8QFjAAegQIBBAB&url=https%3A%2F%2Fwww.incibe-cert.es%2Fsites%2Fdefault%2Ffiles%2Fcontenidos%2Fguias%2Fdoc%2Fcertsi_seguridad_protocolos_industriales_smartgrid.pdf&usg=AOvVaw2rf4E377ghUcoJ0QFJ3E7y Fecha: 22 de mayo de 2020.

25 Ibidem 21.

26 PRIME (PoweRline Intelligent Metering Evolution) es un protocolo que implementa los dos primeros niveles del modelo OSI.

27 Meters and More, protocolo propietario, cubre toda la pila de niveles del modelo OSI.

28 DLMS/COSEM es un protocolo de nivel de aplicación que define desde la capa 4 hasta la capa 7 del modelo OSI.

29 OSGP, Protocolo abierto de Smart grid, por sus siglas en inglés (Open Smart grid Protocol).

En la Tabla 2, se puede ver un cuadro comparativo de las características más importantes de estos protocolos en cuanto a aspectos generales, seguridad, capas implementadas por el modelo OSI y su compatibilidad, entre otras.

	Protocolo	PRIME	DLMS/COSEM	Meters and More	G3-PLC	OSGP
Aspectos generales	Tipo de estándar	Abierto	Abierto	Propietario	Abierto	Abierto
	Medio de transmisión	PLC	Ethernet	PLC Ethernet Serie	PLC Ethernet	PLC Ethernet
	Región de uso	España	España	Italia España	Francia	Norte de Europa
	Compatibilidad	DLMS/COSEM	PRIME M&M G3-PLC OSGP	DLMS/COSEM	DLMS/COSEM	DLMS/COSEM G3-PLC
Seguridad	Cifrado	Perfiles 1 y 2	Niveles Low y High	SI	SI	SI
	Autenticación	Perfiles 1 y 2	Niveles Low y High	SI	SI	SI
Capas implementadas por el protocolo (nivel OSI)	1	X		X	X	X
	2	X		X	X	X
	3			X	X	X
	4		X	X	X	X
	5		X		X	X
	6		X		X	X
	7		X	X	X	X
Recomendaciones de seguridad		Utilizar el perfil de seguridad 1 o 2	Utilizar High Level security Sobre TCP/IP realizar filtrado en el puerto 4059	En despliegues conjuntos con DLMS/COSEM aplicar la seguridad en ambos protocolos	Utilizar autenticación vía RADIUS	Utilizar medidas de cifrado adicionales

Tabla 2. Resumen comparativo de protocolos utilizados en redes inteligentes. Fuente INCIBE[30].

4. NUEVOS RETOS DEL SISTEMA ELÉCTRICO ANTE CIBERINCIDENTES

Los últimos datos consolidados en cuanto a ciberincidentes son los referidos al año 2018, datos publicados por el Ministerio del Interior de España.

Analizando los mismos se puede observar que el sector energético tuvo 20,6% de los ciberincidentes registrados a IC.

En las tablas 3, 4 y 5 pueden apreciarse los ciberincidentes gestionados por el INCIBE-CERT, durante el año 2018 y anteriores. Nótese que no pueden ser localizados a partir de las Tablas referidas, ni de los metadatos de las mismas, los ciberincidentes producidos exclusivamente en el sector energético de la electricidad, al no estar diferenciados. Los datos se refieren a todo el Sector Estratégico de la Energía, incluyendo la electricidad, los hidrocarburos y el gas natural (*Ministerio del Interior, 2019*).

Incidentes por público objetivo	INCIDENTES GESTIONADOS			
	2015	2016	2017	2018
Ciudadanos y empresas	45.693	110.293	116.642	102.414
Red académica (RedIris)	4.153	4.485	5.537	8.383
Infraestructuras Críticas (IICC)	130	479	885	722

Tabla 3. Ciberincidentes por dominio de objeto.[31]

30 Ibídem 21.
31 Recuperado del Informe anual de Ciberdelincuencia 2019, *(Ministerio del Interior, 2019)*

Sector estratégico	INCIDENTES GESTIONADOS			
	2015	2016	2017	2018
Energía	46	126	213	149
Transporte	24	90	152	192
Tecnologías Informac. y Comunicac. (TIC)	17	17	40	46
Sistema tributario y financiero	17	152	250	214
Alimentación	12	47	42	40
Agua	5	40	134	57
Industria nuclear	5	4	12	5
Administración	1	2	10	1
Espacio	0	0	1	3
Industria química	0	0	0	15
Instalaciones de Investigación	0	0	0	0
Salud	0	0	1	0
Todos los sectores afectados	3	1	0	0

Tabla 4. Ciberincidentes gestionados por Sector Estratégico[32].

Tipo de incidente	INCIDENTES GESTIONADOS			
	2015	2016	2017	2018
Intrusión	15	39	97	26
Fraude	8	13	66	41
Malware	75	311	387	200
SPAM	0	8	21	0
Disponibilidad	10	28	55	54
Intento de intrusión	7	24	159	9
Robos de información	2	1	1	7
Contenido Abusivo				11
Recolección de información				111
Sistema Vulnerable				224
Otros	13	55	99	39

Tabla 5. Ciberincidentes gestionados por tipología[33].

4.1. PUNTOS VULNERABLES

Las redes eléctricas actuales están compuestas por dos capas: la capa física, encargada de la generación y transporte de energía hacia el consumidor final, y la capa cibernética, compuesta por los sensores distribuidos a lo largo de la red, los sistemas de comunicación, monitorización y control.

El empleo de las TIC supone una gran ventaja para las Smart grids, sin embargo es también una de las mayores vulnerabilidades de los sistemas eléctricos. El equilibrio entre la demanda y la generación en las Smart grids se realiza gracias a los sistemas de monitorización y control, que están basados en protocolos particulares de OT y de IT. La gestión de las Smart grids es, por tanto, altamente dependiente de las TIC y, como consecuencia, susceptible de sufrir ciberataques por su condición de sector estratégico que puede tener infraestructuras críticas, presentándose como objetivos principales para Estados, grupos de delincuencia organizada, organizaciones ciberterroristas o incluso de hacktivistas, entre otros agentes.

En el ámbito de las Smart grids, los elementos que presentan mayor vulnerabilidad ante una amenaza cibernética son:

- Los sistemas SCADA, empleados en las labores de monitorización y control en tiempo real de las redes eléctricas inteligentes. El acceder a estos sistemas,

32 Ídem 31.
33 Ídem 31.

alterar las lecturas de los dispositivos de medida o realizar el envío de consignas de operación erróneas puede provocar graves daños en la operación de las Smart grids, como la pérdida de estabilidad, que derivarían en efectos en cascada, cuyo fin último sería la pérdida total del suministro eléctrico a una región.

- Los sistemas de medida avanzados (AMI), encargados de conectar los centros de control, responsables de operar la Smart grid, y los dispositivos de medida inteligentes (*Smart meters*) que proveen de información sobre el estado de la red al centro de control. La comunicación entre ambos dispositivos se realiza mediante protocolos basados en IoT (*internet of things*) por su facilidad de implementación. Las medidas registradas por los AMI se emplean para la previsión de la demanda energética del día siguiente y facturación al cliente, entre otras.
- Los Smart meters registran y almacenan información sobre los consumos energéticos de los clientes. Estos datos reflejan, en el fondo, los hábitos de consumo de los clientes y, por lo tanto, de su modo de vida. Aunque a priori los datos de los smart meters se emplean para labores de facturación, también pueden ser empleados por los gestores energéticos de viviendas para controlar el consumo de los dispositivos gestionables mediante las TIC (lavadora, TV, coche eléctrico, etc.), así como la generación de pequeñas unidades fotovoltaicas.
- Las redes de comunicaciones y sus elementos de comunicación, ya sean basadas en protocolos OT o IT.

Las consecuencias de un ciberataque se extienden desde grandes pérdidas económicas hasta el propio bienestar social e integridad física de los habitantes de un país. Además, en las nuevas redes eléctricas inteligentes, el robo de la información intercambiada entre los diferentes dispositivos puede dar lugar a problemas de seguridad para los clientes, ya que la información substraída está clasificada como sensible. Finalmente, con el nuevo Reglamento de Protección de Datos Europeo (GDPR), la pérdida o mala gestión de datos de carácter personal puede acarrear importantes sanciones económicas para las empresas proveedoras de servicio.

4.2. TIPOLOGÍAS DE ATACANTES

Según el informe de amenazas y tendencias 2019, publicado por el CCN-CERT[34], basándose en la operativa de las distintas agencias de ciberseguridad gubernamentales (INCIBE, CNPIC, MCCD, CCN-CERT) y europeo ENISA, fija una serie de agentes que interactúan en el ámbito del ciberespacio con fines que pueden generar ciberincidentes. Así en este informe se identifica como posibles agentes atacantes a:

- Los Estados y grupos patrocinados por Estados, que disponen de altos recursos y capacidades. Sus actuaciones han sido descritas en acciones referidas al ciberespionaje, la desinformación y a la capacidad de actuar sobre sistemas ICS. Esto último con dos acciones claras, la de obtener información mediante el ciberespionaje y la preparación de acciones de ataque futuras.

34 El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI.

- En este informe, se manifiesta que se ha percibido una actividad especial de acciones contra los sistemas ICS europeos. Pueden provocar también DoS, interrupción de servicios y sustracción de información. Basándose en un informe de *Crwodstike*, se establece que los países más activos en orden descendente han sido la República Popular de China, la República Popular de Corea del Norte, República Islámica de Irán, Rusia, Corea del Sur y la India. Resulta paradójico que en este informe no se cite a ningún país occidental.
- Delincuencia organizada en el ciberespacio, siendo este un medio cada vez más rentable por estas organizaciones. Se estima que esta actividad representa más del 90% de los ciberataques que se producen, con un peso del 0,85% PIB del mundo. Se centran fundamentalmente en dos actividades el *ransomware* y el minado de moneda electrónica (*cryptojacking/crytomining*). Se consolida la actividad de la prestación de servicios técnicos en el mundo cibernético para facilitar la comisión de delitos, en un modelo de negocio "*Crime as a Service*".
- Hacktivistas**,** basándose sobre todo en acciones de desfiguración de páginas Web y ataques de DDoS.
- Actores internos**,** como trabajadores y antiguos trabajadores descontentos que actúan contra la organización.
- Ciberterrorismo, en la actualidad no se tienen datos de acciones importantes, salvo las realizadas a nivel de financiación y reclutamiento por el ciberyihadismo. Si bien se espera que, con las vulnerabilidades asociadas a los ICS, la actividad terrorista contra estos sistemas crezca en los próximos años.

4.3. TIPOLOGÍAS DE ATAQUES

En los casos de ciberincidentes sufridos por Letonia, Irán y Ucrania, mencionados anteriormente, los principales intereses han sido la DoS, la interrupción de servicios y el sabotaje. En el caso del reciente ataque sufrido en Portugal por la compañía "edp", el principal objetivo ha sido el robo de información, el cifrado de la misma y el chantaje, utilizando para ello un ransomware.

Para conseguir los objetivos se han seguido ataques en el primer caso, métodos de acceso ilícito utilizando técnicas de ingeniería social, ataques dirigidos a la infraestructura de forma muy dirigida y específica a la tecnología ICS/SCADA de la infraestructura de distribución de potencia en el caso de Ucrania, basados en PLC's del fabricante Siemens.

También se ha utilizado la técnica de Phising dirigida a personal técnico y gerencial de la organización, para conseguir introducir *malware*, en especial ransomware.

En la consecución de los ataques, ha resultado de interés para los atacantes la explotación de vulnerabilidades de hardware y de software. Sin embargo, el tipo de ataque más consolidado durante los años 2017 y 2018 fueron las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés, Advanced Persistent Threat), permitiendo la escalada de privilegios y accesos en aquellos sistemas que se instalan tomando el control de los sistemas y pudiendo destruir, modificar, interceptar y exfiltrar información.

Se reproduce un cuadro publicado en el informe (CCN-CERT 2019, p.54), con los grupos de APT activos en diferentes industrias, entre el 1 de enero y 31 de mayo de 2018 en Alemania. Siendo especialmente relevante la quinta columna, por su relación directa con el sector energético.

Gov. organis.	Milit./ armaments	Opposition	Media	Energy	Finances	Video conf.	NGO	Univer-sities	High tech	Trans./ logistics	Aeron. & aerospace	Health	Law offices
APT12/ Num-beredP. APT28/ Sofacy APT29/ CozyBear APT32/ Ocean-Lotus APT37/ Reaper Bahamut BlueMush-room Cadelle/ Chafer Callisto Charming-Kitten Dark-Caracal DarkHotel Dropping-Elephant Emissary-Panda Extreme-Jackal Gamare-don Gaza-Cybergang Greenbug Hammer-Panda Infy KeyBoy Lapis/ Trans-parentTr. Longhorn Lotus-Panda Machete Micropsia Muddy-Water Naikon/ OverrideP. Leviathan OilRig Operati-onCleaver Project-Sauron Shamoon Snake Sowbug Tick TidePool/ Ke3chang Tonto Transpa-rentTribe Tropic-Trooper/ PirateP. Vermin Viceroy-Tiger	APT28/ Sofacy APT37/ Reaper AridViper BlueMush-room Callisto Charming-Kitten C-Major/ PureStrike Dark-Caracal Dropping-Elephant Gamare-don Gaza-Cybergang Hammer-Panda HelixKitten Lotus-Panda Machete Naikon/ OverrideP. Leviathan OilRig Operation-Cleaver Project-Sauron Snake	Ahtapot APT32/ Ocean-Lotus Bahamut BlackOasis Bookworm Charming-Kitten Dark-Caracal Ener-geticBear Flying-Dragon GroupS Infy Neo-dymium Operation-Cleaver Operation Manul Prome-thium ScarCruft Sima Stealth-Falcon SunTeam Temper-Panda ZooPark	APT28/ Sofacy APT32/ Ocean-Lotus Bahamut BlackOasis BugDrop Callisto Charming-Kitten Dark-Caracal DarkHotel Dropping-Elephant GazaCy-bergang Infy Olympic-Destroyer Operation Manul Sandworm ScarCruft Shrouded-Crossbow Stealth-Falcon SunTeam Tick	APT10 APT18/ Wekby APT29/ CozyBear Charming-Kitten Electric-Powder Emissary-Panda Energetic-Bear Gaza-Cybergang Greenbug HelixKitten Kraken/ Laziok Longhorn Machete Muddy-Water OnionDog Operation-Cleaver Sandworm Shamoon Tropic-Trooper/ PirateP.	APT18/ Wekby APT29/ CozyBear BlueMush-room Dark-Caracal Dropping-Elephant Emissary-Panda Energetic-Bear Equation-Group Gaza-Cybergang Hammer-Panda Longhorn OilRig Sandworm	APT18/ Wekby Codoso Emissary-Panda Hammer-Panda HelixKitten Longhorn Machete Muddy-Water OilRig Project-Sauron Thrip	APT29/ CozyBear APT37/ Reaper Callisto Charming-Kitten DarkHotel Hammer-Panda Honeybee Infy NilePhish Operation-Cleaver Rocket-Kitten	APT10/ menuPass BugDrop Charming-Kitten Codoso Dark-Caracal DarkHotel Greenbug DarkHotel Longhorn Leviathan Rocket-Kitten	APT18/ Wekby Charming-Kitten Codoso LEAD/ Winnti Tick	Cadelle/ Chafer NanHaiShu OilRig OnionDog Project-Sauron Shamoon	APT28 Dropping-Elephant Emissary-Panda Leviathan Hammer-Panda Greenbug Longhorn	APT10/ menuPass Leviathan LEAD/ Winnti	APT29/ CozyBear Codoso Dark-Caracal DeepPanda Leviathan

Ilustración 7. Grupos de APT's activos entre el 1 de enero y 31 de mayo de 2018 en Alemania. Fuente CCN-CERT 2019.

4.4. ORGANISMOS ESPAÑOLES COMPETENTES EN RESPUESTA A CIBERINCIDENTES EN EL ÁMBITO DE LAS INFRAESTRUCTURAS CRÍTICAS

En España, para los operadores críticos, en materia de ciberseguridad y en relación a los ciberincidentes, su conocimiento, gestión y respuesta, existen varias agencias

gubernamentales competentes según los distintos ámbitos. En concreto y en aplicación del *Real Decreto-ley 12/2018*, son los siguientes:

- CCN-CERT, Es el CSIRT, del Centro Criptológico Nacional, actúa en el ámbito del Sector Público general, autonómico y local, así como en sistemas que manejen información clasificada.

- INCIBE-CERT, actúa en el ámbito del sector privado y la ciudadanía y en coordinación con el CCN-CERT para aquellos organismos públicos afiliados a RedIris, la red académica y de investigación.

- ESP-DEF-CERT, del Mando Conjunto de Ciberdefensa (MCCCD), actúa en el ámbito de las redes, los sistemas de información de las Fuerzas Armadas, así como aquellas redes y sistemas que se le encomienden y que afecten a la Defensa Nacional.

- CNPIC, Tendrá conocimiento siempre y actuará en el ámbito de las IC y operadores críticos, cuyas capacidades de respuesta técnica se materializarán a través de los CSIRT de referencia.

En el caso de que el ciberincidente sea constitutivo de un delito, el CNPIC participará, por medio de su Oficina de Coordinación Cibernética (OCC), dando traslado de la información y las actuaciones realizadas a las Fuerzas y Cuerpos de Seguridad y a la Fiscalía para su investigación y judicialización, en su caso.

En el Cuerpo de la Guardia Civil se cuenta con la unidad especializada de la investigación, el Grupo de Delitos Telemáticos de la Guardia Civil (conocido por sus siglas, GDT), por parte del Cuerpo Nacional de Policía se cuenta con la Brigada Central de Investigación Tecnológica (conocida por sus siglas, BIT).

Para facilidad de los distintos usuarios, el Consejo Nacional de Ciberseguridad ha publicado la “Guía Nacional de Notificación y Gestión de Ciberincidentes”[35], que establece un sistema de ventanilla única para que los usuarios de los distintos ámbitos descritos anteriormente puedan participar los ciberincidentes a un único punto.

En la Ilustración 8 puede verse el flujograma que debería seguir un OC, ya sea público o privado para notificar el ciberincidente en la ventanilla única y cómo sería el ciclo de vida, desde su notificación hasta que se inicia la investigación por las FCS y la Fiscalía.

35 Recuperado de https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes, Fecha: 22 de mayo de 2020.

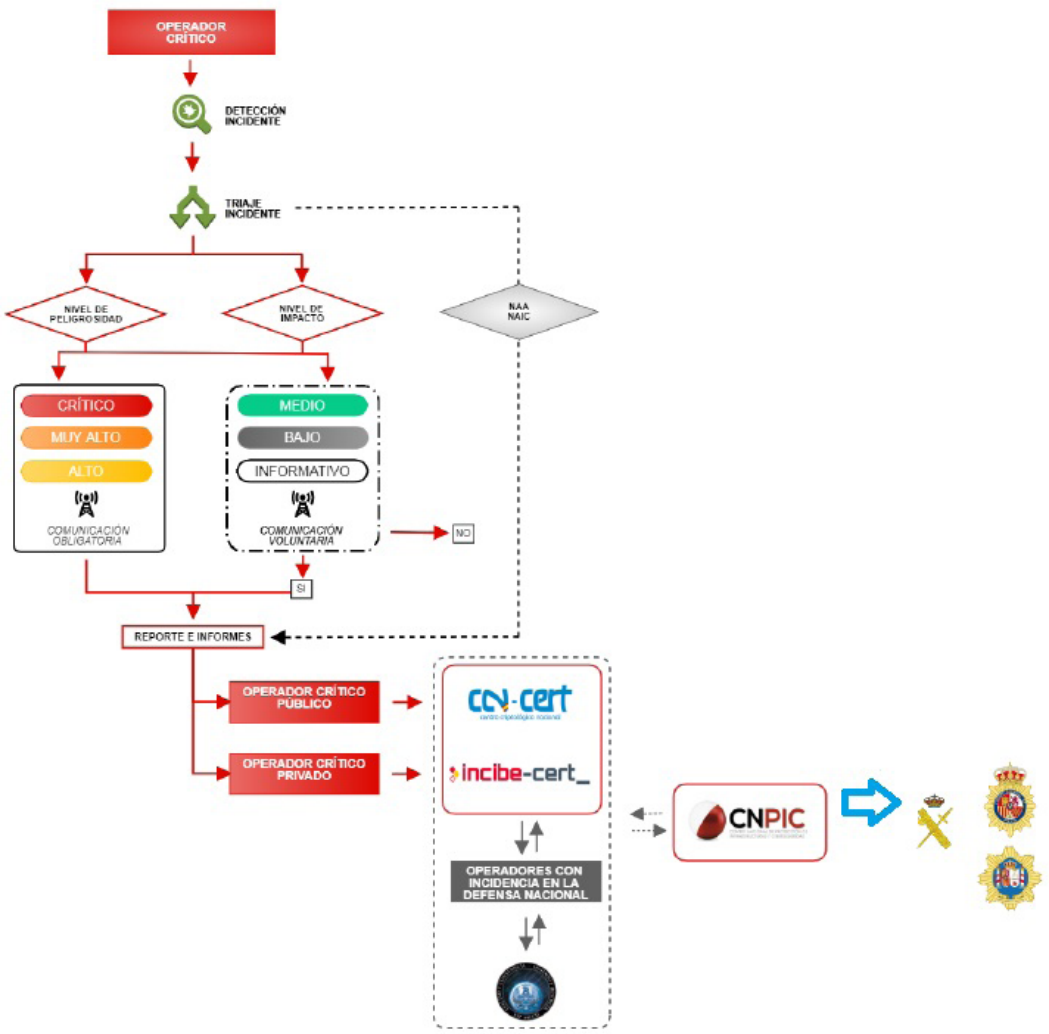

Ilustración 8. Flujograma de gestión y notificación de ciberincidentes en el ámbito PIC[36].

5. CONCLUSIONES

Las tecnologías de la comunicación se han integrado dentro de la estructura del sistema eléctrico dando lugar a redes inteligentes capaces de realizar una gestión más eficiencia de la energía. Sin embargo, la presencia de las TIC supone también un gran reto para las Smart grids en materia de seguridad. Dado el carácter esencial de los sistemas eléctricos como proveedores de servicios, y su condición de infraestructura crítica, el presente documento recoge un compendio de la normativa existente en materia de seguridad en el ámbito de las instalaciones críticas y, más concretamente, la que tiene como objetivo el sector energético eléctrico, así como de la normativa que a lo largo de los últimos años ha configurado el estado del actual sistema eléctrico. Para poder entender las amenazas y vulnerabilidades a las que se enfrentan las redes eléctricas inteligentes, se ha desarrollado un apartado descriptivo del sector eléctrico. Finalmente, se han mostrado las principales vulnerabilidades y amenazas sufridas por las Smart grids. A pesar de que a lo largo de la última década se han producido

36 Versión ampliada por los autores del artículo, en referencia al publicado en la Guía nacional de notificación de Ciberincidentes en su p. 38.

numerosos ataques a diferentes instalaciones críticas pertenecientes a los sistemas eléctricos, no existe en la actualidad jurisprudencia al respecto debido a la complejidad en la detección.

En España se posee un sistema centralizado para la atención de los ciberincidentes en el ámbito de las PIC; se ha mostrado qué principales agencias gubernativas tienen competencia y prestan apoyo a los OC ante los ciberincidentes y también los agentes jurídicos y policiales especializados en la persecución de aquellos delitos que sean realizados por medio de ciberincidentes.

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos.
AMI	Infraestructura de Medida Avanzada (Advanced Metering Infraestructure).
APT	Advanced Persistent Threat.
BIT	Brigada de Investigación Tecnológica, del Cuerpo Nacional de Policía.
CCN	Centro Criptológico Nacional.
CCN-CERT	Equipo de respuesta ante incidentes, del Centro Criptológico Nacional.
CNPIC	Centro Nacional de Protección de Infraestructuras y Ciberseguridad.
COSEM	Companion Specification for Energy Metering.
DCS	Sistema de Control Distribuido.
DLMS	Device Language Message Specification.
DSN	Departamento de Seguridad Nacional.
EDITE	Equipo de Investigación Tecnológica de la Guardia Civil
EDP	Energía de Portugal.
ENISA	La Agencia Europea de Seguridad de las Redes y de la Información.
EPCIP	Programa Europeo de Protección de las Infraestructuras Críticas.
ESN	Esquema Nacional de Seguridad.
G3-PLC	Protocolo estándar de comunicación evolucionado de PLC.
GDPR	Reglamento Europeo de Protección de Datos.
GDT	Grupo de Delitos Telemáticos de la Guardia Civil.
IC	Infraestructura Crítica.
ICE	Infraestructura Crítica Europea.
ICN	Infraestructura Crítica Nacional.
ICS	Sistema de Control Industrial.

INCIBE	Instituto Nacional de Ciberseguridad.
INCIBE-CERT	Equipo de respuesta ante incidentes del INCIBE.
LIPIC	Ley de Protección de Infraestructuras Críticas.
MCCD	Mando Conjunto de CiberDefensa.
OCC	Oficina de Coordinación Cibernética, del CNPIC.
OCNP-PIC	Organismo de Coordinación Nacional de Protección de Infraestructuras Críticas.
OSGP	Protocolo abierto de Smart grid.
PAO	Plan de Apoyo Operativo.
PEPIC	Plan Europeo de Protección de Infraestructuras Críticas.
PES	Plan del Sector Estratégico.
PLC	Controlador Lógico Programable.
PNPIC	Plan Nacional de Protección de las Infraestructuras Críticas.
PPE	Plan de Protección Específico.
PRIME	Protocolo de Medida de la Evolución de la potencia de línea.
PSO	Plan de Seguridad del Operador.
RDPIC	Reglamento de Protección de las Infraestructuras Críticas.
REE	Red Eléctrica de España.
SCADA	Sistema de Control y Adquisición de Datos Avanzados.
TIC	Tecnologías de la Información y la Comunicación.

BIBLIOGRAFÍA

Avance del informe del sistema eléctrico español 2019. Red Eléctrica de España. https://www.ree.es/es/datos/publicaciones/informe-anual-sistema/avance-del-informe-del-sistema-electrico-espanol-2019

(CCN-CERT, 2019) Informe de Amenazas y Tendencias, 2019. Centro Criptológico Nacional. Centro Nacional de Inteligencia de España. 2019. Recuperado el 22 de mayo de 2020, de https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj6k93_p9DpAhUcDWMBHSdNBq4QFjAAegQIGxAB&url=https%3A%2F%2Fwww.ccn-cert.cni.es%2Finformes%2Finformes-ccn-cert-publicos%2F3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019%2Ffile.html&usg=AOvVaw3-58PmX9iFAucPLKd62WO5

Circular 7/2019. Comisión Nacional de Mercado y la libre Competencia. Boletín Oficial del Estado. *Circular 7/2019, por la que se aprueban las instalaciones tipo y los valores unitarios de referencia de operación y mantenimiento por elemento de inmovilizado*

que se emplearán en el cálculo de la retribución de las empresas titulares de instalaciones de transporte de energía eléctrica. (5 de diciembre de 2019). https://www.cnmc.es/sites/default/files/2782108_23.pdf

Clean energy for all Europeans Package. Directorate-General for Energy (European Commission) (26 de julio de 2019) https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans, fecha de visita 25/05/2020.

Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311, pp. 29313 a 29424.

(*Departamento de Seguridad Nacional, 2019*) Informe Anual de Defensa Nacional 2019. Departamento de Seguridad Nacional 2019. Obtenido de https://www.dsn.gob.es/es/file/4037/download?token=bAFRfTyx Fecha 22 de mayo de 2020.

(Directiva Europea 2008/114/CE) UE Directiva COM /114/2008. (s.f.). *Comisión Europea.* Obtenido de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114&from=ES

(ESN, 2017) GOBIERNO DE ESPAÑA. *Real Decreto 1008/2017, Estrategia de Seguridad Nacional 2017.* https://www.boe.es/eli/es/o/2019/02/21/pci161

GOBIERNO DE ESPAÑA, MINPRE. (DICIEMBRE de 2017). ESTRATEGIA DE SEGURIDAD NACIONAL. MADRID, MADRID, ESPAÑA.

GOBIERNO DE ESPAÑA, MINPRE. (2019). ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. MADRID, MADRID, ESPAÑA.

GOBIERNO DE ESPAÑA MINT PPE y PPO. (18 de Septiembre de 2015). *GOBIERNO DE ESPAÑA BOE.* Obtenido de https://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf

GOBIERNO DE ESPAÑA. RD 704/2011. (28 de Mayo de 2011). https://www.boe.es/boe/dias/2011/05/28/pdfs/BOE-A-2011-9284.pdf

GOBIERNO DE ESPAÑA. Real Decreto 1008/2017 (s.f.). *Real Decreto 1008/2017, Estrategia de Seguridad Nacional 2017.* https://www.boe.es/eli/es/l/2011/04/28/8/con

GOBIERNO DE ESPAÑA. Orden PCI/487/2019 (s.f.). *Orden PCI/487/2019, Estrategia Nacional de Ciberseguridad 2019.* https://www.boe.es/eli/es/o/2019/04/26/pci487

GOBIERNO DE ESPAÑA. Orden PCI/161/2019 (s.f.). *Orden PCI/161/2019, Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave.*

GOBIERNO DE ESPAÑA. PCI/179/2019 (s.f.). *PCI/179/2019, Estrategia Nacional contra el Terrorismo 2019.* https://www.boe.es/boe/dias/2019/02/26/pdfs/BOE-A-2019-2638.pdf

GOBIERNO DE ESPAÑA, MINPRE. (2015). ESTRATEGIA DE SEGURIDAD ENERGETICA NACIONAL. MADRID, MADRID, ESPAÑA. https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-energ%C3%A9tica-nacional

GOBIERNO DE ESPAÑA. Ley 17/2007 (s.f.). *Ley 17/2007 del Sector Eléctrico.* (4 de julio de 2007). https://www.boe.es/buscar/pdf/2008/BOE-A-2008-1184-consolidado.pdf

GOBIERNO DE ESPAÑA. Ley 17/2013 (s.f.). *Ley 17/2013 Garantía del suministro e incremento de la competencia en los sistemas eléctricos insulares y extrapeninsulares.* (29 de octubre de 2013). https://www.boe.es/eli/es/l/2013/10/29/17

GOBIERNO DE ESPAÑA. Ley 24/2013 (s.f.). *Ley 24/2013 del Sector Eléctrico.* (26 de diciembre de 2013). https://www.boe.es/eli/es/l/2013/12/26/24/con

GOBIERNO DE ESPAÑA. Real Decreto 223/2008 (s.f.). *Real Decreto 223/2008 Condiciones técnicas y garantías de seguridad en líneas eléctricas de alta tensión y sus instrucciones técnicas complementarias ITC-LAT- 01 a 09.* (15 de febrero de 2008). https://www.boe.es/eli/es/rd/2008/02/15/223

GOBIERNO DE ESPAÑA. Real Decreto 134/2010 (s.f.). *Real Decreto 134/2010 Procedimiento de resolución de restricciones por garantía de suministro* (12 de febrero de 2010). https://www.boe.es/eli/es/rd/2010/02/12/134

GOBIERNO DE ESPAÑA. Real Decreto-ley 9/2013 (s.f.). *Real Decreto-ley 9/2013 Medidas urgentes para garantizar la estabilidad financiera del sistema eléctrico* (12 de julio de 2013). https://www.boe.es/eli/es/rdl/2013/07/12/9

GOBIERNO DE ESPAÑA. Real Decreto-ley 413/2014 (s.f.). *Real Decreto-ley 413/2014 Regulación de la actividad de producción de energía eléctrica a partir de fuentes de energía renovables, cogeneración y residuos* (6 de junio de 2014). https://www.boe.es/eli/es/rd/2014/06/06/413

Gundu M.Z.; Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, vol. 169, Elsevier. https://doi.org/10.1016/j.comnet.2019.107094

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

(Ley PIC, 2011) GOBIERNO DE ESPAÑA. Ley 8/2011. (s.f.). *Ley 8/2011, para la protección de las infraestructuras críticas.* Recuperado el 23 de mayo de 2017, de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

UE Directiva COM/0698/2004. (20 de Octubre de 2004). *COMISION EUROPEA.* Obtenido de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004DC0698&from=ES

UE Directiva COM/0701/2004. (20 de Octubre de 2004). *Comisión Europea.* Obtenido de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004DC0701&from=ES

UE Directiva COM/0702/2004. (20 de Octubre de 2004). *Comisión Europea.* Obtenido de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004DC0702&from=EN

UE Directiva 1148/2016/UE Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión

UE Directiva NIS COM/1148/2016. (6 de Julio de 2016). *Comisión Europea.* Obtenido de https://www.boe.es/doue/2016/194/L00001-00030.pdf

UE Directiva 2003/54/CE. Diario Oficial de la Unión Europea (junio 2003). https://www.boe.es/doue/2003/176/L00037-00056.pdf

UE Reglamento 2019/943, del Parlamento Europeo y del Consejo, relativo al mercado interior de energía. Diario Oficial de la Unión Europea (5 de junio 2019). https://www.boe.es/doue/2019/158/L00054-00124.pdf

UE Reglamento 2016/679, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas. Diario Oficial de la Unión Europea (27 de abril de 2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

Fecha de recepción: 28/05/2020. Fecha de aceptación: 15/07/2020