PLAN DE PREPARACIÓN FRENTE A LOS RIESGOS EN EL SECTOR ELÉCTRICO EN ESPAÑA

Tabla de contenido

Lista de acrónimos y abreviaturas.

Acrónimo/abreviatura	Significado
ACER	*Agency for the Cooperation of Energy Regulators*, Agencia de Cooperación de los Reguladores de la Energía de la Unión Europea.
AEMET	Agencia Estatal de Meteorología.
ARN	Autoridad Reguladora Nacional, la Comisión Nacional de los Mercados y la Competencia.
ARPSI	Áreas de Riesgo Potencial Significativo de Inundación.
BRIF	Brigadas de Refuerzo en Incendios Forestales.
CECOEL	Centro de Control Eléctrico de Red Eléctrica.
CEO	*Chief Executive Officer,* director ejecutivo.
CFO	*Chief Financial Officer*, director financiero.
CME	*Corona Mass Ejection (solar flare),* eyección de masa coronal.
CNMC	Comisión Nacional de los Mercados y la Competencia.
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas.
CORES	Corporación de Reservas Estratégicas de Productos Petrolíferos.
CORESO	Centro de Coordinación Regional (CCR) y proveedor de servicios de los Gestores de las Redes de Transporte (TSO) nacionales.
CSIRT	*Computer Security Incident Response Team,* Equipo de respuesta ante incidentes de seguridad.
CSN	Consejo de Seguridad Nuclear.
DSO	*Distribution System Operator*, gestor de la red de distribución.
EAS	*European Awareness System,* sistema de detección europeo de ENTSO-E
ECG	*Electricity Coordination Group*, Grupo de Coordinación de la Electricidad.
ENS	*Energy Not Served*, energía no servida.
EENS	*Expected Energy Not Served*, cantidad de electricidad no servida.
ENTSO-E	*European Network of Transport System Operators for electricity,* Red Europea de Gestores de Redes de Transporte de Electricidad.
ENTSOG	*European Network of Transport System Operators for gas,* Red Europea de Gestores de Redes de Transporte de Gas.
ERIE	Equipo de Respuesta Inmediata en Emergencias.
ERSE	*Entidade Reguladora dos Serviços Energéticos,* autoridad reguladora de Portugal.
FCSE	Fuerzas y Cuerpos de Seguridad del Estado.
GIETMA	Grupo de Intervención en Emergencias Tecnológicas y Medioambientales.
GEO	Grupo Especial de Operaciones.
GNL	Gas Natural Licuado.
HVDC	*High-voltage Direct Current*, corriente continua de alta tensión.
IDAE	Instituto para la Diversificación y el Ahorro de la Energía.
IGN	Instituto Geográfico Nacional.
INACN	Inventario Nacional de los Activos Críticos Nacionales.
INCIBE	Instituto Nacional de Ciberseguridad.
INE	Instituto Nacional de Estadística.
IPCEI	*Important Projects of Common European Interest*, Proyecto Importante de Interés Común Europeo.
LOLE	*Loss of Load Expectations*, Previsión de Pérdida de Carga, en horas.

mbLg	Magnitud a partir de la amplitud de la fase Lg, unidad de medida de la fuerza de un terremoto.
MIBEL	Mercado Ibérico de la Electricidad.
MIBGAS	Mercado Ibérico del Gas.
MRPFL-U	Modo regulación potencia-frecuencia limitado a subfrecuencia.
EEMM	Estados Miembros de la Unión Europea.
MVA	Megavoltamperio.
NGTS	Normas de Gestión Técnica del Sistema.
NIEPI	Número de interrupciones equivalentes de la potencia instalada en media tensión.
NRBQ	Nuclear, Radiológico, Biológico y Químico.
O&M	Operación y Mantenimiento.
OCC	Oficina de Coordinación de Ciberseguridad.
OCR	*Outage Coordination Region*, región de coordinación de cortes.
OHL	*Overhead Line*, línea aérea.
OMIE	Operador del Mercado Ibérico – Polo Español.
OMS	Organización Mundial de la Salud.
PEGLEM	Plan General de Emergencias del Estado.
PGM	*Power Generation Module*, módulo de generación eléctrica.
Plan (+SE)	Plan + Seguridad para tu Energía (+SE).
PNPIC	Plan Nacional para lo Protección de Infraestructuras Críticas.
PNIEC	Plan Nacional Integrado de Energía y Clima 2021-2030.
PO	Procedimiento de Operación.
PEVOLCA	Plan de Emergencias Volcánicas de Canarias.
RCC	*Regional Coordination Centre*, Centro de Coordinación Regional.
RCDE	Régimen de Comercio de Derechos de Emisión.
Red Eléctrica	Red Eléctrica de España, S.A.U.
RITE	Reglamento de Instalaciones Térmicas en los Edificios.
PPR	Plan de Preparación frente a Riesgos.
RTE	*Réseau de Transport d'Électricité.*
SETNP	Sistemas Eléctricos de los Territorios No Peninsulares.
SNS	Sistema Nacional de Salud.
SoA	*Statement of Applicability*, Declaración de Aplicabilidad.
SOC	*Security Operations Centre*, Centro de Operaciones de Seguridad.
SOR	System Operation Region, Region de Operación del Sistema.
STA	*Short-Term Adequacy,* Cobertura a Corto Plazo.
SWE	*Southwestern Europe*, Sudoeste de Europa.
TEDAX	Técnico Especialista en Desactivación de Artefactos Explosivos.
TEDAX-NRBQ	TEDAX-Nuclear, Radiológico, Biológico y Químico.
TIEPI	Tiempo de interrupción equivalente de la potencia instalada en media tensión.
TIM	Tiempo de Interrupción Medio.
TNP	Territorio No Peninsular.
TSO	*Transmission System Operator*, gestor de la red de transporte.
UE	Unión Europea.
UGE	Unidad de generación de electricidad.
UME	Unidad Miltar de Emergencias.
USR	Usuario Significativo de la Red.

Información general.

Autoridad Competente.

Tal y como se notificó a la Comisión Europea en marzo de 2020, la Autoridad Competente responsable de llevar a cabo las tareas contenidas en el Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo de 5 de junio de 2019, incluida la elaboración del Plan de Preparación frente a los Riesgos en el Sector Eléctrico en España, es el Ministerio para la Transición Ecológica y el Reto Demográfico.

Dentro del mismo, la persona titular de la Dirección General de Política Energética y Minas será el punto de contacto a estos efectos.

Región de Operación del Sistema a la que pertenece España y Estados Miembros integrados en ella.

El sistema eléctrico español está conectado con el de Portugal, Francia, Andorra y Marruecos.

La creciente conectividad entre EEMM da lugar a una mayor interdependencia de todos los países de la zona síncrona europea. En consecuencia, disponer de una mayor capacidad de intercambio de electricidad con los países vecinos proporciona mayor seguridad de suministro, mayor eficiencia y competencia entre sistemas vecinos y una mejor integración de las energías renovables.

De esta forma, los diferentes TSO deben cooperar para operar adecuadamente sus sistemas, considerando que la creciente interconexión conduce al mercado único de la electricidad. El mercado único se organiza en torno a las regiones de operación.

Región de Operación del Sistema de Europa Sudoccidental (SWE SOR)

Se define una región de operación del sistema como el ámbito geográfico que recoge un grupo de Estados miembros cuyos TSO comparten un mismo centro de coordinación regional a que se refieren los artículos 35 y 36 del Reglamento (UE) 2019/943.

De acuerdo con la Decisión 5/2022 de la Agencia de Cooperación de los Reguladores de la Energía sobre la definición de regiones de operación del sistema, España queda integrada en la región suroeste de operación del sistema, o South West Europe SOR (SWE SOR).

En concreto, Portugal, España y Francia conforman esta región.

Red Eléctrica, el TSO español, es accionista de CORESO SA, que actualmente es uno de los Centros de Coordinación Regional que coordina los flujos de electricidad para todos los Operadores de Redes de Transporte de la UE.

En el sector eléctrico, España también participa en el Grupo de Alto Nivel sobre Interconexiones para el Sudoeste de Europa, junto con la Comisión Europea, Portugal y Francia.

Introducción.

Este documento se elabora para dar cumplimiento a las obligaciones establecidas en los artículos 10, 11 y 12 del Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo de 5 de junio de 2019 sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE.

El Plan de preparación frente a los riesgos en el Sector Eléctrico en España (PPR) tiene por objetivo identificar los posibles riesgos que puedan afectar a la seguridad del suministro del sector eléctrico y establecer las medidas de actuación oportunas que permitan hacer frente a dichos riesgos. Es por ello por lo que se configura como el instrumento que recoge las medidas nacionales, regionales y, en su caso, bilaterales frente a los riesgos y las consecuencias planteadas por las crisis de electricidad.

Este PPR se elabora una vez obtenido el resultado de un análisis de escenarios de crisis de electricidad liderado por el TSO español. Inicialmente, el ámbito de análisis de este escenario de crisis de electricidad fue la España peninsular, si bien desde entonces han tenido lugar dos revisiones:

- Se ha modificado el alcance del PPR.
- Se ha adaptado la elección de escenarios.

Aunque la mayoría de los escenarios de crisis de electricidad se analizan específicamente para la Península Ibérica (directamente interconectada con Francia, Portugal, Andorra y Marruecos), se han incluido otros escenarios para abordar el resto de los territorios (los territorios no peninsulares y sus sistemas eléctricos, o SETNP), entre los que se encuentran las erupciones volcánicas.

De este modo, el PPR se aplica en todo el territorio español y en todos sus sistemas eléctricos. Esto significa que su ámbito geográfico incluye no sólo la Península Ibérica (directamente interconectada con Francia, Portugal, Andorra y Marruecos), sino también todos los territorios no peninsulares y sus sistemas eléctricos (SETNP), que incluyen:

- Islas Baleares.
- Islas Canarias.
- Ceuta.
- Melilla.

Lo anterior está exceptuado en la medida en la que el TSO no aplica en los territorios no peninsulares (TNP) la adaptación de programas de intercambio internacional, ya que los TNP no se interconectan con ningún sistema eléctrico de otro Estado Miembro.

Como medida adicional, resulta relevante destacar la adaptación del programa de intercambio con la península a través de la línea HVDC que conecta Baleares con la Península, tanto como medida preventiva en caso de crisis de origen natural, como medida de mitigación de crisis en el Sistema Eléctrico Balear.

El hecho de que el sistema peninsular y los SETNPS coexistan es un tema relevante porque el marco legal para la operación del sistema en cada uno es ligeramente diferente. Considerando las diferencias de naturaleza y tamaño entre sistemas, los procedimientos de operación de los SETNP no son tan extensos como los de la Península Ibérica y presentan algunas particularidades

derivadas de su naturaleza aislada, además de que existen diferencias en el funcionamiento del mercado.

Finalmente, para reducir la vulnerabilidad en estos sistemas aislados, España no sólo los incluye en el PPR, sino que sigue tres líneas de actuación adicionales en estos sistemas:

a) Implementar sistemas de almacenamiento de energía, como plantas hidroeléctricas de bombeo reversible, para reforzar la seguridad del suministro, proporcionar seguridad al sistema y ayudar a la integración de energías renovables no gestionables.
b) Desarrollar nuevas interconexiones entre islas para que éstas se apoyen mutuamente entre sí.
c) Mejorar el mallado de la red, proporcionando vías alternativas de suministro en caso de desabastecimiento.

Considerando todo esto, resulta necesario señalar que el artículo 16 del Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, establece que todas las medidas que se adopten para prevenir o mitigar las crisis de electricidad deberán ajustarse a las normas que rigen el mercado interior de la electricidad y el funcionamiento del sistema.

En relación con esto, por una parte, se ha incluido una descripción de las medidas que se ajuste a los requisitos de transparencia, claridad, proporcionalidad y no discriminación. Por otra parte, y sin perjuicio de lo anterior, esa transparencia también debe tener en consideración que en determinados casos la naturaleza de la información es confidencial. Todas estas consideraciones han sido tenidas cuenta a la hora de redactar las medidas concretas descritas en este plan.

Por último, para la elaboración del presente documento, tal y como establece el artículo 10.1 del Reglamento 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, se ha articulado un mecanismo de consulta a diferentes agentes del sector eléctrico.

Estructura del Plan

El contenido de este plan se alinea con lo recogido en los artículos 10, 11 y 12, así como en el Anexo del Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo de 5 de junio de 2019.

El PPR se estructura en nueve capítulos, que incluyen la información que se detalla a continuación:

I. El capítulo primero introduce el sistema energético español, centrándose en los sistemas eléctrico y gasista, incluye una descripción de las diferentes interconexiones internacionales y recoge otras cuestiones relevantes de seguridad del suministro.

II. El capítulo segundo establece qué es una crisis de electricidad, determina en qué condiciones el gobierno declarará como "crisis" un evento que tenga impacto en el suministro eléctrico y recoge otras cuestiones relevantes relacionadas con la declaración de crisis de electricidad.

III. El capítulo tercero se centra en los escenarios de crisis de electricidad. Incluye un resumen de los escenarios de crisis identificados a nivel nacional, recogiendo una explicación para la selección de aquellos que se consideran más probables para España y para descartar el resto. También incluye aquellas consideraciones relacionadas con los posibles impactos regionales de los escenarios seleccionados.

IV. El capítulo cuarto aborda el marco legal, tanto a nivel de la UE como a nivel nacional.

V. El capítulo quinto describe los sujetos que participan y tienen responsabilidades en relación con el plan. Se hace una referencia específica a la Autoridad Competente y el Coordinador de Crisis.

VI. El capítulo sexto recoge las diferentes acciones y respuestas que se pueden aplicar durante las diferentes crisis de electricidad. Incluye información sobre los desencadenantes de las crisis, así como los diferentes niveles de intensidad que se pueden aplicar para cada acción.

VII. El capítulo séptimo presenta en tablas los procedimientos planificados y las acciones aplicables en los diferentes escenarios de crisis seleccionados, incluyendo acciones preventivas y preparatorias. Estas tablas servirán como referencia rápida para cada agente en caso de una crisis de electricidad.

VIII. El capítulo octavo describe las diferentes consultas realizadas durante la preparación y revisión del PPR, así como el análisis de los comentarios y opiniones proporcionados por las partes interesadas.

IX. El capítulo noveno aborda las simulaciones que se realizan en relación con las crisis de electricidad, centrándose en:

   a. Simulacros de operación del sistema eléctrico, preparados por el TSO y realizados con distintas frecuencias.

   b. Ejercicios relacionados con la ciberseguridad, preparados por INCIBE-CERT.

1. El sistema energético español: perspectiva general de las infraestructuras.

La energía en todas sus formas (incluida la electricidad y la calefacción/refrigeración) es esencial para todos los ciudadanos. En una crisis de electricidad, nadie puede ignorar los impactos y consideraciones transversales. Gas y electricidad van de la mano y esto debe conducir a un enfoque holístico.

El PPR tiene en cuenta la influencia que tienen tanto otras formas de energía en el sistema eléctrico como la electricidad en otros sistemas energéticos.

La primera cuestión cuando se habla de energía es que el suministro energético requiere de infraestructuras que vinculen los lugares donde se genera la energía con aquellos donde se consume.

El Sistema Eléctrico Español.

El suministro de energía eléctrica se define como la entrega de energía a través de las redes de transporte y distribución mediante contraprestación económica en las condiciones de regularidad y calidad que resulten exigibles. Las actividades destinadas al suministro de energía eléctrica son: generación, transporte, distribución, servicios de recarga energética, comercialización e intercambios intracomunitarios e internacionales, así como la gestión económica y técnica del sistema eléctrico. El sistema eléctrico español está constituido por una red de transporte, a la que se conectan varias redes de distribución, conectándose a estas redes todos los demás agentes del sistema.

Una característica relevante en la electricidad es que históricamente generación y consumo debían ser simultáneos. Esto está cambiando a medida que se instalan cada vez más soluciones de almacenamiento, que reducen la brecha entre generación y demanda y que permiten utilizar e integrar más generación procedente de fuentes de energía renovables.

Red Eléctrica, como TSO español, tiene el papel de velar por este equilibrio entre generación y demanda. Para desarrollar esta función como operador del sistema, Red Eléctrica realiza todas las actividades necesarias para garantizar que la energía producida por los generadores sea transportada hasta las redes de distribución en condiciones de calidad, garantizando la seguridad y continuidad del suministro.

Red Eléctrica tiene también el rol de transportista único, es decir, es propietario y responsable del transporte eléctrico en alta tensión. Esta responsabilidad incluye obligaciones para desarrollar y ampliar la red de transporte, realizar su mantenimiento y gestionar el transporte de electricidad entre sistemas exteriores y la península española, así como garantizar el acceso de terceros a la red de transporte en igualdad de condiciones.

Actualmente, la red de transporte está constituida por más de 44.000 kilómetros de líneas de alta tensión, incluye más de 6.000 posiciones de subestaciones y tiene una capacidad de transformación que supera los 93.000 MVA[1].

[1] Información elaborada con datos provisionales a enero del 2024, relativa al Informe del Sistema Eléctrico de 2023 y publicada en la siguiente página web: https://www.sistemaelectrico-ree.es/informe-del-sistema-electrico/transporte/instalaciones-de-la-red-de-transporte

La red de transporte evoluciona y crece constantemente, adaptándose a los desafíos actuales a los que enfrenta el sistema eléctrico. Esto mismo ocurre con las redes de distribución y con el mix de generación.

A continuación, se muestra una tabla que recoge la evolución en cifras del sistema de transporte desde 2017 en adelante. La información se refiere a las líneas de alta tensión que conforman la red de transporte del sistema eléctrico español.

Líneas de alta tensión.

km circuitos	2017	2018	2019	2020	2021	2022	2023
km circuitos 400 kV	21.735	21.737	21.748	21.764	21.768	22.013	22.057
km circuitos 220 kV	19.694	19.788	19.906	19.939	20.121	20.161	20.192
km circuitos <220 kV	2.587	2.739	2.792	2.860	2.879	2.892	2.973
Total	**44.015**	**44.264**	**44.446**	**44.563**	**44.768**	**45.066**	**45.223**

Fuente: Red Eléctrica de España, S.A.U.[2]

En esencia, la red de transporte es la columna vertebral del sistema eléctrico y sirve como enlace con otros sistemas eléctricos. Las conexiones internacionales son una de las herramientas más relevantes que cualquier sistema puede utilizar para garantizar el suministro eléctrico necesario a sus usuarios.

Interconexiones internacionales

Fuente: Red Eléctrica de España, S.A.U.[3]

[2] Tabla de elaboración propia a partir de los datos obtenidos de https://www.sistemaelectrico-ree.es/informe-del-sistema-electrico/transporte/instalaciones-de-la-red-de-transporte

[3] https://www.ree.es/es/red21/refuerzo-de-las-interconexiones

La conexión a otros sistemas eléctricos ayuda a abordar la seguridad del suministro y reduce los riesgos de interrupción del suministro. Así, la generación de los países vecinos puede ayudar en caso de demandas mayores inesperadas o ayudar a restablecer el equilibrio en el sistema en caso de interrupciones imprevistas por el lado de la generación.

El sistema eléctrico español conecta directamente con otros cuatro países, en concreto:

- ***Estados miembros de la UE (sistema eléctrico europeo):***
    - Portugal.
    - Francia.
- ***Terceros países:***
    - Andorra.
    - Marruecos.

Algunas situaciones tienen consecuencias más allá de las fronteras de cualquier Estado Miembro y se manifiestan en los países vecinos, por lo que una mayor coordinación y cooperación entre ellos puede ayudar enormemente ante una situación de crisis de electricidad.

El mercado eléctrico europeo integrado, por su propia naturaleza, ha sido diseñado y funciona según el principio básico de interdependencia de todos los países de la zona síncrona europea.

La creciente conectividad entre EEMM sólo ayuda a aumentar esta interdependencia. Tener una mayor capacidad de intercambio de electricidad con los países vecinos proporciona una mayor seguridad de suministro, una mayor eficiencia y competencia entre dichos sistemas y una mejor integración de las energías renovables. La importancia de las interconexiones eléctricas es aún mayor para los países periféricos, como España, para los que este tipo de infraestructuras se convierten en una pieza imprescindible para el desarrollo de un sistema eléctrico adecuado que garantice sus necesidades de suministro, en cantidad y calidad, presentes y futuras.

Actualmente, las conexiones internacionales entre España y Francia suman una ratio de interconexión[4] del del 4,7% a través de los Pirineos Orientales.

Debido a estas interconexiones y su crecimiento planificado, cualquier crisis de electricidad y cualquier medida adoptada en respuesta a ellas puede afectar a otros EEMM.

Por ejemplo, en los últimos años han acontecido determinadas situaciones que han tenido impactos transfronterizos y han dado paso a pérdidas de sincronismo relevantes dentro del sistema eléctrico europeo:

i. El 4 de noviembre de 2006, un incidente en Alemania afectó a otros Estados Miembros, incluidos Francia, Bélgica, los Países Bajos, Italia y España. Esto provocó una pérdida de carga de 2,5 GW en España y cientos de consumidores se quedaron sin electricidad durante el incidente. El suministro en España volvió a niveles normales pasados 40 minutos.
ii. El 8 de enero de 2021, un incidente en Croacia provocó la separación de dos zonas del Área Síncrona de Europa Continental. Esto dio lugar a importantes desviaciones de frecuencia en ambas áreas. Sin embargo, la rápida coordinación de los TSO mitigó las posibles caídas, sin un impacto significativo en el suministro de energía de los

[4] Ratio de interconexión internacional = capacidad de interconexión internacional / potencia instalada correspondiente a 2023. Dato proporcionado por el TSO.

consumidores. Los TSO de España y Francia[5] informaron a las 14:12 horas de la activación de un intercambio compensatorio coordinado de aproximadamente 1.400 MW para evitar la sobrecarga de la línea de 400kV Vic-Baixas tras la pérdida del enlace HVDC Baixas – Santa Llogaia nº1 y nº2, de forma que Red Eléctrica aumentó la producción y RTE disminuyó la producción de sus sistemas.

iii. El 24 de julio de 2021, un incendio forestal en Francia derivó en la desconexión de los sistemas de transmisión de Portugal, España y de una pequeña parte de Francia del Área Síncrona de Europa Continental. Esto provocó el disparo de diferentes interconectores entre Francia y España, lo que provocó un deslastre de carga automático, seguido de acciones coordinadas por parte de los TSO afectados. Esto dio lugar a un deslastre de carga de 3,6 GW en España, un deslastre de carga de 0,7 GW en Portugal y un deslastre de carga de 0,07 GW en Francia. La resincronización con Europa continental se produjo después de 32 minutos.

Almacenamiento.

Otra herramienta clave que se encuentra actualmente en desarrollo es el almacenamiento. Las soluciones de almacenamiento energético irán ganando relevancia dado que ayudan a adaptar la generación y el consumo, integrando la generación renovable al sistema y aportándole más flexibilidad y equilibrio. En la actualidad, cada vez entran en funcionamiento más soluciones que incluyen almacenamiento. Una de las actividades que cada vez más emplea esta solución es el autoconsumo. También pueden citarse a modo de ejemplo las instalaciones híbridas (que combinan generación y almacenamiento) y las instalaciones de almacenamiento independientes, que actualmente están entrando en funcionamiento.

El Sistema Gasista Español.

La red española de transporte de gas está integrada por más de 13.300 kilómetros de gasoductos de alta presión. La red de gasoductos cuenta además con diecinueve estaciones compresoras que permiten el paso del gas desde los distintos puntos de entrada del Sistema hasta sus destinos finales, elevando la presión del gas hasta los 72/80 bar.

El sistema gasista español comparte muchas de sus características con el sistema eléctrico, pero también presenta varias peculiaridades destacables.

Las diferencias más relevantes son esencialmente que:

- La generación y el consumo no son simultáneos. Por ello, el almacenamiento juega un papel relevante en el suministro de gas.
- El gas es una fuente de energía externa que, con carácter general, España importa al sistema. Tanto las interconexiones internacionales como las plantas de regasificación juegan un papel muy relevante en el sistema.

En este sentido, las infraestructuras más relevantes del sistema gasista son sus plantas de regasificación, sus conexiones internacionales y sus instalaciones de almacenamiento.

[5] Red Eléctrica de España, S.A.U. (Red Eléctrica) y Réseau de Transport d'Électricité (RTE).

Plantas de regasificación.

En 2017, España tenía en funcionamiento seis plantas de regasificación. La ubicación de las plantas de regasificación a lo largo de todo el litoral español, y su nivel de ocupación actual, proporciona una total flexibilidad en el suministro de gas natural en el sistema español. Esta distribución a lo largo del litoral también ayuda a cumplir las exigencias en materia de diversificación de sus orígenes. Hay una distribución uniforme de los puntos de entrada para que se pueda importar gas desde todos los lugares.

En 2023 entró en operación la planta de regasificación de Musel.

La distribución de las plantas de regasificación en operación y construidas aparece reflejada en el siguiente mapa.

Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico - Plan de Acción Preventivo del sistema gasista español 2023-2026.

Las plantas se concentran en la costa atlántica (en el norte de España) en Galicia, Asturias y el País Vasco y en la costa oriental del Mediterráneo, en Cataluña, Comunidad Valenciana y Andalucía. En la costa sur del Atlántico, en Huelva, también hay una planta de regasificación.

La capacidad de emisión acumulada (regasificación y carga de cisternas) de las seis plantas es de 6.862.800 m³ (n)/h (1.916 GWh/día). La planta de "El Musel" proporciona una capacidad de emisión de 800.000 (n)/h adicional.

La siguiente tabla muestra las características técnicas de las plantas en operación:

		Almacenamiento GNL		Capacidad carga cisternas	Atraques	
Planta regasificación	Capacidad máxima vaporización (Nm³/h)	Nº tanques	m³ GNL	GWh/día	Nº atraques	m³ GNL
Barcelona	1.950.000	6	760.000	15	2	266.000
Huelva	1.350.000	5	619.500	15	1	175.000
Cartagena	1.350.000	5	587.000	15	2	266.000
Bilbao	800.000	3	450.000	5	1	270.000
Sagunto	1.000.000	4	600.000	11	1	266.000
Mugardos	412.800	2	300.000	11	1	266.000
Musel	800.000	2	300.000	9	1	266.000
Total	7.662.800	27	3.616.500	81	9	Hasta 270.000

Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico - Plan de Acción Preventivo del sistema gasista español 2023-2026.

Almacenamiento subterráneo.

En España existen cuatro almacenamientos subterráneos de gas natural: Serrablo, Gaviota, Yela y Marismas.

Los almacenamientos subterráneos son infraestructuras clave en las que se almacenan reservas de gas natural para poder ajustar la oferta a la demanda y hacer frente a los picos de consumo que se puedan producir a lo largo del año por variaciones estacionales u otros factores. El gas se almacena bajo tierra, aprovechando antiguos depósitos, o se inyecta en acuíferos profundos o en cavidades generadas en formaciones salinas.

La capacidad útil de los almacenamientos subterráneos fue de más de 35.342 GWh en 2022. La capacidad máxima de inyección asociada a estos almacenamientos es de 129 GWh/día, mientras que la capacidad de extracción es de 190 GWh/día.

Interconexiones internacionales.

El sistema gasista español cuenta con seis interconexiones internacionales que unen la red española de transporte de gas con cuatro países diferentes. Estos puntos de entrada al sistema gozan de un alto grado de seguridad física, ya que no están sujetos a los riesgos asociados al transporte marítimo como pueden ser cierres de puertos, tormentas, etc.

España recibe gas natural del norte de África a través del gasoducto Magreb-Europa y del gasoducto Medgaz.

El gasoducto Magreb-Europa llega a Zahara de los Atunes (Cádiz). Este gasoducto entró en funcionamiento en octubre de 1996. Se trata de la conexión de mayor tamaño existente en el sistema con una capacidad de 444 GWh/día.

La terminal receptora de Medgaz es un gasoducto submarino de 200 kilómetros entre Argelia y España, que llega a la Península en Almería y contribuye a mejorar la seguridad del suministro en nuestro país y en el resto de Europa. Desde noviembre de 2015, la conexión internacional de Almería por Medgaz tiene una capacidad de importación de 290 GWh/día.

Badajoz es el primer punto de conexión entre España y Portugal. El otro está en Tuy (Pontevedra). En 2012 vio la luz el punto de conexión virtual con Portugal (llamado VIP.PT), que engloba las capacidades de los puntos de interconexión física de Tuy y Badajoz.

Ambas conexiones internacionales con Portugal operan en el mercado como una única conexión, denominada VIP Ibérico.

Finalmente, existen dos puntos de conexión entre España y Francia.

La primera conexión es el gasoducto Larrau-Calahorra. Una parte importante de este gasoducto discurre por la Cordillera del Pirineo Navarro en cotas superiores a los 2.000 m. Tiene una capacidad física de intercambio de 165 GWh/día en ambos sentidos.

La segunda conexión internacional con Francia es Irún, que une el País Vasco con Francia. Tiene una capacidad de importación-exportación de 60 GWh/día.

Al igual que ocurre con las conexiones internacionales con Portugal, las interconexiones con Francia operan como una única conexión, denominada VIP Pirineos.

Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico - Plan de Acción Preventivo del sistema gasista español 2023-2026.

2. Crisis de electricidad.

En este capítulo se define qué es una crisis de electricidad y se detallan los requisitos y condiciones bajo los cuales la Autoridad Competente determinará como crisis un evento que tenga impacto en el suministro eléctrico.

También se determinan varios aspectos clave relativos a la declaración de crisis de electricidad, que son:

a) La persona/entidad que declara la crisis de electricidad.
b) La información que el Gobierno incluirá en la declaración y sus actualizaciones.
c) Las entidades que determinen los valores de los distintos indicadores empleados.

2.1 Definición de crisis de electricidad.

El Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, define una crisis de electricidad como *"una situación presente o inminente en la que se produce una escasez significativa de electricidad, determinada por los Estados miembros y descrita en sus planes de riesgo"*.

Para hacer frente a estas crisis es necesario identificarlas, realizar un análisis detallado de ellas y, por último, prepararse para cuando tengan lugar y para responder a sus potenciales impactos.

Para clasificar e identificar adecuadamente cualquier crisis de electricidad (tal y como se define en este PPR), la Autoridad Competente y/o el Coordinador de Crisis utilizarán determinados indicadores.

Indicadores de cobertura.

Red Eléctrica, ENTSO-E y RCC realizan evaluaciones de cobertura periódicamente, incluyendo estudios a largo y corto plazo.

Cuando un análisis de cobertura estacional u otra fuente cualificada proporcione información concreta y fiable de que puede producirse una crisis de electricidad en un Estado Miembro, la Autoridad Competente emitirá una alerta temprana a la Comisión. La Autoridad Competente también proporcionará información sobre las causas de la posible crisis de electricidad, sobre las medidas previstas o adoptadas para prevenir la crisis y sobre la posible necesidad de necesitar ayuda de otros Estados Miembros.

Análisis a largo plazo.

i. Perspectivas estacionales (realizadas por ENTSO-E)
   ENTSO-E analiza los posibles riesgos para la seguridad del suministro en Europa dos veces al año: para los períodos de verano e invierno. Debido a las posibles temperaturas muy bajas o altas y otras condiciones climáticas extremas, los inviernos y los veranos son los períodos más críticos para la red eléctrica.
   El análisis se realiza siguiendo una metodología probabilística basada en simulaciones de Monte Carlo. La información de entrada para el análisis la proporcionan los TSO.
   El principal indicador utilizado en este análisis es el LOLE.
ii. Análisis de cobertura mensuales (realizados por Red Eléctrica)

En los análisis de cobertura mensuales que realiza Red Eléctrica considera las hipótesis y previsiones más actualizadas disponibles para el Sistema Peninsular español. Los posibles riesgos de cobertura se evalúan con una metodología probabilística, abarcando el siguiente año móvil.
El principal indicador utilizado en este análisis es el LOLE.

Análisis a corto plazo.

i. Cobertura a corto plazo (realizada por RCC[6])
Para asegurar un buen equilibrio entre carga y generación, el papel del servicio de Cobertura a Corto Plazo (STA) consiste en:
   a. Realizar análisis de cobertura regional para detectar situaciones en las que se espera un riesgo de cobertura eléctrica en alguna de las áreas de control o a nivel regional (visión paneuropea), considerando posibles intercambios transfronterizos y límites de seguridad operativa. El diagnóstico también puede incluir recomendaciones para optimizar los intercambios transfronterizos.
   b. Realizar un análisis de cobertura regional en la región afectada, cuando lo activen los resultados del análisis STA transfronterizo o a petición del TSO (por ejemplo, en caso de un problema de escasez regional o de capacidades transfronterizas insuficientes). Para reducir el riesgo, el RCC propondrá acciones correctivas a los TSO asociados y las coordinará con los RCC afectados.

Para que los RCC puedan realizar dichos análisis de cobertura, cada TSO proporcionará a los RCC la información necesaria (carga total esperada, disponibilidad de módulos de generación de energía y límites de seguridad operativa) para su área de control. Estos datos se recopilan en la herramienta industrial STA, también llamada herramienta paneuropea o transfronteriza.
Los principales indicadores utilizados son el ENS y el LOLE.

ii. Evaluación continua de cobertura (realizada por Red Eléctrica)
Red Eléctrica realiza análisis de cobertura del sistema eléctrico calculando los márgenes de fiabilidad esperados considerando las previsiones más actualizadas disponibles sobre la demanda, generación renovable y las caídas de unidades de potencia. En caso de que Red Eléctrica detectara un posible riesgo de cobertura, informaría a la Autoridad Competente.
Los principales indicadores utilizados por Red Eléctrica son el LOLE y el estándar de fiabilidad utilizado como referencia.

Evaluaciones de incidentes.

Ante una crisis de electricidad, Red Eléctrica realizará una evaluación general del sistema eléctrico considerando:

- Estado general del sistema incluyendo degradación de frecuencia, voltaje, reservas, etc.
- La pérdida de carga.
- Elementos de la red de transporte, incluidas las interconexiones con TSO vecinos.
- Instalaciones de generación de energía.
- Desacople de las redes.
- Pérdidas de herramientas e instalaciones.
- Apagones parciales o totales.

[6] https://www.coreso.eu/services/sta/

Red Eléctrica podrá solicitar información a los DSO y a las instalaciones de generación eléctrica para completar la evaluación.

Red Eléctrica informará a la Autoridad Competente de la situación general, de las medidas adoptadas y previstas para mitigar los problemas y del tiempo previsto para recuperar la situación normal.

Tras su evaluación, la Autoridad Competente podrá declarar una crisis de electricidad en los términos contemplados en el Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019. En este caso, procederá a notificar dicha declaración a la Comisión y a las Autoridades Competentes de los Estados Miembros dentro de la misma región. La información trasladada incluirá las causas del deterioro de la situación del suministro de electricidad, los motivos para declarar una crisis de electricidad, las medidas previstas o adoptadas para mitigarla y la necesidad de cualquier ayuda de otros Estados Miembros.

2.2 Condiciones para una crisis de electricidad.

Se considerará crisis de electricidad cualquier situación de falta de suministro eléctrico potencial o real cuando el indicador ENS, el indicador LOLE o ambos alcancen un determinado umbral. Como referencia temporal, en lugar del indicador LOLE, se podrá utilizar el indicador TIM[7], que es equivalente al anterior, pero expresado en minutos y no en horas.

Como regla general, para determinar si un incidente es o no una crisis de electricidad las autoridades utilizarán valores reales para los correspondientes indicadores a la hora de valorar un incidente.

No obstante, el uso de valores estimados puede ser necesario cuando no se dispone de mejor información.

Criterio para determinar si existe una crisis de electricidad y establecer su gravedad.

Habrá una crisis de electricidad cuando el LOLE o el ENS supera el umbral establecido para la clasificación de "insignificante."

Hay que tener en cuenta que es posible que la gravedad de un incidente sea diferente en función del indicador, pudiendo incluso ser clasificado como crisis en base a un indicador y no en base al otro.

En estas circunstancias la gravedad del incidente se corresponderá siempre con la de mayor grado, incluso cuando se utilicen valores estimados para cualquiera de los indicadores.

Indicadores y umbrales para la valoración.

Los valores específicos LOLE y EENS utilizados para la identificación de los escenarios de crisis son valores estimados, utilizados en la identificación de escenarios de crisis eléctrica, y no se pueden utilizar para evaluar el impacto de una crisis. Estos valores se han establecido siguiendo una metodología, aplicando una serie de suposiciones establecidas *ex-ante*, para valorar casos unos casos hipotéticos, es decir, los escenarios de crisis de electricidad.

En una crisis real, la situación es diferente. La gravedad y el impacto de la crisis vendrá determinada por las circunstancias y consecuencias reales del incidente. Para valorar estas consecuencias se emplearán los indicadores ENS y LOLE.

El indicador LOLE no solo se puede aplicar en la identificación de escenarios potenciales de crisis, sino que también es directamente aplicable a una crisis real porque lo que mide en todo momento es el tiempo de interrupción.

No ocurre lo mismo con el EENS ya que es un valor relativo que depende de la demanda que se haya fijado en las hipótesis del procedimiento de identificación de los escenarios de crisis. Es por eso por lo que resulta necesario emplear el ENS, que informa de la energía no suministrada en un incidente concreto en términos absolutos y que se adapta a la situación real del sistema eléctrico en cada año.

ENS es la energía no servida en una zona determinada y en un período de tiempo determinado. Es energía que no se suministra por insuficiencia de recursos para abastecer la demanda durante

[7] Tiempo de Interrupción Medio, conforme a lo establecido en el artículo 26 del Real Decreto 1955/2000, de 1 de diciembre.

el periodo en el que hay restricción de carga debido al evento de crisis de electricidad y se expresa en MWh.

Los umbrales para el indicador ENS que permitirán clasificar la gravedad de una crisis de electricidad son:

a) Desastrosa, cuando el indicador de la ENS sea el 0,25% de la demanda anual de España del año anterior en MWh o más.
b) Crítica, cuando el indicador ENS sea superior o superior al 0,05% e inferior al 0,25% de la demanda anual de España del año anterior en MWh.
c) Mayor, cuando el indicador ENS sea superior o superior al 0,01% e inferior al 0,05% de la demanda anual de España del año anterior en MWh.
d) Menor, cuando el indicador ENS sea igual o superior al 0,002% e inferior al 0,01% de la demanda anual de España del año anterior en MWh.
e) Insignificante, cuando el indicador ENS sea inferior al 0,002% de la demanda anual de España del año anterior en MWh.

Como referencia del volumen de energía no suministrada, los umbrales vendrán fijados por la demanda anual de España del año anterior al momento de producirse la crisis.

LOLE representa el número de horas en las que en una determinada zona los recursos son insuficientes para abastecer la demanda debido al evento de crisis de electricidad. Se expresa en horas.

Los umbrales para el indicador LOLE que permitirán clasificar la gravedad de una crisis de electricidad son:

a) Desastrosa, cuando el indicador LOLE sea de 168 horas o más.
b) Crítica, cuando el indicador LOLE sea mayor o igual a 48 horas e inferior a 168 horas.
c) Mayor, cuando el indicador LOLE sea mayor o igual a 12 horas e inferior a 48 horas.
d) Menor, el indicador LOLE es mayor o igual a 3 horas e inferior a 12 horas.
e) Insignificante, cuando el indicador LOLE sea inferior a 3 horas.

La gravedad de la crisis de electricidad se determinará utilizando la categoría más grave.

Otra información complementaria para informar de la gravedad de una situación.

De manera complementaria y con el único fin de resaltar la relevancia de una situación, también se podrán tener en consideración cualquiera de los siguientes indicadores:

i. Población afectada por la crisis, en número total o porcentaje.
ii. Consumidores vulnerables afectados por la crisis.
iii. Número de hogares en situación de pobreza energética que se ven afectados por la crisis de electricidad.

Por otra parte, en el caso de escenarios de crisis de electricidad que surjan o tengan una duración superior a una semana cualquiera de los siguientes indicadores también puede ayudar a analizar la gravedad de un incidente, junto con la ENS y la LOLE:

i. Variación de la demanda eléctrica para el período de referencia.
ii. Porcentaje de disponibilidad de combustible durante el período de referencia.
iii. Volumen y porcentaje de las reservas de combustible existentes para cualquiera de los combustibles empleados en la generación de electricidad.

2.3 Declaración de una crisis de electricidad.

Cuando tiene lugar una situación en la que el valor del indicador ENS, del indicador LOLE o en el que los valores de ambos indicadores se encuentren por encima del umbral mínimo establecido en el punto anterior, la Autoridad Competente declarará una crisis de electricidad.

La Autoridad Competente, previa consulta al TSO, notificará la declaración de crisis de electricidad a la Comisión Europea usando los canales gestionados por ECG lo antes posible.

La Autoridad Competente también podrá notificar la declaración a terceros países vecinos. Esta notificación será obligatoria si la Comisión considera que la crisis declarada tiene impactos transfronterizos y que la situación se convierte en una crisis regional.

2.3.1 Actualizaciones de la declaración de una crisis de electricidad.

La Autoridad Competente actualizará la declaración de crisis de electricidad por primera vez en un plazo de 24 horas cuando:

i. Se pasa de "potencial crisis de electricidad" a "crisis de electricidad".
ii. Hay un cambio en la clasificación de la gravedad de la crisis.
iii. Los impactos transfronterizos se manifiestan.

La Autoridad Competente o el Coordinador de Crisis podrán actualizar la declaración de crisis de electricidad en cualquier otro momento.

Adicionalmente, la Autoridad Competente o el Coordinador de Crisis podrán publicar cada 24 horas recordatorios de la declaración e información relevante con respecto a la misma.

2.3.2 Agentes que determinan el valor de los indicadores.

Gestor de la Red de Transporte (TSO).

Red Eléctrica proporcionará a la Autoridad Competente las evaluaciones y los indicadores establecidos en el apartado 2.1.

Autoridad Competente.

La Autoridad Competente podrá solicitar la colaboración de otros ministerios y organismos para recabar información adicional que permita determinar alguno de los siguientes indicadores:

i. Población afectada por la crisis, en términos absolutos o relativos.
ii. Consumidores vulnerables afectados por la crisis.
iii. Número de hogares en situación de pobreza energética que afectados directa o indirectamente por la crisis de electricidad.

De forma análoga, la Autoridad Competente podrá solicitar a ENAGAS (el TSO del sector del gas) y a CORES información para determinar:

i. El volumen de reservas de combustibles fósiles.
ii. La capacidad de almacenamiento.
iii. Porcentaje (%) de la disponibilidad total de combustible.

2.4 Otra información relevante relativa a las crisis de electricidad y sus fuentes.

La Autoridad Competente podrá solicitar a la AEMET información sobre las condiciones meteorológicas, el riesgo de incendios forestales y las predicciones meteorológicas que tengan en cuenta determinados escenarios de crisis.

La Autoridad Competente también podrá solicitar a los gobiernos regionales y locales información sobre la evolución de determinadas amenazas y/o crisis como incendios forestales o erupciones volcánicas y coordinarse con ellos para decidir qué acciones tomar y en qué momento.

Asimismo, podrá solicitar a los gobiernos regionales y locales información sobre:

i. Población afectada por la crisis, en número total o porcentaje.
ii. Información adicional sobre los hogares que pueden encontrarse en pobreza energética sufriendo directa o indirectamente la crisis de electricidad.

Por último, la Autoridad Competente podrá requerir a los órganos de seguridad pública y a las Fuerzas Armadas la información adicional que considere necesaria.

3. Escenarios de crisis de electricidad.

En este capítulo se identifican los diferentes escenarios de crisis de electricidad que pueden tener lugar en España.

Esta identificación comienza con una lista de 31 posibles escenarios determinados por ENTSO-E, que se clasifican en una de las nueve categorías siguientes:

- Ciberataques.
- Ataques, ya sean ataques físicos contra las infraestructuras o equipos, acciones llevadas a cabo por personal infiltrado o amenazas al personal clave.
- Eventos climáticos extremos.
- Desastres naturales.
- Escasez de combustible.
- Factor humano.
- Errores de mercado.
- Fallos técnicos.
- Otros escenarios de crisis.

A continuación, la Autoridad Competente y el TSO han analizado y evaluado los 31 escenarios siguiendo la metodología desarrollada por ENTSO-E.

Esta evaluación ha considerado dos aspectos relacionados con todas las crisis:

i. La probabilidad de que ocurra una crisis.
ii. El impacto de esa crisis.

Utilizando una matriz de impacto, el TSO ha evaluado los 31 escenarios posibles teniendo en cuenta su gravedad, en concreto, la probabilidad de que se produzca una crisis y el impacto de esta. La evaluación de cada escenario posible considera también la probabilidad de que tenga consecuencias transfronterizas.

España ha acabado identificando 10 escenarios como escenarios seleccionados para el PPR español y ha descartado el resto de la lista de 31 posibles escenarios de crisis de electricidad.

Este capítulo explica en detalle y justifica como se ha realizado la identificación de los escenarios nacionales para España, describiendo de forma resumida la metodología empleada en esta fase.

Para finalizarlo, se explican las razones que tiene España para descartar los demás escenarios de crisis.

3.1 Escenarios de crisis regionales.

Conforme a lo establecido en el artículo 6 del Reglamento (UE) 2019/941, ENTSO-E identificó y estableció los escenarios de crisis regionales que se encontraban en el informe *"Identification of regional electricity crisis scenarios"*.

El informe estableció 31 escenarios posibles, agrupados en nueve categorías principales, que se muestran a continuación:

Este informe presentaba un total de 31 posibles escenarios que se agruparon en 9 grandes categorías, tal y como se muestra a continuación:

I. Ciberataques:

a. Ciberataque a entidades conectadas a la red eléctrica – lo que supone un ataque contra sistemas TIC bien del TSO, de uno o más DSOs, de plantas de generación o de grandes consumidores.

b. Ciberataque a entidades no conectadas a la red eléctrica – lo que supone un ataque contra los sistemas TIC de sujetos del mercado eléctrico no conectados de manera directa a las redes, como, por ejemplo, plataformas de mercado.

II. Ataques:

a. Ataque físico a infraestructuras críticas – consiste en un ataque de naturaleza física haciendo uso de las vulnerabilidades de líneas eléctricas, transformadores, subestaciones, plantas de producción y/o centros de datos.

b. Ataque físico a infraestructuras de control – consiste en un ataque de naturaleza física haciendo uso de las vulnerabilidades de los centros de control principales o de reserva del TSO, de DSOs relevantes o de los centros de operaciones de las principales plantas de producción.

c. *Amenaza al personal clave* – En esta situación los afectados son parte del personal clave, por ejemplo, operadores del sistema, administradores de servicios TIC, personal con privilegios de alto rango, CEO, CFO, etc.) y se les coacciona a llevar a cabo una acción que desestabiliza el sistema.

d. Ataque desde dentro – se trata de sabotajes llevados a cabo por uno o más empleados de la propia empresa o de las subcontratas mediante una acción física o el uso indebido de los sistemas TIC.

III. Fenómenos meteorológicos extremos:

a. Tormenta solar – se trata de un evento Carrington o similar. En estas situaciones el sol produce una fuerte eyección de masa de la corona (CME). Los efectos serán más apreciables en los países del norte de Europa, aunque también habrá impactos significativos en centro Europa. Las Agencias Espaciales pueden predecir esto tipo de eventos con unos días de antelación.

b. Tormenta – consiste en una situación en el que una tormenta predicha aumenta su fuerza y extensión en una hora. El tamaño es tal que abarca desde Europa oriental a Europa occidental con una velocidad media del viento de al menos 150 km/h y con rachas que superan los 200 km/h.

c. *Ola de frío* – se produce en toda Europa una ola con temperaturas entre -10 y -20°C por debajo del promedio estacional, de modo que:

i. El agua en los depósitos (lagos, ríos, pantanos, etc.) se congela y se agotan las reservas.

ii. Hay ausencia de viento.

iii. Hay incrementos en la demanda como consecuencia del frío, en particular en los países con una importante penetración de medios de calefacción eléctrica.

iv. Hay una reducción en la generación como consecuencia de limitaciones en la capacidad de refrigerar los módulos térmicos de las redes de distribución/transporte (PGM[8]) porque las reservas de agua/líquido refrigerante están congeladas y/o surgen problemas operativos en los equipos de los módulos de generación e incluso el combustible que se emplea para la generación puede encontrarse congelado en algunos países.

v. Hay limitaciones en la generación como consecuencia de restricciones en la capacidad de refrigerar los módulos de generación porque las reservas de agua/líquido refrigerante están congeladas y/o surgen problemas operativos en los módulos de los equipos.

vi. La producción hidroeléctrica se ve reducida.

vii. Como consecuencia de las condiciones meteorológicas algunos elementos de red pueden verse sometidos a mayor tensión (por congelación, etc.) y que se fiabilidad se reduzca.

d. *Precipitaciones e inundaciones* – se producen fuertes lluvias durante varios días que provocan inundaciones en subestaciones y plantas de producción de energía eléctrica.

e. *Incidente invernal* - en esta situación se producen múltiples fallos en líneas eléctricas aéreas como consecuencia de la acumulación de nieve o hielo, que provocan fallos en los elementos aislados de las líneas aéreas (OHL) o la caída física de los cables. Asimismo, pueden ocurrir fallos en las torres como consecuencia de la acumulación de hielo o nieve que pueden dar lugar a múltiples disparos en los circuitos. Las avalanchas de nieve en las regiones montañosas también pueden provocar múltiples disparos en los circuitos.

f. *Fallos múltiples por fenómenos meteorológicos extremos* – el desencadenante puede ser:

i. Múltiples fallos provocados por unas condiciones meteorológicas extremas.

ii. Un conjunto de componentes de la red que comienzan a fallar sin aviso por una ola de calor repentina en un breve periodo de tiempo, afectando a la distribución eléctrica.

g. *Ola de calor* – la ola de calor afecta la seguridad de suministro mediante:

i. La reducción de capacidad de generación en las instalaciones de producción.

[8] Power Grid Modules – módulos de generación

ii. Provocando disparos repentinos en varias unidades de generación por refrigeración insuficiente de los módulos de generación.

La ola de calor afecta a la seguridad de las redes:

i. Sobrecargando determinados elementos que provoquen incidentes de tipo N-1[9] como consecuencia de fallos.

ii. Limitando la capacidad de las líneas por un aumento de la demanda asociada al aire acondicionado. Los recursos propios de los diferentes operadores del sector también pueden verse afectados.

La ola de calor puede verse acompañada de incidentes relacionados con:

i. Problemas de capacidad.

ii. Degradación estructural.

iii. Problemas de estabilidad en las infraestructuras.

h. *Sequía* – los niveles de agua bajos suponen una producción hidroeléctrica baja (con un numero crítico de instalaciones hidroeléctricas fuera de operación). También varias unidades térmicas de producción pueden verse obligadas a parar o reducir su generación como consecuencia de las limitaciones en su capacidad de refrigeración.

IV. Desastres naturales:

a. *Erupción volcánica* – este incidente supone la presencia de un volcán activo que previsiblemente vaya a producir una gran cantidad de ceniza. También se prevé que antes de la erupción se produzca actividad sísmica en las inmediaciones del volcán, aunque lo más probable es que sea con menos de una hora de preaviso.

b. *Terremoto* – puede tener lugar un terremoto de magnitud considerable que dañe las infraestructuras de transporte y distribución de energía o las instalaciones de producción.

c. *Incendio forestal* – los incendios se inician y se propagan por el calor y el viento. En algunos casos no pueden ser controlados durante semanas y se ven agravados por tormentas veraniegas puntuales y fuertes (que llevan asociados vientos fuertes y relámpagos que pueden propagar o crear nuevos focos).

Los incendios forestales no controlados pueden dar lugar a indisponibilidades o a que no se puedan operar determinadas unidades de generación, de transporte o distribución. Algunas de las posibles consecuencias son:

i. Incidentes masivos N-1 crean un efecto en cascada.

ii. Degradación estructural.

[9] Un fallo/incidente N-1 se define como un fallo simple de uno cualquiera de los elementos del sistema (grupo generador, línea, transformador o reactancia) (criterio N-1) – Ver- P.O. 1.1 Criterios de funcionamiento y seguridad para la operación del sistema eléctrico. En este caso el fallo de un equipo tiene un impacto tal sobre el sistema que acaba provocando una crisis y el fallo de otros elementos que agravan la crisis.

d. *Pandemia* – se trata de una propagación de una enfermedad a escala internacional. El personal del TSO podría verse afectado, así como el personal de las subestaciones, de las plantas de producción y de los DSOs, hasta el punto de no disponer de suficientes recursos humanos.

V. Desabastecimiento de combustible

a. *Desabastecimiento de combustibles fósiles (incluido el gas natural)* – el desencadenante tiene lugar durante un año que combina una alta demanda de combustible doméstico con unas reservas bajas. Puede ocurrir en alguno de los siguientes casos:

   i. Una interrupción prolongada en la producción de combustible nuclear.

   ii. Un fallo o cierre en el sistema de suministro del combustible, de carácter técnico o provocado.

   iii. Una limitación en la oferta por motivos de mercado, políticos y/o meteorológicos.

   iv. En el caso de combustibles importados, los estados de tránsito pueden incluso limitar más el combustible disponible con el objetivo de garantizar su propio suministro, lo que da lugar a una reducción significativa del combustible que llega a las plantas de generación afectadas.

   Esto coincide con la incapacidad de compensar las restricciones con el suministro de otras fuentes o proveedores. Adicionalmente, la producción a partir de instalaciones gestionables alternativas o la capacidad de importar energía puede verse restringida.

b. *Desabastecimiento de combustible nuclear* – el desencadenante tiene lugar durante el año, cuando simultáneamente hay una elevada demanda de electricidad y unas reservas bajas de combustible nuclear. Puede coincidir con indisponibilidades intermitentes tanto en la generación como en las interconexiones. Las causas pueden ser:

   i. Una interrupción prolongada en la producción de combustible nuclear.

   ii. Un fallo o cierre en el sistema de suministro del combustible, de carácter técnico o provocado.

   iii. Una limitación en la oferta por motivos de mercado, políticos y/o meteorológicos que impide la llegada de suficiente combustible a las plantas nucleares afectadas.

VI. Factor humano

a. *Error humano* – el desencadenante puede ser:

   i. Un error de los operadores que desconectan un elemento de esencial de la red.

   ii. En general, cualquier violación del criterio N-1 provocado por error humano.

b. *Huelga, disturbio, acción sindical* – el evento que inicia la crisis puede ser:

   i. Disputas de algún tipo que se escalen a acciones en industrias de tamaño considerable.

   ii. Que tengan lugar revueltas, bloqueos o disturbios sociales (sin tener en cuenta los motivos o causas)

VII. Errores del mercado:

a. *Interacción imprevista de las reglas del mercado* – el desencadenante será el comportamiento altamente inusual y extremo de algunos sujetos de mercado (entrando en una situación de pánico de mercado), posiblemente como resultado de alguna de las siguientes circunstancias:

   i. Cambios en algunas de las reglas de mercado o mecanismos en al menos un país que produjeran efectos indeseados en los mercados (como *gaming* o arbitrajes que vayan en detrimento de la seguridad del sistema).

   ii. Condiciones meteorológicas, de demanda o del sistema altamente inusuales con las que muchos de los sujetos del mercado no estén familiarizados.

      1. Las condiciones meteorológicas altamente inusuales pueden suponer temperaturas extremas durante 10 o más días consecutivos.

      2. Una demanda altamente inusual puede venir producida por una perturbación en la demanda que dure más de 10 días consecutivos y que venga provocada por motivos económicos, sociales o políticos.

b. *Flujo no deseado de electricidad* – el desencadenante es un flujo de energía mayor de lo planificado como consecuencia de una mayor producción de renovables (principalmente, solar y eólica) y otras condiciones externas, como redespachos regionales.

VIII. Fallos técnicos:

a. *Fallo técnico local* – el desencadenante es un fallo técnico local con impacto transfronterizo. Se trata de un incidente más grave que un tipo N-1, que podría derivar de:

   i. Un fallo de un elemento crítico (por ejemplo, un transformador o un componente relacionado con la estabilidad del sistema).

   ii. Fuegos o explosiones en una subestación.

b. *Perdida de los sistemas TIC en el funcionamiento en tiempo real* – en este tipo de crisis el evento desencadenante puede ser:

   i. La pérdida o indisponibilidad de una parte sustancial de las infraestructuras o sistemas de telecomunicaciones empleados en los sistemas y en la operación del sector eléctrico.

ii. La pérdida o indisponibilidad de uno o más sistemas TIC empleados en la planificación y operación en tiempo real del sistema eléctrico (por ejemplo, los sistemas de cálculo de seguridad de operación de las redes, las predicciones de generación renovable o las medidas del sistema).

c. *Múltiples fallos simultáneos* – se pueden producir alguno de los siguientes fallos:

i. Fallos en cables HVDC[10] que provocan la desconexión de varias plantas de producción dando lugar a una ratio de potencia perdida que supera los umbrales del escenario N-1.

ii. Fallos en subestaciones o líneas de transporte/distribución que provocan cortes de suministro de gran volumen a consumidores.

iii. Fallos simultáneos o muy próximos en el tiempo en múltiples equipos que superan los umbrales de seguridad y para los cuales el sistema no está preparado.

iv. Una amenaza al sistema desconocida. Esta amenaza se puede manifestar como consecuencia de que las pruebas offline no fueron suficientemente precisas o porque el escenario en cuestión no se estudió.

v. Una amenaza al sistema desconocida por el funcionamiento deficiente de los equipos de monitorización.

vi. La violación de un estándar/protocolo de seguridad como consecuencia de un error operacional o porque la respuesta de control no fue lo suficientemente rápida para preservar la seguridad del sistema.

vii. Fallos múltiples en activos de red que provocan la separación de una parte del sistema con insuficiente capacidad de generación.

viii. Cortocircuitos.

d. *Fallo en serie de equipos* – se produce cuando algunos de los elementos de las redes de transporte o distribución comienzan a mostrar comportamientos anómalos que incrementan el riesgo de fallo o que llevan a dichos fallos.

El análisis en algunos casos permite descubrir que la causa es un defecto sistemático, de fabricación, de instalación o de mantenimiento (componentes defectuosos en los interruptores de circuito en toda la serie, en particular los interruptores de cortocircuito, la instalación de algoritmos de protección erróneos, etc.). En consecuencia, todos los elementos del mismo tipo/serie de producción son susceptibles de sufrir el mismo fallo/defecto.

Además, el problema podría afectar a otros Estados Miembros.

IX. Otros:

a. Complejidad de los mecanismos de control del sistema eléctrico – el desencadenante de este tipo de crisis son fallos técnicos en los sistemas TIC, en

[10] High-Voltage Direct Current

los sistemas de comunicación o que un componente de protección de la red mande una señal a otras redes, unidades de producción o componente de los centros de control que dé lugar a un fallo en cascada, como consecuencia de la alta interdependencia entre sistemas altamente complejos.

b. *Accidente industrial/nuclear* – tiene lugar cuando se produce un accidente industrial, como un escape de contaminación radiológica resultado de una explosión en una planta nuclear o la emisión de contaminantes tóxicos de una planta química por una variedad de motivos (fallos técnicos, terremoto, sabotaje, ataque terrorista, error humano, etc.)

c. *Error inusualmente grande en la predicción de participación de renovables* – el desencadenante es una considerable diferencia entre la producción real y la prevista de las unidades renovables como consecuencia de errores inusualmente grandes en las predicciones, de errores en los datos de las propias previsiones o por cambios rápidos e imprevistos en el tiempo.

3.2 Metodología y justificación de la identificación de los escenarios de crisis nacionales.

3.2.1 Resumen.

A la hora de determinar cuáles son los escenarios de crisis de la electricidad que se deben tener en cuenta en este plan, se ha llevado un procedimiento de análisis y valoración de las 31 propuestas descritas en el punto 3.1 de este plan.

La escala de valoración de los escenarios empleada ha tenido en cuenta dos aspectos relativos a las crisis:

- La probabilidad de que se produzca una crisis.
- El impacto de esa crisis.

En relación con la **probabilidad de que tenga lugar**, las crisis se clasifican en:

I. **Muy probable** – si se cree que la frecuencia de ocurrencia es mayor de 0,5 por año o el tiempo máximo entre eventos es de menos de 2 años.

II. **Probable** – si se estima que tendrán lugar aproximadamente cada dos años. En concreto, la frecuencia de ocurrencia se sitúa entre el 0,2 y el 0,5 por año o el tiempo máximo entre eventos se sitúa en el intervalo de 2 a 5 años.

III. **Posible** – si se considera la crisis como una amenaza potencial. En este sentido, la frecuencia de ocurrencia se sitúa entre el 0,1 y el 0,2 por año o el tiempo máximo entre eventos se sitúa en el intervalo de 5 a 10 años.

IV. **Improbable** - si se prevé que la crisis es un evento muy raro. En concreto, la frecuencia de ocurrencia se sitúa entre el 0,01 y el 0,1 por año o el tiempo máximo entre eventos se sitúa en el intervalo de 10 a 100 años.

V. **Muy Improbable** - si se considera la crisis como una amenaza irrelevante o extremadamente rara. En este sentido, la frecuencia de ocurrencia se sitúa por debajo de 0,01 por año o el tiempo máximo entre eventos es de 100 años o más.

En relación con el **impacto** de la crisis se emplean dos indicadores para su valoración, que son:

I. **EENS – Expected Energy Not Served**. Se trata de la estimación de energía no suministrada y se expresa como un porcentaje sobre la demanda de energía anual.

II. **LOLE - Loss of Load Expectations**. Se trata de la estimación de pérdida de carga y se expresa en horas

Teniendo en cuenta estas tres variables (probabilidad, EENS y LOLE) se establece una valoración de los escenarios de crisis calificándolos como “Desastre”, “Crítico”, “Importante”, “Menor” o “Insignificante” y asignándoles la siguiente valoración en función de cada categoría:

Crisis scenario rating	Value *(used for regional scenario rating)*
Disastrous	**10**
Critical	**5**
Major	**2**
Minor	**1**
Insignificant	**0**

Fuente: Red Eléctrica de España, S.A.U.

Además, se ha valorado el potencial impacto trasfronterizo de las crisis consideradas. En la metodología se ha establecido el factor de dependencia transfronteriza (*Cross-border Dependency Rating o CBD Rating*), cuyo valor asignado depende de:

i. Si la crisis no tiene impacto en otros países (valor 1),
ii. Si dicha crisis puede ser susceptible de agravar una crisis que se esté produciendo simultáneamente en al menos otro país (valor de 1.2) o,
iii. Si es susceptible de provocar una crisis transfronteriza por causa directas o indirectas en al menos otro país (valor 2).

Cross-border dependency rating	Value	Description
None	1	The crisis has no impact on other countries, even if they are facing simultaneous crisis.
Minor	1.2	The crisis is susceptible to aggravate a simultaneous crisis in at least one other country, either through direct or indirect causes (cf. Article 3).
Major	2	The crisis is susceptible to generate a cross-border crisis in at least one other country, either through direct or indirect causes (cf. Article 3).

Fuente: Red Eléctrica de España, S.A.U.

Este factor de dependencia transfronteriza se emplea para corregir la valoración obtenida de los escenarios de crisis y así obtener la valoración final de dichos escenarios para los correspondientes Estados Miembros.

$$Valoracion\ Nacional = Valoracion\ Escenarios\ de\ Crisis\ \times CBD\ Rating$$

Aquellos escenarios de crisis que podrían tener un fuerte impacto en las interconexiones, e incluso provocar su pérdida, se han clasificado en la categoría "Mayor". Esta pérdida de la interconexión podría a su vez provocar una crisis en otro Estado Miembro (como un ataque intencionado a los centros de control, uno de los escenarios seleccionados españoles).

Los escenarios que podrían agravar una crisis simultánea en otro Estado miembro pertenecían a la categoría "Menor". Un ejemplo de ello en los escenarios seleccionados españoles es un escenario de incendio forestal que podría afectar tanto a Galicia como al norte de Portugal).

Por último, todos aquellos escenarios de crisis que no tuvieron impacto en otros Estados miembros se incluyeron en la categoría "Ninguno".

Finalmente, basándose en todas las consideraciones relacionadas con la probabilidad, el impacto y los efectos transfronterizos, se han evaluado los 31 escenarios propuestos por ENTSO-E.

3.2.2 Probabilidad de que ocurra una crisis.

La frecuencia con la que ocurre una crisis es una cuestión relevante. Cuanto más largo sea el período entre crisis, más tiempo habrá para realizar un análisis de los acontecimientos y adaptar los planes de preparación para ellos.

La clasificación utilizada al analizar la probabilidad de que ocurra una crisis considera la frecuencia con la que ocurre un evento. Los valores de frecuencia se cuantifican teniendo en cuenta el:

i. Número de eventos por año, y
ii. Número de años entre eventos individuales.

La siguiente tabla detalla la relación entre frecuencia y valor/clasificación:

Classification	Events per year	1 x in … years	Description/example of initiating event
Very likely	≥ 0.5	2 or less	event expected practically every year, e.g. winds/storms causing multiple failures of overhead lines may be expected nearly every year in some areas
Likely	0.2-0.5	2-5	event expected once in a couple of years, e.g. heat wave causing limits on output of open-loop water-cooled power plants, low water levels at hydro plants, higher load, etc.
Possible	0.1-0.2	5-10	event expected or taken into consideration as a potential threat, e.g. cyber or malicious attack
Unlikely	0.01-0.1	10-100	very rare event, e.g. simultaneous floods causing unavailability of generation, distribution and transmission infrastructure
Very unlikely	≤ 0.01	100 or more	event irrelevant, or extremely rare, e.g. earthquake causing a huge destruction of transmission, distribution and generation infrastructure

Fuente: Red Eléctrica de España, S.A.U.

3.2.3 Impacto de una crisis.

El alcance o tamaño de una crisis es la otra característica relevante. Los indicadores EENS y LOLE sintetizan la cantidad de electricidad no servida durante el incidente y el tiempo que dura la crisis.

Por un principio de prudencia, la clasificación más severa de los dos indicadores siempre determina la gravedad o el impacto de la crisis:

Classification	EENS% (of annual demand)	LOLE [hours]
Disastrous	≥0,25%	≥168
Critical	≥0,05% and <0,025%	≥48 and <168
Major	≥0,01% and <0,05%	≥12 and <48
Minor	≥0,002% and <0,01%	≥3 and <12
Insignificant	<0,002%	<3

Fuente: Red Eléctrica de España, S.A.U.

EENS es un indicador que se expresa en términos relativos (un porcentaje), lo que permite una mejor comparación entre escenarios.

El análisis de los escenarios nacionales utilizó datos de 2019 para fijar valores de los indicadores EENS y LOLE en el territorio continental (sistema interconectado).

El TSO representó cada escenario y lo tradujo en términos de energía no suministrada y duración del incidente. Con estos insumos, el TSO clasificó los 31 escenarios considerando los pasos descritos en los siguientes puntos.

3.2.4 Matriz de probabilidad e impacto.

Teniendo en cuenta ambos criterios, España ha empleado una matriz de probabilidad e impacto para analizar la relevancia de los 31 escenarios propuestos y seleccionar los incluidos en este Plan PPR.

En concreto, la combinación de ambos criterios permite clasificar los escenarios como Desastrosos, Críticos, Mayores, Menores e Insignificantes.

Los valores para la calificación del escenario de crisis se establecen en la siguiente tabla.

Crisis scenario rating	Value *(used for regional scenario rating)*
Disastrous	10
Critical	5
Major	2
Minor	1
Insignificant	0

Fuente: Red Eléctrica de España, S.A.U.

Considerando esto, la siguiente tabla representa la matriz de impacto de los 31 escenarios de crisis:

Impact		Likelihood				
EENS%	LOLE	Very likely	Likely	Possible	Unlikely	Very unlikely
Disastrous	Disastrous	Disastrous	Disastrous	Critical	Major	Minor
Disastrous	Critical	Disastrous	Critical	Critical	Major	Minor
Critical	Disastrous	Disastrous	Critical	Critical	Major	Minor
Disastrous	Major	Disastrous	Critical	Major	Major	Minor
Major	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Minor	Disastrous	Critical	Major	Major	Minor
Minor	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Insignificant	Disastrous	Critical	Major	Major	Minor
Insignificant	Disastrous	Disastrous	Critical	Major	Major	Minor
Critical	Critical	Disastrous	Critical	Major	Minor	Minor
Critical	Major	Critical	Critical	Major	Minor	Minor
Major	Critical	Critical	Critical	Major	Minor	Minor
Critical	Minor	Critical	Major	Major	Minor	Minor
Minor	Critical	Critical	Major	Major	Minor	Minor
Critical	Insignificant	Critical	Major	Major	Minor	Minor
Insignificant	Critical	Critical	Major	Major	Minor	Minor
Major	Major	Critical	Major	Major	Minor	Insignificant
Major	Minor	Major	Major	Minor	Minor	Insignificant
Minor	Major	Major	Major	Minor	Minor	Insignificant
Major	Insignificant	Major	Major	Minor	Minor	Insignificant
Insignificant	Major	Major	Major	Minor	Minor	Insignificant
Minor	Minor	Major	Minor	Minor	Insignificant	Insignificant
Minor	Insignificant	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Minor	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Insignificant	Minor	Minor	Insignificant	Insignificant	Insignificant

Fuente: Red Eléctrica de España, S.A.U.

3.2.5 Evaluación de la dependencia transfronteriza.

Al considerar la posible perspectiva regional de la crisis, las valoraciones de los escenarios de crisis (considerados inicialmente a nivel nacional) pueden cambiar. El valor asignado a un escenario de crisis aumenta cuando efectivamente tiene un impacto transfronterizo.

Para reflejar esta circunstancia, se utiliza el coeficiente *Cross-border Dependency Rating o CBD Rating* para corregir la valoración obtenida y así obtener la calificación final de los escenarios para los correspondientes Estados Miembros.

3.3 Escenarios seleccionados.

El análisis de los 31 escenarios de crisis posibles en el sistema eléctrico español se realiza a través de una matriz de impacto y probabilidad. La matriz es un mapa que identifica las diferentes áreas en las que aparecen los escenarios de crisis. El criterio para determinar estas áreas es la gravedad general del escenario.

España ha descartado escenarios de gravedad insignificante y ha tenido en cuenta todos aquellos escenarios en los que la gravedad alcanzaba un valor de al menos "Menor".

Con la participación y aportaciones de diferentes sujetos del sistema eléctrico y partes interesadas, así como del CNPIC, en diciembre de 2020 se analizaron los Escenarios de Crisis de Electricidad Nacionales.

El resultado de dicho análisis mostró que los siguientes escenarios se encuentran en la categoría "Menor":

a) ***Escenario 1 - Ciberataque contra entidades conectadas a la red eléctrica***.
b) ***Escenario 4 - Ataque físico a centro de control***.
c) ***Escenario 9 - Tormenta***.
d) ***Escenario 31 - Incendio forestal***.
e) ***Escenario 27 - Pandemia***.

Tras analizar las repercusiones transfronterizas, se identificaron los siguientes escenarios adicionales que se han incluido en el PPR:

f) ***Escenario 3 - Ataque físico a infraestructuras críticas***.
g) ***Escenario 15 - Fallo técnico local - incendio o explosión en un activo crítico***
h) ***Escenario 6 – Sabotaje por parte de personal crítico***.

Finalmente, el PPR español ha incluido una variación del escenario correspondiente a ciberataques, que considera un ciberataque a equipos críticos de control, protección y telecomunicaciones (*Ciberataque contra equipos críticos empleados en actividades de control, protección y telecomunicaciones*). La razón detrás de esto es que es un escenario que el TSO ha señalado que tiene similar posibilidad de ocurrir en España, siendo igualmente similares las probabilidades y consecuencias como el escenario Ciberataque contra entidades conectadas a la red eléctrica.

Aunque inicialmente era un escenario descartado, España ha incluido un último escenario en el PPR.

El 19 de septiembre de 2021, a las 15:12 (GMT), el volcán Cumbre Vieja entró en erupción en la isla de La Palma. El volcán expulsó al menos 159 millones de metros cúbicos de lava, que cubrieron más de 1.219 hectáreas de terreno, sepultaron 73,8 kilómetros de carreteras y afectaron 2.988 edificaciones[11].

La erupción duró 85 días y provocó graves daños en la isla, incluida una crisis en el suministro eléctrico.

[11] Información recogida en el INFORME SOBRELAS ACTUACIONES Y MEDIDAS EMPRENDIDAS TRAS LA ERUPCIÓN DEL VOLCÁN DE CUMBRE VIEJA (LA PALMA), SEIS MESES DESPUÉS DEL INICIO DE LA EMERGENCIA de junio de 2022 publicado por la Comisión mixta para la reconstrucción, recuperación y apoyo a la isla de La Palma.

Considerando esto, el escenario de ***erupción volcánica*** ahora forma parte del PPR.

Finalmente, los escenarios nacionales de crisis de electricidad seleccionados son los siguientes:

I. **Pandemia.**
II. **Tormenta extrema.**
III. **Ciberataque contra Sistemas de Control.**
IV. **Ciberataque contra equipos críticos empleados en actividades de control, protección y telecomunicaciones.**
V. **Ataque físico a infraestructuras críticas.**
VI. **Ataque físico a centro de control.**
VII. **Fallo técnico local - incendio o explosión en un activo crítico.**
VIII. **Sabotaje por parte de personal crítico.**
IX. **Incendio forestal.**
X. **Erupción volcánica.**

3.4 Escenarios de crisis nacionales descartados.

3.4.1 Escenarios nucleares (escasez de combustible y accidente nuclear). Reducción de la dependencia del suministro de combustible nuclear de terceros países.

En España hay siete reactores nucleares en funcionamiento, ubicados en cinco emplazamientos. La potencia instalada es de 7.398,7 MWe, lo que representa el 6,5% del total de potencia instalada. La electricidad producida por estos reactores supuso el 21,4% de la producción nacional total en 2019.

Accidente o avería nuclear (accidente nuclear industrial)

Las centrales nucleares deben cumplir una serie de requisitos que afectan a la seguridad nuclear de la instalación, desde dos perspectivas:

- Seguridad nuclear operativa o seguridad tecnológica y
- Seguridad en el control de materiales nucleares o seguridad física.

Considerando estas dos perspectivas, los eventos que pueden afectar la operación de una central nuclear pueden ser:

- Sucesos internos: como roturas de tuberías, fallos de equipos, incendios, proyectiles internos (partes de maquinaria que se desprenden y salen proyectadas a gran velocidad), etc.
- Sucesos externos: como condiciones climáticas extremas, terremotos, tsunamis, accidentes aéreos, viento (ciclones, huracanes, tornados), ondas expansivas, incendios, inundaciones, actividad criminal (sabotaje, intrusión, toma de rehenes y chantaje, ataque terrorista, amenazas de bomba), ocupación de la instalación, actos vandálicos, etc.), fallos de la red eléctrica exterior, etc.

En caso de huelga, el Ministerio para la Transición Ecológica y el Reto Demográfico, previo informe del CSN[12], establece los correspondientes servicios mínimos que deberán satisfacer el cumplimiento de los documentos oficiales que establezcan los requisitos y condiciones a los que las instalaciones están sujetas. Estos requisitos aparecen en la Autorización de la central nuclear.

El escenario ENTSO-E denominado "Accidente industrial o nuclear de gran impacto" supondría en el peor de los casos la pérdida de la generación eléctrica de una o varias plantas.

Escasez de combustible nuclear

España ha descartado el escenario de "escasez de combustible nuclear". Es poco probable y, aunque si alguna circunstancia condujera a un impacto prolongado en la cadena de suministro, no tendrá efectos significativos en la generación de electricidad de origen nuclear si las reservas físicas se mantienen dentro de los límites. Además, la planificación y preparación a largo plazo en la cadena de suministro de combustible proporciona a las autoridades un margen de acción y si fuera necesario, el sistema podrá trasladar a otras tecnologías el suministro cubierto por la generación nuclear de forma ordenada y planificada.

[12] Consejo de Seguridad Nuclear.

3.4.2 Ciberataques.

España no ha incluido el escenario de un ciberataque contra entidades no conectadas a la red eléctrica. Esta situación se produce cuando tiene lugar un ataque contra los sistemas TIC de sujetos del mercado eléctrico que no están conectados física ni directamente a las redes (por ejemplo, en las plataformas de mercado). La razón para no incluir este escenario es que, incluso si el ataque afectara a una pluralidad de agentes, no tendría un impacto significativo en el suministro físico. Si bien puede haber riesgos indirectos para el funcionamiento normal del mercado, estos no afectan directamente a las condiciones de suministro ni al funcionamiento de la red. Además, el TSO cuenta con una serie de herramientas para mantener la seguridad del suministro en estos casos.

3.4.3 Ataques.

España no ha incluido estos escenarios por la muy baja probabilidad de que ocurran. Además, el impacto esperado en términos de EENS es insignificante y menor en términos de LOLE.

Estos escenarios están muy localizados y, por tanto, limitados geográficamente.

3.4.4 Fenómenos meteorológicos extremos.

España no ha incluido estos escenarios porque, aunque la probabilidad de que se produzca algunos de ellos existe, el posible impacto en términos de EENS y LOLE se ha evaluado como insignificante según la metodología.

Además, los impactos transfronterizos también son poco probables. En el caso de las olas de calor y las sequías, uno de los principales factores impulsores de una crisis es la indisponibilidad de energía hidroeléctrica. En España, las centrales hidroeléctricas generan entre el 7 y el 11%[13] del total de electricidad. Esto significa que existen otras tecnologías para satisfacer la demanda en el funcionamiento diario y durante la crisis eléctrica.

i. **Tormenta solar -** este es un evento similar a Carrington. En estas situaciones, el sol produce una fuerte eyección de masa de corona. Los efectos serán más notorios en los países del norte de Europa, aunque también habrá impactos significativos en Europa central. El sur de Europa será la región menos afectada.

ii. **Ola de frío –** en esta situación, se produce una ola en toda Europa con temperaturas entre -10 y -20°C por debajo de la media estacional. Esta ola de frío tendría en teoría un menor impacto en España (y el resto de los países del sur de Europa), ya que es una región que presenta condiciones climáticas más suaves en general.

iii. **Precipitaciones e inundaciones –** en esta situación, se producen fuertes lluvias durante varios días provocando inundaciones en subestaciones y centrales eléctricas.

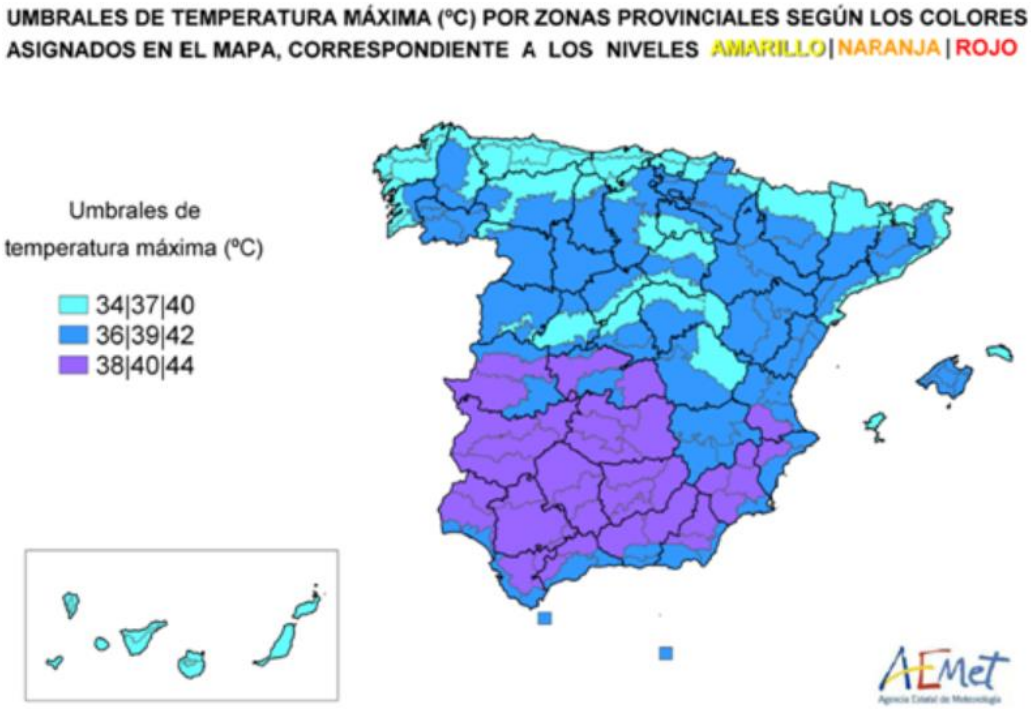
[13] Fuente: página web OMIE (https://www.omie.es/es/market-results/annual/daily-market/monthly-power?scope=annual&year=2023&system=1) La producción hidráulica en mercado Español en 2023 fue de 10,73%

Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico.

Debido a las condiciones climáticas más suaves en el sur de Europa, la probabilidad de que se produzcan inundaciones a gran escala es muy baja.
Además, el Mapa de Peligrosidad y Riesgo de Inundación muestra que las Área de Riesgo Potencial Significativo de Inundación cubren un área muy pequeña y por lo tanto el riesgo de que las inundaciones provoquen una crisis eléctrica y de que tengan impacto transfronterizo es cercano a cero. Como se muestra en el mapa, las regiones ARPSI representan sólo 10.357,54 km repartidos en una superficie de 505.944 km².

iv. **Incidente invernal** - en esta situación se producirían múltiples fallos en las líneas eléctricas aéreas debido a la acumulación de nieve o hielo. Esto podría provocar fallos en elementos aislados de las líneas OHL o en la caída física de los cables. Aunque la probabilidad de que se produzca este escenario existe, el posible impacto en EENS y LOLE se ha evaluado como insignificante según la metodología.

v. **Ola de calor** - una ola de calor puede afectar la seguridad del suministro al sobrecargar ciertos elementos que causan incidentes N-1 y limitar la capacidad de la línea o aumentar la demanda eléctrica debido a la demanda de energía asociada al aire acondicionado. Las reservas y los recursos propios de diferentes operadores también pueden verse afectados.



Fuente: AEMET (Ministerio para la Transición Ecológica y el Reto Demográfico.)

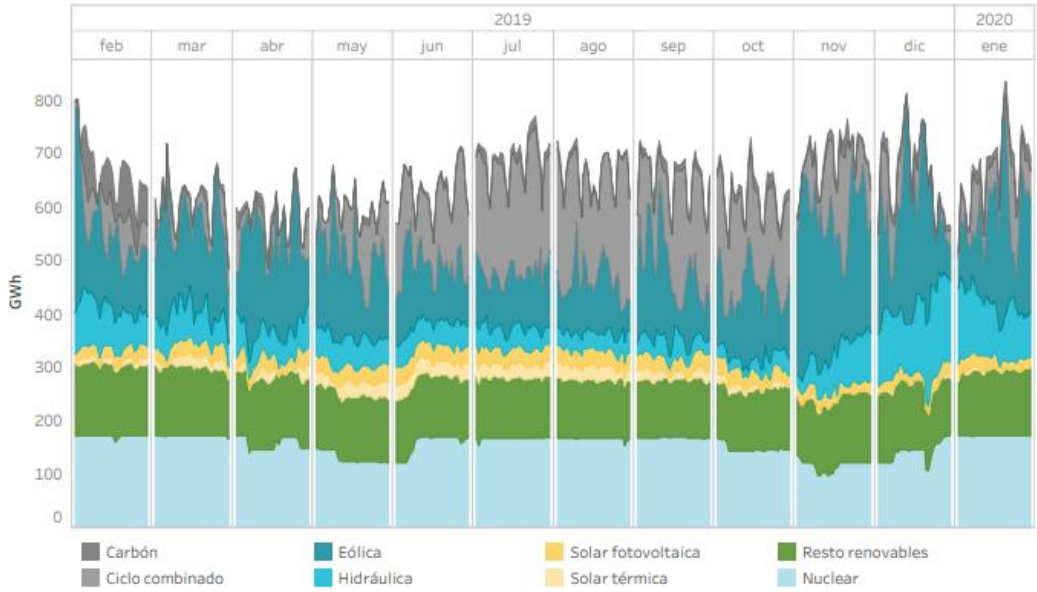
AEMET hace un seguimiento de las condiciones de calor en España. Ha clasificado las diferentes regiones de España según las temperaturas medias. Además, la agencia utiliza cuatro indicadores al estudiar las olas de calor:

a. Duración.
b. Número de provincias a las que afecta.
c. Temperatura máxima - temperatura máxima media medida en las diferentes estaciones meteorológicas para el día más caluroso.
d. Anomalía de la ola de calor, que es la diferencia entre la temperatura umbral y la temperatura máxima.

Con la información sobre el impacto de una ola de calor y su extensión (tanto temporal como geográfica), el TSO puede preparar la respuesta adecuada, ya sea por el lado de la demanda o poniendo en funcionamiento generación adicional si las condiciones lo permiten.

vi. **Sequía** – los niveles bajos de agua reducen la producción hidroeléctrica (con un número crítico de instalaciones hidroeléctricas fuera de funcionamiento). Además, es posible que varias unidades de generación térmica también tengan que parar o reducir la producción debido a limitaciones en la capacidad de refrigeración.

En el tema de las instalaciones hidroeléctricas, la generación eléctrica por plantas que utilizan esta tecnología no representa una proporción relevante de la generación total. Como se dijo anteriormente, en 2019 cubrió el 7,4% y en 2023 alcanzó el 10,73% de la demanda anual.



Fuente: Informe mensual febrero 2020 OMIE (NEMO español) - Energia por tecnologías en el Programa Diario Base de Funcionamiento (PDBF)

El gráfico de la *Energia por tecnologías en el Programa Diario Base de Funcionamiento (PDBF)* muestra que la participación de la generación hidroeléctrica alcanza su punto máximo en diciembre y enero. Otras tecnologías de generación pueden cubrir la generación hidroeléctrica (la participación hidroeléctrica es mucho menor en los meses de verano, mientras que la generación de gas aumentó).

vii. **Fallos múltiples por fenómenos meteorológicos extremos** - este escenario se descartó porque, aunque la probabilidad de este escenario existe, el posible impacto en EENS y LOLE se ha evaluado como insignificante según la metodología.

3.4.5 Desastres naturales - terremoto.

España ha descartado el escenario de terremoto debido a la incertidumbre de que ocurra tal evento. Además, cuando se analizan datos históricos, su magnitud rara vez ha alcanzado un nivel que haya llevado a una crisis eléctrica. El Instituto Geográfico Nacional (IGN), adscrito al Ministerio de Transportes y Movilidad Sostenible, realiza un seguimiento de estos acontecimientos en España.

El escenario supone que se produce un terremoto de magnitud considerable. El impacto es tal que las infraestructuras de energéticas se ven dañadas.

En el siglo XX se han producido cuatro terremotos con magnitudes entre 5,0 y 7,8 mbLg en el sur de España: Dúrcal (Granada), Arbolote (Granada), SO. Cabo San Vicente y Lorca (Murcia).

La vigilancia y la alerta temprana son cuestiones clave en la prevención y España dispone de 119 estaciones sismológicas para ello. Las estaciones se encuentran principalmente en las Islas Canarias, el Pirineo, la costa occidental y Andalucía, donde se concentra la actividad sísmica.

La probabilidad de que se produzca un terremoto es muy baja, son sucesos muy localizados y su intensidad es baja en la Escala Macrosísmica Europea. Debido a que la mayor parte de la

actividad sísmica ocurre en los SETNP, cualquier impacto transfronterizo en el SETNP es inexistente.

Sin embargo, existe una región continental relevante donde se producen terremotos en el sur de España. Dado que los terremotos son de ocurrencia local, su intensidad no suele ser alta y la región donde es probable que ocurran está lejos de la frontera franco-española, los impactos transfronterizos son insignificantes.

Teniendo en cuenta todo lo anterior, España ha descartado los escenarios de terremotos.

3.4.6 Factor humano.

España ha descartado estos escenarios porque en ambos casos los impactos, en términos de EENS y LOLE, son insignificantes. En el escenario de error humano, esto afecta directamente a una única instalación y la probabilidad de tener un efecto en cascada en otras instalaciones es muy pequeña. Esta desconexión accidental o error puede dar lugar a una situación N-1, pero las redes eléctricas y los operadores del sistema están bien preparados para hacer frente a este tipo de eventos. La probabilidad de error humano es posible debido a la falibilidad humana.

i. **Error humano** – el evento desencadenante puede ser un error de los operadores que desconectan un elemento esencial de la red, o cualquier violación del criterio N-1 causada por un error humano.

ii. **Huelga, disturbio, acción sindical** - el evento que inicia la crisis pueden ser disputas de algún tipo que escalan a acciones en grandes industrias o disturbios.

En el caso de las huelgas, en repetidas ocasiones las empresas cuyos trabajadores se declaran en huelga han cumplido diligentemente con sus obligaciones en materia de servicios mínimos. Estos servicios mínimos se fijan de conformidad con la normativa[14]. Estas empresas deberán mantener estos servicios mínimos para mantener los niveles de operación y garantizar la seguridad de las personas y bienes en todas las instalaciones involucradas en el servicio público de suministro eléctrico. Siempre que hay una huelga que afecta a una o varias empresas implicadas en el suministro eléctrico, hay un proceso de consulta y el Ministerio para la Transición Ecológica y el Reto Demográfico fija por orden los servicios mínimos para estas empresas.

Teniendo todo esto en cuenta, además de datos históricos que reflejan que las huelgas no han tenido ningún tipo de impacto relevante en la oferta, el gobierno español ha descartado posibles impactos transfronterizos por alguno de estos escenarios.

3.4.7 Errores de mercado.

España ha descartado estos escenarios porque, al igual que en el apartado anterior, en ambos casos los impactos son insignificantes. Además, la probabilidad de que se produzca cualquiera de los dos escenarios es baja o muy baja.

[14] Real Decreto 1170/1988, de 7 de octubre, sobre prestación de servicios mínimos en las Empresas afectas al servicio público de suministro de energía eléctrica ante situaciones de huelga.

El mercado español está creciendo en número de participantes y en su grado de competitividad, tanto por el lado de la demanda como por el de la generación. Los índices Herfindahl-Hirschman muestran una tendencia de reducción de la concentración del mercado en los mercados mayorista y minorista.

3.4.8 Fallos técnicos.

España no ha incluido estos escenarios por la muy baja probabilidad del evento y/o porque estos eventos no han alcanzado suficiente magnitud.

i. **Perdida de los sistemas TIC en el funcionamiento en tiempo real** - en este tipo de crisis el evento desencadenante puede ser:

   a. La pérdida o indisponibilidad de una parte sustancial de las infraestructuras o sistemas de telecomunicaciones empleados en los sistemas del sector eléctrico o de operación del mercado eléctrico.
   b. La pérdida o indisponibilidad de uno o más sistemas TIC empleados en la planificación y operación en tiempo real del sistema eléctrico (por ejemplo, los sistemas de cálculo de seguridad de operación de las redes, las predicciones de generación renovable o las medidas del sistema).

ii. **Múltiples fallos simultáneos** – se producen algunos de los siguientes fallos:

   a. Fallos en cables HVDC que provocan la desconexión de varias plantas de producción dando lugar a una ratio de potencia perdida que supera los umbrales del escenario N-1.
   b. Fallos en subestaciones o líneas de transporte/distribución que provocan cortes de suministro de gran volumen a consumidores.
   c. Fallos simultáneos o muy próximos en el tiempo en múltiples equipos que superan los umbrales de seguridad y para los cuales el sistema no está preparado.
   d. Una amenaza al sistema desconocida. Esta amenaza se puede manifestar como consecuencia de que las pruebas offline no fueron suficientemente precisas o porque el escenario en cuestión no se estudió.
   e. Una amenaza al sistema desconocida por la operación de la medida deficiente por el funcionamiento deficiente de los equipos de monitorización.
   f. La violación de un estándar/protocolo de seguridad como consecuencia de un error operacional o porque la respuesta de control no fue lo suficientemente rápida para preservar la seguridad del sistema.
   g. Fallos múltiples en activos de red que provocan la separación de una parte del sistema con insuficiente capacidad de generación.
   h. Cortocircuitos.

iii. **Fallo en serie de equipos** – algunos de los elementos de las redes de transporte o distribución comienzan a mostrar compartimentos anómalos que incrementan el riesgo de fallo o que llevan a dichos fallos.

En el caso del escenario de pérdida de sistemas TIC, la probabilidad de que el evento (en cualquiera de sus variantes) se produzca es baja debido a la redundancia y confiabilidad de los sistemas actuales.

Aunque el escenario de múltiples fallos simultáneos tiene una mayor probabilidad que los otros dos escenarios de esta categoría, las salvaguardas del sistema actual detienen los fallos en su origen antes de que tengan la oportunidad de propagarse. Aunque se produzcan múltiples fallos, el impacto sigue siendo insignificante, tanto en términos de LOLE como de EENS, debido a la fiabilidad de la red.

Finalmente, España descartó el escenario de fallos en cascada o en serie de equipos porque tiene la misma probabilidad de producirse que el escenario de pérdida de sistemas TIC. Esto se debe a que las salvaguardias del sistema actual detienen los fallos en su origen tan pronto como se hacen evidentes.

De los tres escenarios de esta categoría, sólo los fallos en cascada o en serie de los equipos tenían una calificación de dependencia transfronteriza. España lo descartó porque era un evento muy improbable y sus impactos eran insignificantes.

3.4.9 Desabastecimiento de combustibles fósiles (incluido el gas natural).

España no ha incluido el escenario de escasez de combustibles fósiles por varios motivos.

En primer lugar, la generación eléctrica anual asociada al gas natural oscila entre el 7,5-10%, alcanzando en ocasiones picos del 20% de la energía generada en los sistemas eléctricos español y portugués[15].

Otras tecnologías podrán asumir, sin dificultades relevantes, la cuota de generación eléctrica en caso de que se produzca una escasez de gas natural que afecte a estas instalaciones.

Por otra parte, se espera que disminuya la proporción de generación de electricidad a base de gas natural. Hay una gran proporción de renovables en el sistema eléctrico español y está creciendo rápidamente. La creciente proporción de energías renovables está reduciendo y reducirá la proporción de generación de electricidad a partir de gas natural.

Además, la adopción de soluciones de almacenamiento favorecerá la integración de las energías renovables en el sistema eléctrico español, acelerando la reducción de la cuota de electricidad procedente del gas natural.

Por último, en caso de una escasez real de gas natural, España podría responder rápidamente aumentando las importaciones de gas (GNL) a través del gran número de plantas de regasificación desplegadas a lo largo de la costa.

Aunque para España se ha descartado la crisis de escasez de combustibles fósiles, el escenario puede tener relevancia indirecta en otros Estados miembros, especialmente en aquellos que tienen una fuerte dependencia del gas natural porque tienen, entre otras, una cuota de generación eléctrica a partir de combustibles fósiles mayor. El hecho es que España es un punto de entrada relevante y puede servir como correo de transmisión hacia otros EEMM del gas

[15] Información de la página web de OMIE: https://www.omie.es/es/market-results/monthly/daily-market/daily-power?scope=monthly&year=2023&month=6

natural importado. El gas entraría en la UE a través de las plantas de regasificación del país y fluiría hacia Europa utilizando las interconexiones con Francia.

Finalmente, si bien el escenario de "Desabastecimiento de combustibles fósiles (incluido el gas natural)" no se ha incluido como parte del PPR español, es una cuestión relevante para otros Estados Miembros.

La existencia de 7 plantas de regasificación en territorio peninsular garantiza que España disfrute no solo de una fuerte diversificación de fuentes de suministro de gas natural, sino que también pueda servir como punto de entrada en la UE de este combustible.

3.4.10 Otros escenarios de crisis.

Al igual que ocurre con los escenarios de desastres naturales descartados, España no ha incluido estos escenarios por la muy baja probabilidad de que ocurran y porque, como muestran los datos históricos, estos eventos no han alcanzado la magnitud suficiente.

i. **Complejidad del mecanismo de control del sistema eléctrico** - El desencadenante de este tipo de crisis son fallos técnicos en los sistemas TIC, en los sistemas de comunicación o una señal errónea. En este último caso, un componente de protección de la red envía una señal a otras redes, unidades de producción o componente de los centros de control que da lugar a un fallo en cascada, debido a la alta interdependencia entre sistemas extremadamente complejos.

ii. **Accidente industrial/nuclear** – tiene lugar cuando ocurre un accidente industrial grave, como una liberación de contaminación radiológica resultante de una explosión en una planta nuclear o la emisión de contaminantes tóxicos de una planta química por diversas razones (fallo técnico, terremoto, sabotaje/ataque terrorista, error humano, etc.).

   En las últimas décadas se han mejorado los niveles de seguridad en la industria química y petroquímica, con controles y legislación cada vez más eficaces. Los accidentes químicos ocurren[16]:

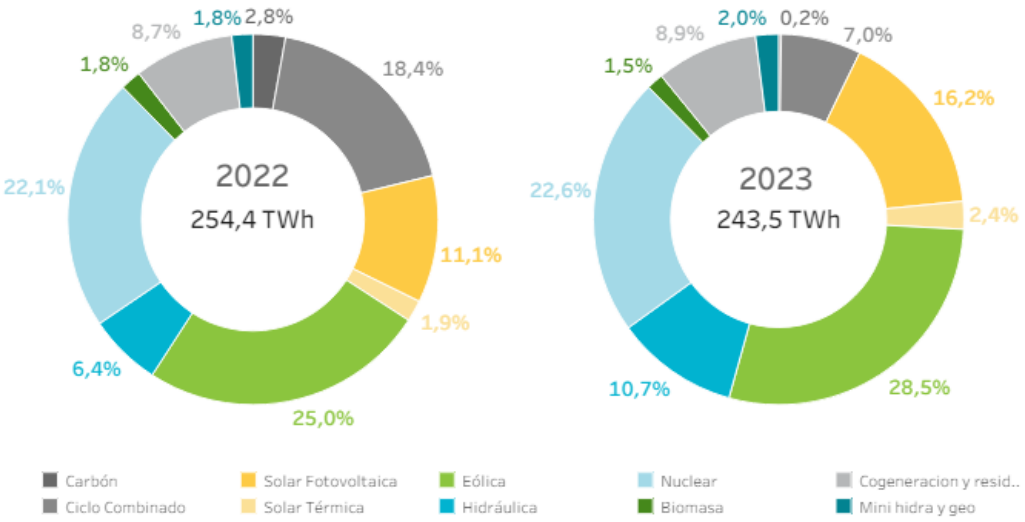
   a. El 44% del tiempo durante el transporte del producto.
   b. El 19% del tiempo en las áreas de procesamiento de las fábricas.
   c. El 15% del tiempo mientras los productos están en tanques de almacenamiento.
   d. El resto, por operaciones de traslado, manipulación o depósito de los compuestos.

   Comenzando con la Directiva Seveso (y sus actualizaciones), las legislaciones nacionales regulan la implantación de sistemas de gestión de seguridad y los planes de emergencia internos en cada instalación. Esto favorece que la probabilidad de que se produzca un accidente grave que provoque una crisis eléctrica es muy baja. Además, medidas de seguridad implementadas hacen que este tipo de accidentes queden confinados y que su impacto en el suministro eléctrico sea bajo o muy bajo.
   Sobre los motivos para descartar el escenario de accidente nuclear, ver el punto 3.4.1.

[16] E. Planas, J. Arnaldos, R.M. Darbra, M. Muñoz, E. Pastor, J.A. Vílchez. "Historical evolution of process safety and major-accident hazards prevention in Spain. Contribution of the pioneer Joaquim Casal". Journal of Loss Prevention in the Process Industries 28: 109-117, 2014.

Por todo lo anterior, España ha descartado el escenario de accidente industrial/nuclear.

iii. **Error inusualmente grande en la predicción de participación de renovables** - el desencadenante es una diferencia considerable entre la generación real y la prevista por unidades renovables, debido a errores inusualmente grandes en la predicción, errores en los datos de pronóstico en sí o debido a cambios rápidos e imprevistos con el tiempo. Las renovables representan entre el 50 y el 55% de la operativa base diaria. La mayor contribución de las energías renovables proviene de la energía eólica (21-22% del total) y la participación de la tecnología solar crecerá significativamente en los próximos años.



Fuente: Informe anual Evolución del mercado de electricidad 2023 OMIE (NEMO español). Tecnologías en el PDBF

No obstante, España no ha considerado este escenario porque:

a) Si el error conduce a una generación excesiva, el TSO tiene herramientas suficientes para hacerle frente.
b) Si el error provoca generación insuficiente, podrá entrar en funcionamiento capacidad no utilizada u ociosa para cubrir la diferencia. Además, existen otras alternativas como el deslastre de carga.

4. Marco jurídico aplicable.

Este capítulo describe el marco regulatorio, tanto a nivel de la UE como nacional. El PPR se regula específicamente en disposiciones propias del sector eléctrico.

No obstante, para poder llevarlo a cabo hay que tener en cuenta que pueden participar agentes de otros sectores relacionados con la energía, como pueden ser del sector del gas natural, de la ciberseguridad y de seguridad pública.

Por último, resulta necesario señalar que todas las actuaciones que se describen en este plan ya aparecen específicamente reguladas en la normativa propia de los diferentes sujetos, ya sean del sector eléctrico o de otros sectores. Este es el caso de la participación de:

- Agentes del sector eléctrico, que tienen un marco de actuación ampliamente desarrollo desde la Ley 24/2013, de 26 de diciembre, hasta los Procedimientos de Operación del Sistema, y, en particular, la normativa de preparación frente a riesgos del sector eléctrico.
- Otros agentes externos al sector eléctrico, que juegan papeles relevantes en las crisis de electricidad y cuyas obligaciones y acciones se regulan en su normativa específica.

El PPR no es un instrumento a través del cual se establecen nuevas obligaciones para aquellos agentes que no pertenecen al sector eléctrico, sino todo lo contrario. Se limita a resumir aquellas actuaciones y obligaciones propias derivadas de normativa ya existente.

4.1 Normativa comunitaria.

4.1.1 Normativa del sector eléctrico.

Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE

Como indica el propio reglamento en su parte expositiva, la *"mejor garantía para la seguridad del suministro eléctrico es el buen funcionamiento de los mercados y sistemas, con unas interconexiones eléctricas adecuadas. No obstante, incluso cuando los mercados y sistemas funcionan correctamente y están interconectados, nunca queda descartado el riesgo de que se produzca una crisis de electricidad como resultado de desastres naturales tales como condiciones meteorológicas extremas, ataques malintencionados o escasez de combustible."*

El mercado europeo de la electricidad está configurado por el conjunto de sistema eléctricos de los diferentes Estados Miembros y demás participantes en el mismo.

Teniendo en cuenta que los mercados y sistemas eléctricos nacionales están en mayor o menor medida interconectados, la prevención y la gestión de las crisis de electricidad no deben abordarse como tareas exclusivamente nacionales.

4.1.2 Normativa del sector gasista.

Reglamento (UE) 2017/1938 del Parlamento Europeo y del Consejo, de 25 de octubre de 2017, sobre medidas para garantizar la seguridad del suministro de gas y por el que se deroga el Reglamento (UE) nº 994/2010.

Este Reglamento establece el marco tanto en lo relativo a la preparación ante emergencias como a la reacción de la UE ante las interrupciones del suministro de gas.

Reglamento (UE) 2022/1032 del Parlamento Europeo y del Consejo de 29 de junio de 2022 por el que se modifican los Reglamentos (UE) 2017/1938 y (CE) nº 715/2009 en relación con el almacenamiento de gas.

Tras la invasión rusa de Ucrania a principios de 2022, este nuevo reglamento introduce medidas para abordar los desequilibrios del mercado energético y garantizar un almacenamiento de gas completo en la UE. El almacenamiento de gas adquiere gran importancia ya que contribuye a la seguridad del.

Reglamento (UE) 2022/1369 del Consejo de 5 de agosto de 2022 sobre medidas coordinadas para la reducción de la demanda de gas.

Este Reglamento del Consejo pretende reducir la demanda de gas natural mediante medidas coordinadas entre todos los Estados Miembros y el establecimiento de un nuevo mecanismo obligatorio de reducción de la demanda a nivel europeo en caso de crisis de suministro.

4.1.3 Otra normativa.

INFRAESTRUCTURAS CRÍTICAS.

Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

En esta Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de estas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

CIBERSEGURIDAD.

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

La Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, determina que los Estados miembros deberán garantizar la existencia de un interlocutor nacional operativo a efectos del intercambio de información sobre ciberataques. Así mismo, establece la necesidad de que éstos cuenten con

procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar, en un plazo máximo de ocho horas a partir de la recepción de la solicitud de ayuda, si la misma podrá ser atendida, y la forma y el plazo aproximado de ello.

4.2 Normativa nacional

4.2.1 Normativa del sector eléctrico

Ley 24/2013, de 26 de diciembre, del Sector Eléctrico.

La Ley 24/2013, de 26 de diciembre, tiene como finalidad básica establecer la regulación del sector eléctrico garantizando el suministro eléctrico con los niveles necesarios de calidad y al mínimo coste posible, asegurar la sostenibilidad económica y financiera del sistema y permitir un nivel de competencia efectiva en el sector eléctrico, todo ello dentro de los principios de protección medioambiental de una sociedad moderna.

Fundamento jurídico del Plan en la normativa española

En primer lugar, conviene destacar que la ley recoge una habilitación normativa específica relativa a la garantía de suministro. En este sentido, el artículo 7 de la Ley 24/2013, de 26 de diciembre, establece en su apartado 2 que:

> *"2. El Gobierno podrá adoptar, para un plazo determinado, las medidas necesarias para garantizar el suministro de energía eléctrica cuando concurra alguno de los siguientes supuestos:*
>
> *a) Riesgo cierto para la prestación del suministro de energía eléctrica.*
>
> *b) Situaciones de desabastecimiento de alguna o algunas de las fuentes de energía primaria.*
>
> *c) Situaciones de las que se pueda derivar amenaza grave para la integridad física o la seguridad de las personas, de aparatos o instalaciones o para la integridad de la red de transporte o distribución de energía eléctrica previa comunicación a las Comunidades Autónomas afectadas.*
>
> *d) Situaciones en las que se produzcan reducciones sustanciales de la disponibilidad de las instalaciones de producción, transporte o distribución o de los índices de calidad del suministro imputables a cualquiera de ellas."*

De este modo se establece en la normativa nacional el fundamento jurídico para actuar y preparar las actuaciones necesarias frente a crisis que amenacen el suministro eléctrico.

En este sentido, el propio artículo 7 recoge en su apartado 3 establece como tales *"cualesquiera otras medidas que puedan ser recomendadas por los Organismos internacionales de los que España sea miembro o que se determinen en aplicación de aquellos convenios en que se participe".* Esto incluye el PPR.

Análisis de los sujetos y actividades relacionados con las crisis en el sector eléctrico

En el marco normativa descrito inicialmente, la citada ley define las diferentes actividades destinadas al suministro de energía eléctrica, así como los sujetos que las desarrollan. Entre estos sujetos se encuentran algunos de los cuales tienen especial relevancia en el contexto del Plan Nacional de Preparación frente a los riesgos en el sector de la electricidad y entre los que se pueden mencionar:

a) El operador del sistema (OS), que también es el gestor de la red de transporte (TSO).

b) El transportista o titular de la red de transporte de energía eléctrica (Red Eléctrica) - Red Eléctrica de España, S.A.U.

c) Los distribuidores o gestores de las redes de distribución (DSO).

d) Los productores de energía eléctrica.

e) Los consumidores.

Real Decreto 738/2015, de 31 de julio, por el que se regula la actividad de producción de energía eléctrica y el procedimiento de despacho en los sistemas eléctricos de los territorios no peninsulares.

El PPR se aplica en todo el sistema eléctrico español (incluidos los SETNPS). Este reglamento establece el marco regulatorio para los SETNP, dado quesu carácter aislado produce una serie de diferencias respecto al sistema continental.

Procedimientos de operación.

El PPR se aplica a toda España. Esto significa que el ámbito geográfico incluye no sólo la Península Ibérica (directamente interconectada con Francia, Portugal, Andorra y Marruecos), sino también todos los sistemas eléctricos de los territorios no peninsulares (SETNP).

Los procedimientos operativos relevantes en el PPR incluyen cuestiones relacionadas con:

i. Medidas operativas para garantizar la cobertura en situaciones de alerta y emergencia.
ii. Establecimiento de planes de seguridad para el funcionamiento del sistema.
iii. Previsiones de cobertura y análisis de seguridad del sistema eléctrico.
iv. Restricciones técnicas.
v. Gestión de conexiones internacionales.

En los Sistemas Eléctricos No Peninsulares (SETNP), también cobra relevancia:

i. Operación de sistemas eléctricos no peninsulares.
ii. Cobertura, programación de generación y ampliaciones al despacho económico.
iii. Programación de generación en tiempo real.

Los Procedimientos de Operación están disponibles públicamente en la web de Red Eléctrica[17].

4.2.2 Normativa del sector gasista.

Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

La planificación, la garantía de suministro y las actuaciones frente a emergencias son tres cuestiones clave en esta ley de garantía de suministro y emergencias. En concreto la Ley recoge medidas sobre situaciones de desabastecimiento, la obligación de mantener existencias mínimas de seguridad, la obligación de mantener reservas estratégicas, la necesidad de

[17] Procedimientos de operación | Red Eléctrica (ree.es)

diversificar el suministro y regula el funcionamiento de CORES, que es la Entidad Central de Almacenamiento según la definición establecida en la Directiva 2009/119/CE.

Real Decreto 1716/2004, de 23 de julio, por el que se regula la obligación de mantenimiento de existencias mínimas de seguridad, la diversificación de abastecimiento de gas natural y la corporación de reservas estratégicas de productos petrolíferos.

Esta norma establece la obligación sobre los sujetos que intervienen en el sector del gas natural de mantener unas existencias mínimas de seguridad de 27,5 días de sus ventas o consumos de carácter firme en el año natural anterior.

Orden TED/72/2023, de 26 de enero, por la que se desarrollan los procedimientos necesarios para el cumplimiento de la obligación de mantenimiento de existencias mínimas de seguridad de gas natural.

Se trata de la norma a través de la cual se desarrollan cuestiones esenciales de la normativa española de mantenimiento de existencias mínimas de seguridad.

Resolución de 26 de septiembre de 2021, de la Dirección General de Política Energética y Minas, por la que se aprueba el Plan de actuación invernal para la operación del sistema gasista.

Se trata de una medida adicional para garantizar el suministro de gas natural ante situaciones imprevistas durante las temporadas invernales.

Procedimientos de Operación del Sistema.

Al igual que ocurre con los procedimientos de operación eléctrica, el sector gasista cuenta con una regulación específica de operación en forma de Normas de Gestión Técnica del Sistema (NGTS) y protocolos detallados. Incluyen procedimientos para la gestión del Sistema en escenarios de funcionamiento normal (procedimiento NGTS-09), excepcional (procedimiento NGTS-10) y de emergencia (procedimiento NGTS-11).

4.2.3 Otra normativa.

INFRAESTRUCTURAS CRÍTICAS.

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Esta ley regula las infraestructuras críticas, que se encuentran bajo una serie de amenazas y son unas de las prioridades estratégicas de seguridad nacional más relevantes.

El OS, el TSO, los DSO y otros agentes juegan un papel relevante en la protección de las infraestructuras críticas para la electricidad. Ciertos escenarios de crisis incluidos en el PPR son precisamente ciberataques o ataques físicos a infraestructuras críticas del sector eléctrico.

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Este reglamento establece la regulación específica para la elaboración y revisión del Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), de los Planes Estratégicos Sectoriales, de los Planes de Seguridad del Operador, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo.

CIBERSEGURIDAD.

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

La Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos.

Parte del concepto de Seguridad Nacional incluye la ciberseguridad, que es un área de especial interés en el PPR.

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Mediante este real decreto-ley se establecen una serie de mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Se trata de un reglamento que lleva a cabo el desarrollo del el Real Decreto-ley 12/2018, de 7 de septiembre, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, al cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad.

SEGURIDAD PÚBLICA.

Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.

Esta ley regula el sistema de protección civil. El sistema es un instrumento de seguridad pública, integrado a la política de Seguridad Nacional.

La ley incluye todas las fases de un ciclo de emergencia: previsión, prevención, planificación, intervención, recuperación y coordinación general de la acción política mediante la integración de estrategias de toda la actividad pública y privada en la materia. En este tema, fortalece los centros de coordinación operativa y establece al Centro Nacional de Seguimiento y Coordinación de Emergencias de Seguridad Pública como la entidad responsable en emergencias de interés nacional.

Real Decreto 524/2023, de 20 de junio, por el que se aprueba la Norma Básica de Protección Civil.

Esta norma básica fija el marco para alinear las fases y las situaciones operativas con las fórmulas aplicadas en los Planes Territoriales y, en particular, en el Plan Estatal General de Emergencias (PLEGEM), con el objetivo de garantizar la ordenada sucesión de planes en los supuestos de escalada de las situaciones de gravedad.

También prevé la configuración en el PLEGEM y en los Planes Territoriales, de una fase especial de apoyo a otras situaciones que no sean estrictamente de protección civil.

Estrategia Nacional de Protección Civil.

La Estrategia Nacional de Protección Civil toma en consideración factores que afectan a todo tipo de riesgos y su gestión, así como otros factores específicos de cada uno.

Plan General de Emergencias de Seguridad Ciudadana (PEGLEM), aprobado por Resolución de 16 de diciembre de 2020.

El PLEGEM es el instrumento operativo para la plena integración del Sistema Nacional de Seguridad Pública en el Sistema Nacional de Seguridad.

Ley Orgánica 2/1986, de 13 de marzo, sobre Fuerzas y Cuerpos de Seguridad.

Esta ley establece el marco regulatorio para las fuerzas policiales y los cuerpos de seguridad. Las Fuerzas y Cuerpos de Seguridad del Estado deben garantizar el libre ejercicio de los derechos y libertades, así como la seguridad ciudadana. Algunas de estas funciones adquieren especial relevancia durante cualquier evento que desemboque en una crisis de electricidad, así como en el transcurso de la propia crisis.

Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

Esta Ley Orgánica regula la defensa nacional y establece las bases de la organización militar, incluyendo la regulación de la Unidad Militar de Emergencia (UME).

Real Decreto 1097/2011, de 22 de julio, por el que se aprueba el Protocolo de Intervención de la Unidad Militar de Emergencias.

Este protocolo regula las condiciones de intervención de la UME, con el objetivo de dotar a dicha Unidad del marco normativo que le sirva de eficaz instrumento para el satisfactorio cumplimiento de la misión que se le ha encomendado.

SANIDAD

Ley 33/2011, de 4 de octubre, General de Salud Pública.

La ley establece las bases legales que sustentan las acciones de coordinación y cooperación de las Administraciones públicas en materia de salud pública.

Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Recoge la regulación relativa a los medios a través de los cuales el Ministerio de Sanidad articula la gestión y coordinación de alertas sanitarias y de salud pública, incluidos el Centro de Coordinación de Alertas y Emergencias Sanitarias, así como las competencias propias del ministerio relacionadas con pandemias y epidemias.

MOVILIDAD Y GEOGRAFÍA.

Real Decreto 253/2024, de 12 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Transportes y Movilidad Sostenible, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Esta norma recoge las funciones básicas del Instituto Geográfico Nacional, integrado en la Subsecretaría de Transportes y Movilidad Sostenible del Ministerio de Transportes y Movilidad Sostenible.

METEOROLOGIA Y DESASTRES NATURALES.

Estatuto de la Agencia Estatal de Meteorología, aprobado por el Real Decreto 186/2008, de 8 de febrero.

Constituye la regulación propia del Servicio Meteorológico Nacional de España, siendo una de las funciones primordiales de los SMN suministrar información y servicios que permitan a los gobiernos y a las demás partes interesadas minimizar los costes de los desastres naturales (incluidos incendios y erupciones volcánicas), mediante la realización de actuaciones preventivas ante los fenómenos meteorológicos adversos y la mitigación de sus posibles efectos.

5. Sujetos que participan en el Plan Preparación frente a Riesgos en el Sector Eléctrico en España: Coordinador de crisis, Autoridad Competente y otros agentes.

5.1 Introducción.

El PPR requiere de la participación de una multiplicidad de actores cuyas acciones deben llevar a la mejor gestión posible de los escenarios de crisis de electricidad contemplados, siempre con el fin último de garantizar el suministro de energía eléctrica dentro del sistema.

En lo que se refiere a los principales agentes implicados en las actuaciones derivadas del plan, éstos se agrupan en 3 grandes pilares:

I. Autoridades.
II. El Sistema Eléctrico Nacional.
III. Seguridad Pública – Servicios de Emergencia y de Primera Intervención.

5.1.1 Autoridades.

El primer pilar sobre el que se sustenta el PPR es el formado por las autoridades.

Los agentes de este grupo desempeñan dos roles fundamentales: el de Autoridad Competente y el de Coordinador de Crisis.

También existen otros roles clave dentro del sector público que participan en el plan, proporcionando no sólo un punto de contacto al que acudir para obtener información, sino colaborando también en la toma de decisiones, dirección y coordinación.

Los agentes más relevantes incluyen **al Ministerio para la Transición Ecológica y el Reto Demográfico**, competente en materia energética, que ejerce de **Autoridad Competente** y de **Coordinador de Crisis** en el marco del plan, y otros departamentos ministeriales como otros ministerios, como el **Ministerio de Salud, el Ministerio del Interior** y el **Ministerio de Defensa,** que actúan de conforme a sus respectivas competencias.

Determinadas agencias y organismos también pueden tener un papel relevante durante una crisis de electricidad, entre los que se incluyen:

- **Centro Nacional de Protección de Infraestructuras Criticas (CNPIC)**, organismo perteneciente al Ministerio del Interior, responsable de dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas y El Plan Nacional de Protección de las Infraestructuras Críticas.
- **Instituto Nacional de Ciberseguridad de España (INCIBE),** empresa dependiente del Ministerio para la Transformación Digital y de la Función Pública. Su actividad se centra en el desarrollo de la ciberseguridad y la confianza digital ciudadana, la red académica y de investigación, los profesionales, las empresas y especialmente para los sectores estratégicos. INCIBE velará por apoyar la resolución de los ciberincidentes que puedan producirse en las infraestructuras del sector.

- **Oficina de Coordinación de Ciberseguridad (OCC)**, que es el órgano técnico de coordinación de la Secretaría de Estado de Seguridad en materia de ciberseguridad y que también pertenece al Ministerio del Interior. Sus funciones, en el marco de este plan, incluyen:
    - Proporcionar un canal de alerta temprana permanente en lo relativo a vulnerabilidades, ciberamenazas y ciberataques.
    - Establecer cauces de intercambio de información entre otros actores, públicos y privados, nacionales e internacionales.
    - Desarrollar mecanismos de respuesta ante un ciberincidente.

Como se verá a lo largo de los siguientes capítulos, la participación de estos agentes en la gestión de las crisis de suministro es directa e inmediata y tiene como objetivo dirigir la respuesta para que la crisis se vea resuelta o mitigada hasta su resolución, de modo que las incidencias en el suministro de electricidad se van minimizadas.

5.1.2 El Sistema Eléctrico Nacional.

El segundo de los pilares sobre el que se sustenta el PPR es el de los sujetos del sistema eléctrico español y, fundamentalmente, los siguientes:

- **Red Eléctrica de España, S.A.** que es simultáneamente el Operador del Sistema, el gestor de la red de transporte de energía eléctrica (TSO) y el propietario de la red de transporte.
- Los diferentes **gestores de las redes de distribución** de energía eléctrica (DSO).
- Las **empresas de generación.**
- **Consumidores.**
- **Comercializadoras de electricidad.**

Estos agentes tienen una participación directa e inmediata en la gestión de las crisis de suministro. Sus acciones son directa e inmediatas y tienen como objetivo operar el sistema durante las crisis para que se resuelvan los riesgos o se mitiguen sus impactos hasta su resolución. Sus actuaciones deben reducir el número de incidencias o interrupciones en el suministro eléctrico.

También tienen una participación directa en el mercado eléctrico. Por esto, sus decisiones y respuestas deben analizarse no sólo desde una perspectiva puramente técnica y operativa, sino también desde un punto de vista económico.

5.1.3 Seguridad Pública – Servicios de Emergencia y de Primera Respuesta.

El último pilar está formado por los Servicios de Emergencias y Primera Respuesta, que intervienen directamente en la seguridad ciudadana. Si bien su participación no es directa en la operación del sistema eléctrico como sujetos o agentes del mismo, son un elemento clave en la gestión de algunos de los escenarios identificados. Esta categoría incluye:

- **El Cuerpo Nacional de Policía.**

El Cuerpo Nacional de Policía tiene como misión garantizar que los ciudadanos puedan ejercer libremente sus derechos, proteger su libertad y garantizar la seguridad ciudadana, en el territorio nacional.

En el contexto de crisis y acontecimientos, incluidas las crisis eléctricas, tiene facultades[18] para:

i. Ayudar y proteger a las personas y velar por la conservación y custodia de los bienes que por cualquier motivo se encuentren en peligro.
ii. Mantener y restablecer, en su caso, el orden y la seguridad ciudadana.
iii. Prevenir la comisión de actos delictivos.
iv. Cooperar con todos los servicios de Seguridad Pública, en casos de grave riesgo, catástrofe o calamidad pública, en los términos establecidos en la legislación específica de Seguridad Pública.

La Policía Nacional incluye:

a) El Grupo de Operaciones Especiales (GEO)[19], que es una unidad de élite dispuesta a intervenir en situaciones que requieran calificaciones especiales en su ejecución, particularmente de carácter terrorista, y otras que supongan un riesgo grave para la vida y los bienes de las personas.
b) La Unidad Central de Desactivación de Explosivos. Conformada por el TEDAX-NRBQ[20] (Nuclear, Radiológico, Biológico y Químico).
c) La Comisaría General de Policía Judicial, que incluye en su estructura la Brigada Central de Investigación Tecnológica[21].
d) La Comisaría General de Seguridad Ciudadana[22], a la que corresponde organizar y gestionar los asuntos relacionados con la prevención de disturbios, el mantenimiento del orden y, en su caso, el restablecimiento tanto del orden como de la seguridad pública.

- **La Guardia Civil.**

La Guardia Civil es un Cuerpo de Seguridad Pública de carácter militar que forma parte de las Fuerzas y Cuerpos de Seguridad del Estado y que opera en todos los puntos de España.

Su organización pertenece tanto al Ministerio del Interior[23] como al Ministerio de Defensa[24].

Dirige sus esfuerzos en diferentes materias, algunas de las cuales pueden tener impacto directo en el sector energético, entre ellas:

e) Ciberseguridad y actividades delictivas TIC[25].

---

[18] Competencias recogidas en el art. 11.1 de la Ley Orgánica 2/1986, de 13 de marzo.
[19] https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_especialidades_geo.php
[20] https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cginformacion_especialidades_tedax.php
[21] https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php
[22] https://www.policia.es/_eu/tupolicia_conocenos_estructura_dao_cgseguridadciudadana.php
[23] Art. 4 del Real Decreto 207/2024, de 27 de febrero.
[24] Ver art. 1.5 del Real Decreto 205/2024, de 27 de febrero.
[25] Mediante los Grupo de delitos telemáticos. Ver: https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/gdt/index.html

f) Desactivación de Explosivos y Defensa NRBC[26].
g) Protección de edificios[27].
h) Terrorismo[28].

- **Los cuerpos policiales de las distintas comunidades autónomas.**

En España, algunas comunidades autónomas cuentan con cuerpos policiales autonómicos. Estos cuerpos policiales pueden ser propios[29] o pueden ser unidades especiales del Cuerpo Nacional de Policía especialmente adscritas a una comunidad autónoma[30].

Prestan servicio en diversas áreas relevantes como la seguridad ciudadana (vigilancia, actuación de respuesta inmediata, etc.), el orden público (control de multitudes, la conocida policía antidisturbios) y el tráfico, entre otras[31].

- **Servicios de Protección Civil.**

El titular del Sistema Nacional de Protección Civil es el Ministerio del Interior[32], quien ostenta la máxima autoridad en materia de Protección Civil y tiene a la Dirección General de Protección Civil y Emergencias[33], como órgano rector de la asistencia.

El Sistema Nacional de Protección Civil integra la actividad de Protección Civil de todas las Administraciones Públicas para garantizar una respuesta coordinada y eficiente a través de las siguientes actuaciones[34]:

i. Anticipación.
ii. Prevención.
iii. Planificación.
iv. Respuesta inmediata.
v. Recuperación.
vi. Evaluación e inspección.

Para la coordinación y seguimiento de las actividades de protección civil en España, las Delegaciones y Subdelegaciones del Gobierno cuentan con unidades de protección civil que colaboran con las autoridades de las Comunidades Autónomas en sus territorios[35].

Las Comunidades Autónomas[36] gestionan y responden a las emergencias de Protección Civil, utilizando su organización regional de Protección Civil, que puede ser diferente en cada una de ellas.

---

[26] Mediante el Servicio de Desactivación de Explosivos y Defensa NRBQ. Ver: https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/tedax/index.html
[27] Mediante la Unidad de Protección y Seguridad. Ver: https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/uprose/index.html
[28] Mediante el Grupo de Acción Rápida. Ver: https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/gar/index.html
[29] Art. 37 de la Ley Orgánica 2/1986, de 13 de marzo.
[30] Art. 47 de la Ley Orgánica 2/1986, de 13 de marzo.
[31] Título III de la Ley Orgánica 2/1986, de 13 de marzo.
[32] Art. 34 de la Ley 17/2015, de 9 de julio.
[33] Art. 13 del Real Decreto 207/2024, de 27 de febrero.
[34] Ver https://www.proteccioncivil.es/coordinacion/snpc
[35] Ver https://www.proteccioncivil.es/coordinacion/que-hacemos-en-proteccion-civil/unidades-proteccion-civil-delegaciones-subdelegaciones-gobierno
[36] Ver https://www.proteccioncivil.es/que-hacemos-en-proteccion-civil/proteccion-civil-ccaa

Los ayuntamientos de más de 20.000 habitantes[37] también gestionan las situaciones derivadas de emergencias de Protección Civil. Aproximadamente 400 ayuntamientos realizan actuaciones propias de Protección Civil, cuando surge la necesidad.

- **Bomberos.**

En España la extinción de incendios es un servicio cuya responsabilidad recae en la Administración Local y Autonómica. Además, el Ministerio para la Transición Ecológica y el Reto Demográfico cuenta con las Brigadas de Refuerzo contra Incendios Forestales (BRIF)[38].

Las brigadas BRIF son unidades helitransportadas de personal de extinción de incendios altamente especializado. Prestan un servicio de apoyo a las comunidades autónomas, pudiendo actuar en cualquier lugar del territorio nacional, incluida Canarias.

Actualmente hay diez BRIF operativas durante la temporada de verano, cuando el riesgo de incendio es mayor:

i. Nueve BRIF-A (con 60 personas y 2 helicópteros).
ii. Un BRIF-B (con 30 personas y 1 helicóptero).

Durante la temporada invierno-primavera (febrero-abril) de máximo riesgo de nieve y formación de hielo, también operan cinco BRIF de invierno más pequeñas (como un BRIF-B).

Las brigadas BRIF complementan las tareas de extinción con labores preventivas.

- **Servicios de Emergencias Médicas y Cruz Roja.**

La atención de urgencias y emergencias médicas se produce en dos lugares: en los hospitales, en sus servicios de urgencias, y fuera de los hospitales, donde debe desplazarse la asistencia sanitaria para llegar al paciente.

El Sistema Español de Salud (SNS) se organiza de forma similar al Sistema Nacional de Protección Civil: está descentralizado, por lo que las Comunidades Autónomas prestan Asistencia Sanitaria en sus territorios[39], y todo está coordinado a nivel estatal[40].

Los Servicios de Emergencias Médicas en España se han desarrollado de la mano de la consolidación del Sistema Nacional de Salud.

La Cruz Roja actúa para ayudar a las personas a superar situaciones agudas o crónicas que ponen en peligro su vida[41]. Atiende diferentes emergencias (incendios forestales, terremotos, nevadas, inundaciones, etc.), ofreciendo una respuesta inmediata y urgente en un enfoque de ayuda sostenida. Por su parte, los Equipos de Respuesta Inmediata a Emergencias (ERIE)[42] responden a las necesidades de las personas afectadas por una emergencia.

---

[37] Ver https://www.proteccioncivil.es/que-hacemos-en-proteccion-civil/proteccion-civil-ayuntamientos
[38] Ver https://www.miteco.gob.es/es/biodiversidad/temas/incendios-forestales/extincion/brif.html
[39] Art. 41 de la Ley 14/1986, de 25 de abril.
[40] Capítulo IV del Título III de la Ley 14/1986, de 25 de abril.
[41] Art. 2 del Real Decreto 415/1996, de 1 de marzo.
[42] Ver https://www.servicioscruzroja.com/poblacion-en-general-socorros/equipo-de-respuesta-inmediata-de-intervencion-psicosocial-erie/

Por último, el hecho de que intervenga la Cruz Roja en un incidente forma parte integral del mecanismo de planificación y respuesta que las distintas administraciones públicas han establecido en sus planes de emergencia.

- **Unidad Militar de Emergencias (UME)**

La Unidad Militar de Emergencia (UME), es una fuerza conjunta, organizada con carácter permanente, que tiene como misión la intervención en cualquier lugar del territorio nacional, para contribuir a la seguridad y bienestar de los ciudadanos[43]. Tiene un espíritu inequívoco de complementar los servicios de emergencia de otras Administraciones, principalmente de las Comunidades y Ciudades Autónomas.

La UME incluye el Regimiento de Apoyo e Intervención en Emergencias (RAIEM), el Grupo de Intervención en Emergencias Tecnológicas y Ambientales (GIETMA), así como cinco Batallones de Intervención en Emergencias (BIEM I a V), ubicados en las provincias de Madrid, Sevilla, Valencia, Zaragoza y León, así como una unidad perteneciente al BIEM II desplegada en Canarias[44].

La UME es una unidad militar que interviene en respuesta a una amplia gama de emergencias, incluidas aquellas que pueden desencadenar una crisis eléctrica.

Las emergencias a las que responde la UME no se limitan a catástrofes naturales, sino que incluyen aquellas situaciones que se derivan de cualquier riesgo tecnológico y las derivadas de ataques terroristas o actos ilegales y violentos, incluidas aquellas actuaciones contra infraestructuras críticas[45].

En este sentido, también realiza actuaciones en entornos como centrales nucleares, para lo que se prepara mediante la realización de simulacros y diferentes ejercicios. Por ejemplo, el Grupo de Intervención en Emergencias Tecnológicas y Ambientales (GIETMA) organizó, entre el 26 y el 30 de septiembre de 2022, el ejercicio "Beta Central Nuclear Garoña 2022"[46] con el objetivo de entrenar a las unidades de la Unidad Militar de Emergencias (UME) en apoyo a la población civil.

La actuación de la UME se coordina desde el Ministerio de Defensa, siguiendo siempre el Protocolo de Intervención de la Unidad Militar de Emergencia, aprobado por el Real Decreto 1097/2011, de 22 de julio.

[43] Ver https://www.defensa.gob.es/ume/CONOCENOS/que-es/
[44] Ver https://www.defensa.gob.es/ume/LA_UME_POR_DENTRO/organizacion/
[45] Artículo tercero del Protocolo de Intervención de la Unidad Militar de Emergencias.
[46] Ver https://www.defensa.gob.es/ume/Noticias/2022/09/Noticias/beta_gietma.html

5.2 Autoridad Competente.

Tal y como se notificó a la Comisión Europea en marzo de 2020, la Autoridad Competente responsable de llevar a cabo las tareas contenidas en el Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo de 5 de junio de 2019 es el Ministerio para la Transición Ecológica y el Reto Demográfico.

Tal y como establece el apartado 2 del artículo 3 del Reglamento, dentro de la Autoridad Competente, se establece que la persona de contacto a estos efectos es la persona titular de la Dirección **General de Política Energética y Minas.**

5.2.1 Funciones y responsabilidades.

Conforme a lo establecido en el artículo 3 del Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, el Ministerio para la Transición Ecológica y el Reto Demográfico será el encargado de llevar a cabo las diferentes tareas previstas en el Reglamento, que incluyen, entre otros:

- Elaborar y revisar los planes nacionales de preparación ante riesgos en el sector eléctrico.
- Cooperar con las autoridades competentes de otros Estados Miembros en crisis del sector eléctrico, siempre y cuando exista la posibilidad de que puedan tener impactos transfronterizos.
- Informar a los Estados Miembros y a la Comisión Europea de las amenazas y riesgos detectados en España de potenciales crisis de suministro eléctrico, incluso cuando no sea previsible que vayan a tener repercusiones transfronterizas. España realizará estas comunicaciones a través del Grupo de Coordinación de la Electricidad (ECG) de la Comisión Europea.
- Notificar las alertas tempranas a la Comisión Europea, a las Autoridades Competentes de los Estados Miembros de la misma región y, si no pertenecen a esta región, a las Autoridades Competentes de los Estados Miembros directamente conectados. La información que acompaña a estas alertas incluirá, cuando sea posible:
    - Información sobre las causas de la posible crisis de electricidad.
    - Las medidas que existen para evitar que se produzca una crisis de electricidad.
    - Si es necesaria la ayuda de otros Estados Miembros.
- Ante una crisis de electricidad, previa consulta al gestor de la red de transporte, declarar la crisis e informar a las autoridades competentes de los Estados miembros de la misma región y, si no pertenecen a esta región, a las Autoridades Competentes del Estado Miembro directamente conectado, así como a la Comisión.
- Cuando tenga lugar una crisis de electricidad, presentar los informes de evaluación al ECG y a la Comisión, previa consulta a la autoridad reguladora. Para ello podrá solicitar la colaboración del Operador del Sistema en la elaboración del informe de evaluación o delegar la misma en el mismo.

5.2.2 Funciones delegadas.

La Autoridad Competente no ha delegado en otras entidades o autoridades ninguna de las funciones previstas en el Reglamento (UE) 2019/941. Esto se entiende sin perjuicio de posibles delegaciones futuras de conformidad con el artículo 3, apartado 3, del Reglamento (UE) 2019/941.

En caso de que se produzca una delegación de funciones, el Ministerio supervisará cómo se llevan a cabo las tareas delegadas.

Además, la delegación formal aparecería en sucesivas actualizaciones de este Plan.

5.3 Coordinador de Crisis.

El apartado 13 del artículo 2 del Reglamento (UE) 2019/941 define al *"Coordinador de Crisis"* como una persona, un grupo de personas, un equipo compuesto por gestores nacionales de crisis de electricidad pertinentes o una institución encargada de actuar como interlocutor y coordinar los flujos de información durante una crisis eléctrica.

La cuestión considerada al establecer el Coordinador de Crisis es que las crisis contempladas en este plan ocurren en el sector energético. Por ello se establece que el Ministerio para la Transición Ecológica y el Reto Demográfico es el Coordinador de Crisis designado.

Al igual que en el caso de la Autoridad Competente, la persona de contacto a estos efectos será la persona titular de la **Dirección General de Política Energética y Minas.**

5.3.1 Funciones y responsabilidades.

Las funciones y responsabilidades del coordinador de crisis incluyen, entre otras:

- Mantener una comunicación constante con los TSO (electricidad y gas), recibiendo información actualizada sobre las diferentes situaciones y las diferentes zonas afectadas por cualquiera de las crisis eléctricas.
- Proponer al resto del gobierno soluciones para gestionar crisis o emergencias y eliminar sus consecuencias negativas o reducir el impacto de la interrupción del suministro eléctrico.
- Proponer recursos financieros adicionales, reservas de combustible y otros recursos para las actividades del sector energético que ayuden a hacer frente a una crisis o emergencia.
- Gestionar la cooperación y coordinación tanto a nivel nacional como internacional, que incluye:
    - Comunicación con las autoridades competentes y coordinadores de crisis de los Estados Miembros pertinentes.
    - Coordinación de todas las acciones relacionadas con la asistencia proporcionada a/recibida de otros Estados Miembros
- Comunicarse y consultar entidades relevantes que puedan contribuir a la solución de la crisis.
- Colaborar con las diferentes administraciones públicas estatales, autonómicas y locales.
- Si es necesario, involucrar e impulsar a la acción a otros representantes del sector eléctrico.

5.3.2 Funciones delegadas.

El Ministerio para la Transición Ecológica y el Reto Demográfico podrá delegar algunas de las funciones del Coordinador de Crisis en el TSO cuando la crisis:

- Requiera exclusivamente la adopción de medidas operativas de gestión y una respuesta inmediata y en tiempo real.

- Cuando sea necesario establecer contacto con el organismo de coordinación de crisis en caso de una crisis transfronteriza o si existe un riesgo verificable de que una crisis nacional pueda convertirse en una crisis transfronteriza.

El Ministerio informará de esta delegación funcional a la Comisión, al ECG y a ENTSO-E, especialmente cuando el motivo esté relacionado con medidas regionales y bilaterales a las que se refiere el artículo 12, apartado 1, letra a), del Reglamento (UE) 2019/941.

Esto se entiende sin perjuicio de posibles delegaciones futuras. En caso de que se produzca una delegación de funciones, como se establece para la autoridad competente en el apartado 3 del artículo 3 del Reglamento (UE) 2019/941, el Ministerio supervisará cómo el TSO lleva a cabo las tareas delegadas.

Finalmente, si la delegación se hiciera frecuente, se formalizaría y aparecería en sucesivas actualizaciones de este Plan.

5.3.3 Instrumentos de coordinación en España.

Está demostrado que un marco de coordinación estable y continuo es una herramienta resiliente y eficaz.

Así, el marco para todo este tipo de esquemas y mecanismos de coordinación en España se fija en diferentes normativas. Una de las normas más relevantes que regulan la coordinación es:

- **Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.**

Establece el marco general de coordinación en el sector público y cubre:

i. Comisiones interministeriales, que ayudan a coordinar toda la acción del gobierno estatal.
ii. Diferentes órganos de coordinación administrativa, que contribuyen a coordinar las actuaciones de las distintas administraciones (estatal, autonómica y local) para luchar contra una crisis.

I. Comisiones Interministeriales.

En materia energética, el órgano coordinador es la Comisión Interministerial para el Cambio Climático y la Transición Energética, creada mediante el Real Decreto 958/2018, de 27 de julio, de la nueva Comisión Interministerial para el Cambio Climático y la Transición Energética.

II. Órganos de Coordinación Administrativa.

Estos órganos proporcionan una coordinación fluida y eficaz, en la que cada administración puede proponer la medida que autorice en el ámbito de sus competencias. Las más relevantes durante las crisis incluyen la Conferencia de Presidentes, las Conferencias Sectoriales (incluida la Conferencia Sectorial de Energía), las Comisiones Sectoriales y sus Grupos de Trabajo y las Comisiones Administrativas.

5.3.4 Instrumentos de coordinación fuera de España.

España participa en otros instrumentos y cuerpos de coordinación. Este segundo grupo de órganos de coordinación son de carácter internacional y resultan de gran relevancia cuando una crisis puede tener impactos transfronterizos.

España participa en estas iniciativas de coordinación bien directamente (a través de sus poderes públicos y en los distintos niveles administrativos) o indirectamente, a través de entidades que la representan. Entre los órganos de coordinación que juegan un papel más relevante durante una crisis eléctrica se encuentran:

- La Comisión Europea, a nivel político.
- El Grupo de Coordinación Eléctrica (ECG), en el que la Autoridad Competente o sus empleados contribuyen al trabajo que realiza, que también puede servir como puente de conexión entre la política y la operación del sistema.
- ACER, en la que participa la Comisión Nacional de los Mercados y la Competencia (CNMC), la Autoridad Nacional Reguladora (ANR) de España. La CNMC colabora con los reguladores energéticos de Portugal (ERSE) y Francia (CRE) en foros de cooperación regional (a través de iniciativas regionales de gas y electricidad), así como en el desarrollo del Mercado Ibérico de la Electricidad (MIBEL) y del Mercado Ibérico del Gas (MIBGAS), para promover la integración de los mercados y el desarrollo de infraestructuras energéticas.
- CORESO SA, que actualmente es uno de los Centros de Coordinación Regional que coordina los flujos de electricidad para todos los Operadores de Redes de Transporte de la UE. Red Eléctrica, Operador del Sistema de Transporte de electricidad en España peninsular, es accionista de CORESO SA.
- ENTSO-E, en la que Red Eléctrica trabaja activamente con el resto de TSO eléctricos europeos.
- ENTSOG, en la que Enagás, S.A. también desarrolla una labor relevante en colaboración con el resto de TSO gasistas europeos.

Estas tres últimas entidades son muy relevantes desde una perspectiva operativa.

6. Procedimientos y acciones: descripción general.

El PPR cubre una serie de acciones y procedimientos que van desde las actuaciones de carácter preventivo a las de carácter mitigante y de las más generales a las más en detalle.

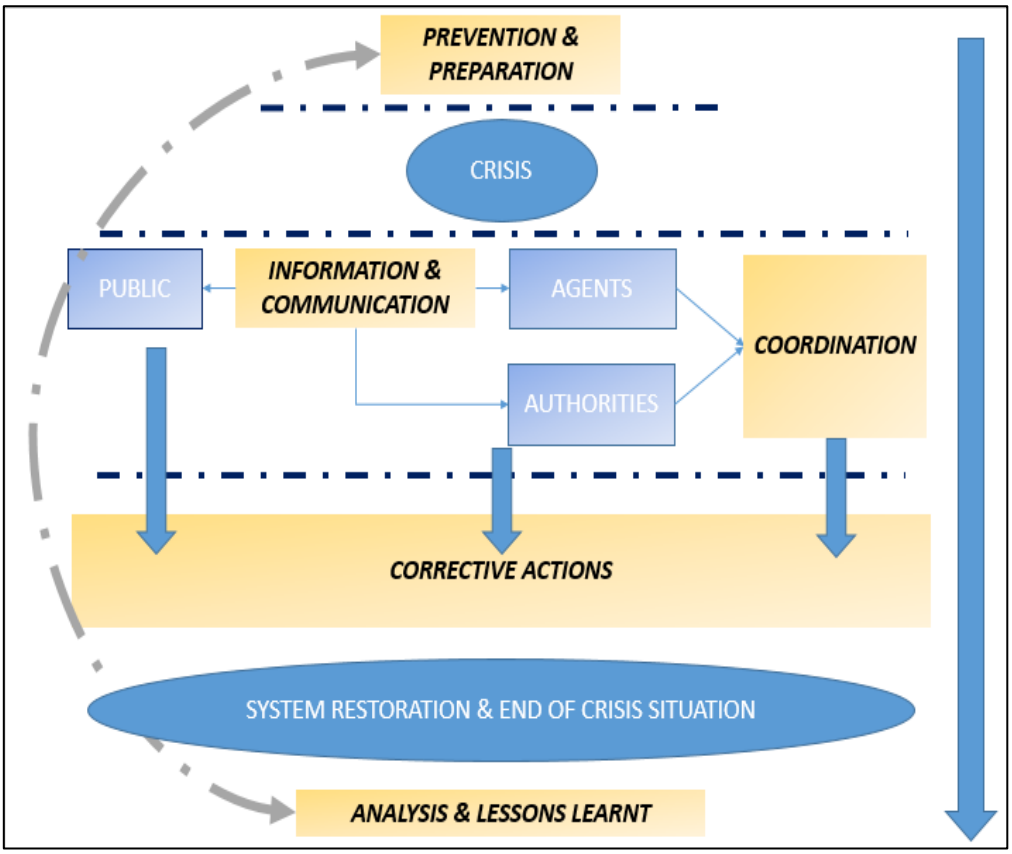
En primer lugar, conviene recordar que las actuaciones descritas en este plan ya aparecen específicamente reguladas en la normativa propia de los diferentes sujetos. Este es el caso de la participación de:

- Agentes del sector eléctrico, que tienen un marco de actuación ampliamente desarrollado desde la Ley 24/2013, de 26 de diciembre, hasta los Procedimientos de Operación del Sistema, incluida la normativa de preparación frente a riesgos del sector eléctrico.
- Agentes que no se encuentran directamente comprendidos dentro del sector eléctrico, como las FCSE, la AEMET, la UME, el CNPIC o el INCIBE.

El PPR no es un instrumento a través del cual se establecen nuevas obligaciones para aquellos agentes que no pertenecen al sector eléctrico, sino todo lo contrario. Se limita a resumir aquellas actuaciones y obligaciones propias derivadas de la normativa ya existente.

En este punto del PPR describiremos las diferentes acciones realizadas por cada uno de los agentes que intervienen.

Las crisis de electricidad, como cualquier otro tipo de crisis, y las respuestas a ellas siguen flujograma de actuaciones cíclico y no lineal. Por ello, para prepararse mejor ante futuras crisis, siempre debe haber alguna forma de retroalimentación productiva de incidentes anteriores.



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Como se puede observar en el flujograma, existen diferentes participantes que llevan a cabo una serie de acciones que tienen un impacto directo en el resultado. La participación de una amplia gama de agentes y entidades no hace más que subrayar la relevancia que tiene la coordinación en el PPR.

Esta coordinación ayuda a integrar las diferentes acciones de cada participante para lograr un objetivo común, que debe concretarse en el adecuado control de la crisis.

Las acciones que realizan los diferentes agentes y autoridades se encuadran en alguna de las siguientes categorías:

1. **Acciones preventivas y de preparación** – que incluyen el análisis y preparación, la detección de crisis y todos los trabajos orientados a la declaración de crisis, incluidas todas las acciones adoptadas en preparación de alertas tempranas.
2. **Actuaciones informativas** – Se trata de las comunicaciones que se realizarán antes, durante y después de la crisis. Estas incluyen las notificaciones de alerta temprana y declaraciones de crisis enviadas a las autoridades y entidades pertinentes.
3. **Activación de la coordinación** – Este es el siguiente paso a la comunicación inicial ya sea de la alerta temprana o de la notificación de la crisis eléctrica. La Comisión, los demás Estados miembros de la región SWE y de otros Estados miembros reciben estas comunicaciones y comienzan a trabajar.
4. **Medidas correctivas** – principalmente relacionadas con el sistema eléctrico.
5. **Análisis e informe: lección aprendida** – una vez superada una crisis, el análisis de su evolución y la respuesta dada por los diferentes participantes es un paso necesario. En el análisis ex post aparecen respuestas defectuosas o insuficientes, mejoras y otras vías para abordar las diferentes crisis.

Los siguientes puntos de este capítulo proporcionan una descripción detallada no sólo de las categorías de acciones, sino también de las acciones más relevantes en sí mismas.

6.1 Acciones preventivas y de preparación.

Las acciones preventivas y de preparación son un pilar clave en la preparación ante riesgos.

Una adecuada prevención y preparación integral son las mejores formas de afrontar una crisis desde todos los puntos de vista: reduce o incluso anula impactos negativos en la oferta, en el bienestar ciudadano y en la economía, entre otros. Algunas de las acciones que pueden mencionarse son las siguientes:

- Alertas meteorológicas en caso de fenómenos meteorológicos adversos.
- Prevención de incendios en la proximidad de las redes eléctricas.
- Disponer de reservas suficientes de combustible para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad.
- Preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.
- Preparación del TSO.
- Independencia energética y seguridad de suministro, incluyendo el despliegue del autoconsumo.

- La ciberseguridad. Las actuaciones preventivas y de preparación en materia de ciberseguridad se centran en los usuarios finales de los servicios TIC y en los equipos TIC.
- Simulaciones, que complementan en gran medida la preparación de TSO y la preparación para la ciberseguridad.

El análisis ex post (tal como se establece en el punto 6.5) determinará cómo de adecuada es la prevención y cómo de amplios son los preparativos. Sin embargo, la experiencia de otras situaciones y de otros países proporciona una guía útil a la hora de configurar las diferentes acciones de esta categoría.

6.1.1 Acciones relacionadas con la meteorología y las condiciones climáticas.

Dado que las condiciones climáticas provocan o agravan muchos de los escenarios de crisis, una de las acciones críticas es un seguimiento adecuado del tiempo y del clima y su evolución. Este seguimiento se realiza a través de la AEMET y es una de las funciones centrales de la Agencia recogida específicamente en su normativa propia, el Estatuto de la Agencia Estatal de Meteorología. Este seguimiento del clima ayuda a prepararse e incluso evitar una crisis eléctrica.

La alerta temprana sobre el clima y los incendios forestales permite:

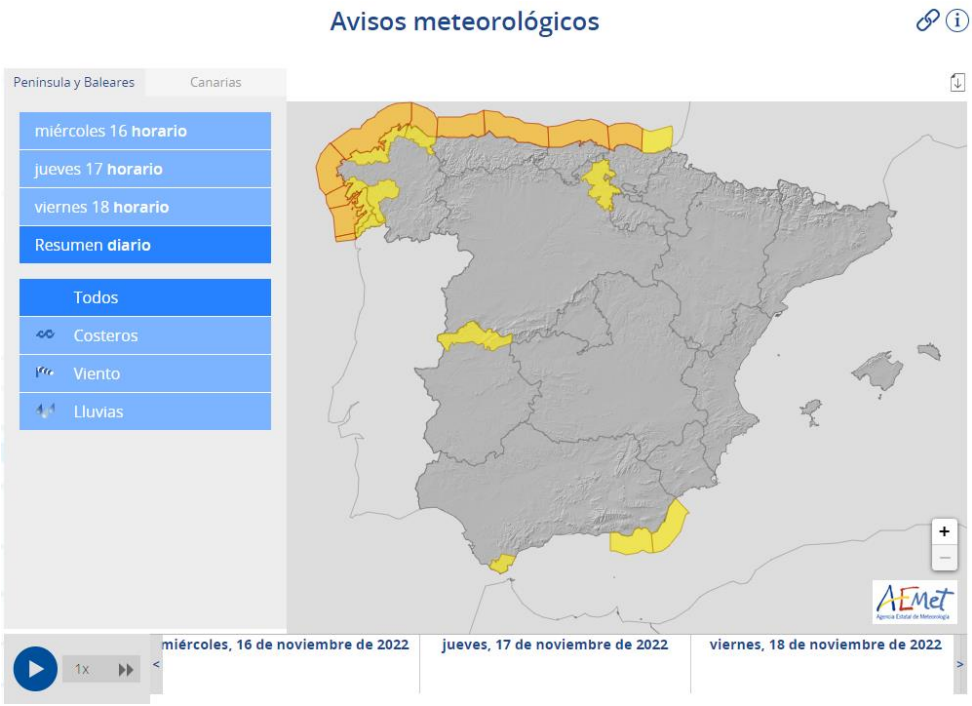
i. Preparativos del mercado eléctrico: todos los participantes del mercado eléctrico ajustan sus ofertas y demandas teniendo en cuenta las condiciones climáticas; Las olas de calor o las olas de frío conllevan un aumento de la demanda eléctrica y los diferentes agentes se adaptan a estas condiciones.
ii. Preparativos técnicos para evitar un incidente: el TSO y los DSOs también se preparan para estas circunstancias, manteniendo una estrecha vigilancia del sistema en general y de las respectivas redes. En el peor de los casos, esto puede incluir la activación de generadores portátiles y de emergencia, la reducción del consumo de ciertos consumidores para evitar restricciones, etc. Esto requiere que los actores relevantes activen su logística, de modo que el material y el equipo estén disponibles en esas regiones o lugares donde los riesgos de incidentes son mayores.

La función principal de AEMET es el seguimiento de las condiciones meteorológicas y del riesgo de incendio. Informa de sus predicciones utilizando principalmente:

- Mapas de alerta meteorológica.
- Mapas de riesgo de incendio.

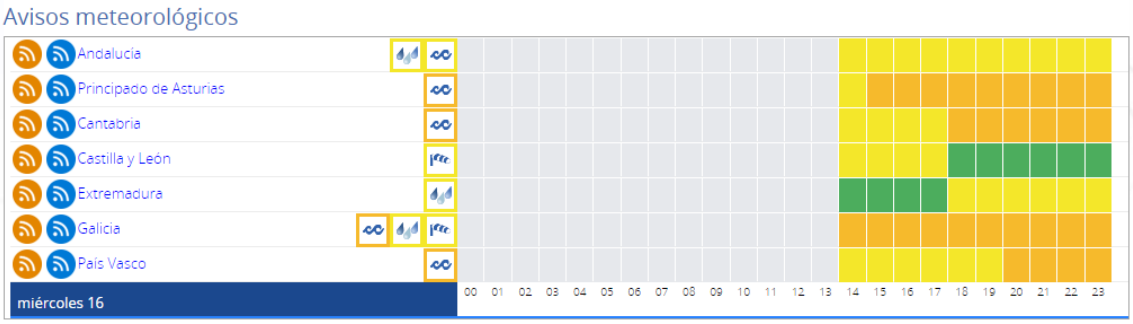
Mapas de alerta meteorológica.

Esta herramienta proporciona información detallada sobre el tipo de anomalía meteorológica (viento, lluvia, alta mar en zonas costeras), el inicio y el final del evento, su intensidad, su evolución y el nivel de riesgo general.



Fuente: AEMET[47]*.*

AEMET utiliza una herramienta de alerta meteorológica para informar de las previsiones de condiciones meteorológicas adversas. También proporciona información específica para cada comunidad autónoma y provincia.

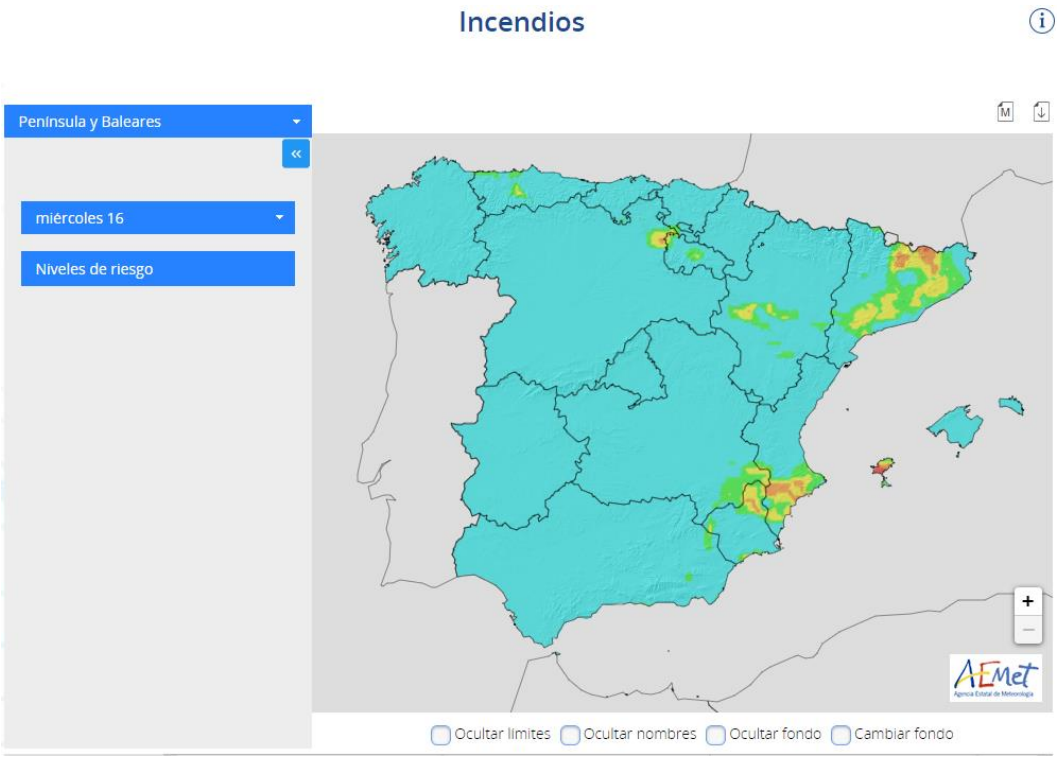


Fuente: AEMET

Mapas de riesgo de incendio.

AEMET ha publicado en su página web una herramienta de predicción de incendios al alcance de todos. El sistema considera variables como la temperatura del aire, la humedad relativa, la velocidad del viento y las precipitaciones registradas en las últimas 24 horas.

[47] Los mapas avisos meteorológicos se pueden localizar en el siguiente enlace de la página web de AEMET: https://www.aemet.es/es/eltiempo/prediccion/avisos



Fuente: AEMET[48]

El riesgo de incendio en las distintas regiones de España puede ser bajo, moderado, alto, muy alto y extremo. Estos sirven como indicador de la probabilidad de ocurrencia de incendios (frecuencia, estacionalidad y causalidad), así como de su extensión e intensidad.

6.1.2 Prevención de incendios en la proximidad de las redes de distribución y transporte.

La prevención de incendios cerca de las redes eléctricas es necesaria para reducir el riesgo de incidentes que puedan provocar una crisis eléctrica.

Los gestores de las redes de transporte y distribución de electricidad pueden mantener libres de vegetación los márgenes donde discurren las líneas, para evitar la generación o propagación de incendios forestales.

Además, cualquier nueva infraestructura requiere que sus pliegos de contratos de mantenimiento incluyan cláusulas específicas relativas a la limpieza y desmalezado de los taludes como medida de prevención de incendios.

6.1.3 Reservas de combustible.

Varias plantas de generación de electricidad utilizan gas natural como combustible. Muchos sistemas de calefacción también utilizan este combustible. La cantidad de gas natural que

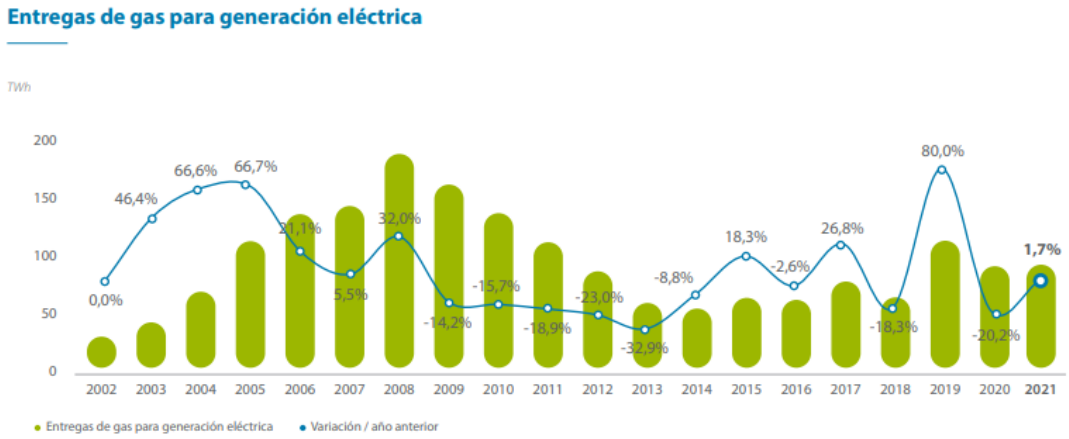
[48] Los mapas avisos de incendios se pueden localizar en el siguiente enlace de la página web de AEMET: https://www.aemet.es/es/eltiempo/prediccion/incendios

necesita cualquier país depende en gran medida de las condiciones climáticas, la demanda de electricidad y la actividad industrial.

En relación con la disponibilidad de gas natural, el Gobierno español actúa en tres frentes: conocimiento y análisis del consumo de gas natural de los generadores en el sector eléctrico (análisis continuo), mantenimiento de suficientes reservas estratégicas de gas natural (respuesta inmediata) y diversificación de las fuentes de gas natural (medidas de medio y largo plazo).

Participación del gas natural utilizado para la generación de electricidad (análisis continuo).

Este análisis puede mostrar la relevancia de las medidas a largo plazo tanto en el sector eléctrico como en el sector gasista. La evolución de la cuota de gas natural utilizada en la generación eléctrica ayuda a planificar y adoptar las decisiones necesarias para compensar los impactos negativos en el sector eléctrico.



Fuente: Enagás – Informe del Sistema Gasista Español 2021.

Reservas de gas natural (preparación para respuesta inmediata).

En caso de interrupción del suministro, podrá utilizar reservas estratégicas de gas natural para satisfacer la demanda por un período determinado de días.

La obligación de mantener existencias mínimas de seguridad de gas natural en España se sitúa actualmente en 20 días de ventas o consumos en firme del año natural anterior[49], que deberán ser mantenidas íntegramente siempre por los sujetos obligados y en almacenamientos subterráneos. Adicionalmente deberá existir una reserva adicional de gas equivalente a 7,5 días de sus ventas o consumos firmes en el año calendario anterior, al menos hasta noviembre.

CORES únicamente supervisa y controla el stock mínimo de seguridad[50]. Está en contacto directo con el Ministerio para la Transición Ecológica y el Reto Demográfico, para que la Autoridad Competente tenga conocimiento instantáneo del volumen de reservas estratégicas.

[49] Art. 2 del Real Decreto 1716/2004, de 23 de julio.
[50] Art. 23 del Real Decreto 1716/2004, de 23 de julio.

Fuente: CORES.

La obligación de mantener existencias mínimas de gas natural recae en los proveedores de gas natural y en los consumidores directos del mercado (por la parte de su consumo firme no proporcionada por un proveedor o comercializador).

Estas entidades deberán disponer, siempre en almacenamiento subterráneo, de un stock mínimo de seguridad de carácter estratégico equivalente a 20 días de ventas o consumos del año natural anterior[51]. Además, al menos hasta el 1 de noviembre, deberán mantener un stock adicional de 7,5 días[52].

Las existencias de mínima seguridad de carácter estratégico sólo podrán estar en almacenamiento subterráneo.

La autoridad para movilizar las existencias mínimas de seguridad de gas natural en caso de necesidad corresponde exclusivamente al Gobierno[53].

El gobierno ordena la movilización de reservas estratégicas sólo cuando la oferta ha demostrado ser incapaz de satisfacer la demanda. Otras medidas pueden acompañar a la activación de reservas, tales como:

a) Suspensión o intervención del mercado.
b) Medidas de restricción de la demanda.

Diversificar las fuentes de gas natural (medida de medio y largo plazo)[54].

Esta medida forma parte de la estrategia de planificación del sector gasista. En materia de seguridad de suministro, CORES contribuye a garantizar una adecuada diversificación del suministro de gas natural en España, controlando que el suministro desde cualquier país no supere el límite del 50% del suministro total.

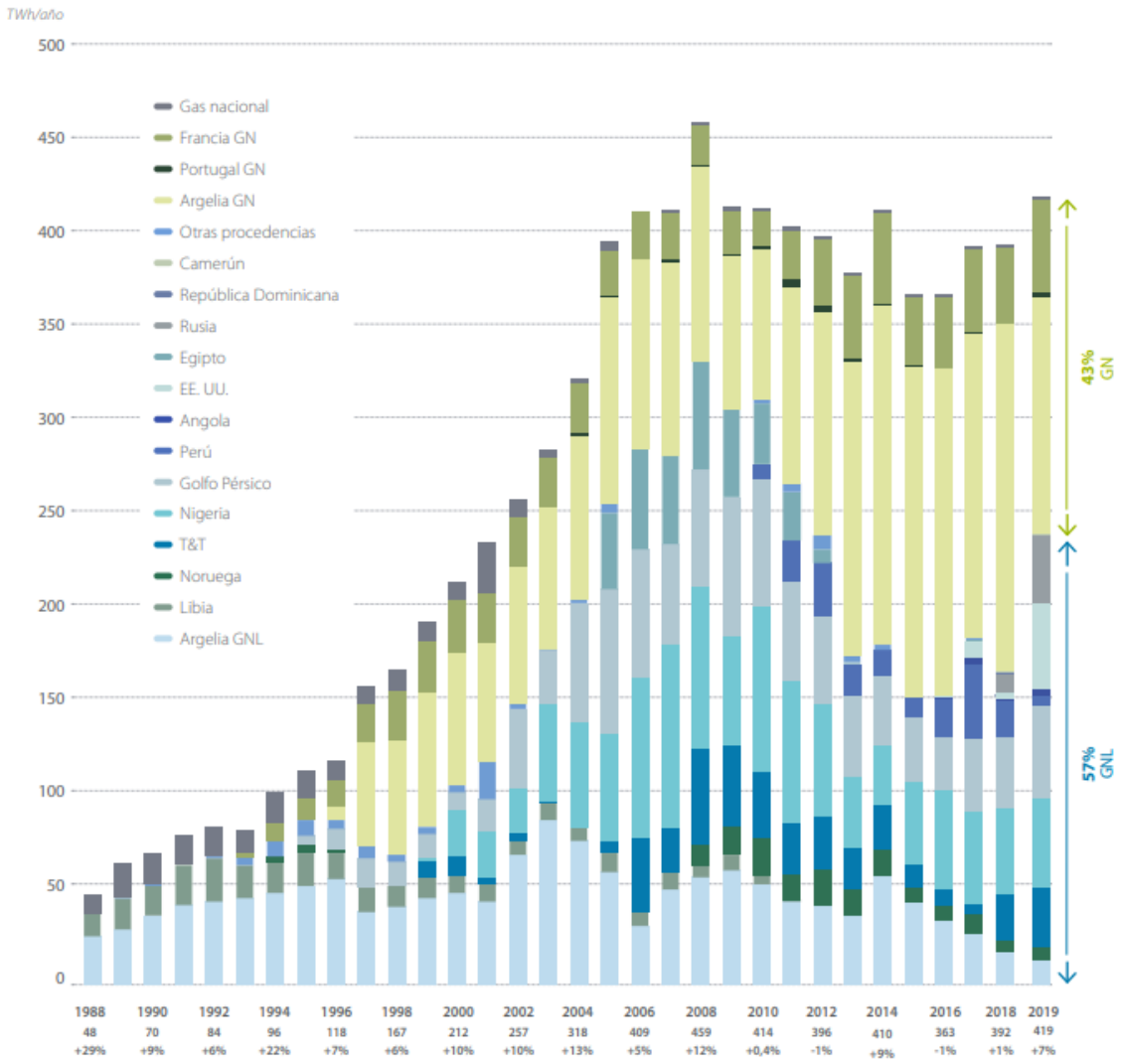
En caso de que la suma de los suministros anuales de gas natural destinados al consumo nacional desde un mismo país de origen sea superior al 50%, se producirán determinados intercambios. En concreto, los comercializadores/proveedores con una cuota superior al 7% de los suministros anuales deberán diversificar su cartera, de modo que su suministro desde el principal país proveedor al mercado nacional sea inferior a dicho 50%.

En 2023, la mayor fuente de gas natural fue Argelia con una cuota del 29,3%, seguida de Estados Unidos, con una cuota del 20,9%[55].

[51] Art. 4 de la Orden TED/72/2023, de 26 de enero.
[52] Art. 17.2 del Real Decreto 1716/2004, de 23 de julio.
[53] Art. 17.1 del Real Decreto 1716/2004, de 23 de julio
[54] https://www.cores.es/es/seguridad-suministro/gas-natural
[55] Fuente: CORES https://www.cores.es/es/estadisticas

Las estadísticas actuales muestran un crecimiento en las cuotas de gas natural de EE.UU. y Nigeria, mientras que el suministro de Argelia ha disminuido, reduciendo la dependencia del gas argelino.

Teniendo en cuenta el punto de entrada, en 2023 España importó 119.356 GWh de gas natural por gasoducto (30,1% del total) y 277.078 GWh mediante transporte y regasificación de GNL (60,9%).



Fuente: Enagás – Informe del Sistema Gasista Español 2021.

Otras consideraciones energéticas sobre las reservas de combustible.

El gas natural (y cualquier otro combustible utilizado como fuente primaria en la generación de electricidad) tiene otros usos. El análisis y seguimiento de las reservas de combustible es una prioridad no sólo para el sector eléctrico, sino también para el sector energético, la economía en general y el bienestar social.

6.1.4 Preparación de la red eléctrica y del sistema.

El PNIEC 2021-2030 y el Plan (+SE) son dos planes nacionales que establecen un marco integral para el despliegue y preparación de la red en España en los próximos años. Sus vectores de trabajo más relevantes incluyen:

- ***Incentivos al desarrollo y operación de la red.***
- ***Mecanismos de apoyo a las renovables.***
- ***Acceso y conexión a la red.***

1. Incentivos al desarrollo y operación de la red.

Los DSOs son responsables de construir, operar, mantener y, si es necesario, desarrollar sus redes de distribución y las conexiones con otras redes. Deben garantizar que sus redes tengan capacidad para hacer frente, en el largo plazo, a una demanda eléctrica razonable.

Tienen incentivos económicos para reducir las pérdidas en sus redes y mejorar la calidad del suministro y del servicio. Penalizan o premian a cada empresa en función de su desempeño respecto al resultado medio del sector. El impacto económico es neutro para los consumidores finales. Los incentivos consideran dos parámetros:

- TIEPI, tiempo de interrupción equivalente de la potencia instalada en media tensión.
- NIEPI, número de interrupciones equivalentes de potencia instalada en media tensión.

Estos parámetros miden las interrupciones programadas e imprevistas en las redes TSO y DSO.

El factor que determina si cada empresa distribuidora debe recibir un incentivo o pagar una penalización cada año es el "indicador de cumplimiento de calidad promedio".

La Circular 6/2019, de 5 de diciembre, de la CNMC, establece la regulación para los DSOs e incluye los incentivos/penalizaciones por la calidad del suministro y del servicio. También regula un incentivo para reducir las pérdidas en la red, siguiendo un esquema similar al de la calidad del suministro.

2. Mecanismos de apoyo a las renovables.

España se encuentra en pleno proceso de descarbonización para garantizar el cumplimiento de la obligación de reducir las emisiones de gases de efecto invernadero y alcanzar la neutralidad climática en 2050, con el objetivo de conseguir un sistema eléctrico 100% renovable.

El PNIEC 2021-2030 tiene como objetivo un despliegue de potencia instalada de energía renovable de modo que previsiblemente generará el 81%[56] de toda la electricidad del país.

Para promover aún más la adopción de energías renovables y la eficiencia energética en el sistema eléctrico español, el gobierno ha aprobado un nuevo mecanismo económico, el régimen económico de energías renovables[57].

[56] Actualizado en la revisión del PNIEC aprobada mediante el Real Decreto 986/2024, de 24 de septiembre.
[57] Regulado en el Real Decreto 960/2020, de 3 de noviembre, por el que se regula el régimen económico de energías renovables para instalaciones de producción de energía eléctrica.

Existe un calendario orientativo para la asignación del régimen económico de las instalaciones de energías renovables, indicando los volúmenes mínimos de potencia acumulada para cada tecnología de generación renovable.

La persona titular del Ministerio para la Transición Ecológica y el Reto Demográfico actualizará este calendario orientativo, al menos anualmente, y lanzará las sucesivas subastas para cumplir el calendario. El calendario orientativo aparece a continuación:

		Volúmenes mínimos de potencia (MW)				
		2022	2023	2024	2025	2026
Eólica.	Incremento anual.	1.500	1.500	1.500	1.500	1.500
	Acumulado desde 2020.	4.000	5.500	7.000	8.500	10.000
Fotovoltaica.	Incremento anual.	1.800	1.800	1.800	1.800	1.800
	Acumulado desde 2020.	4.600	6.400	8.200	10.000	11.800
Solar Termoeléctrica.	Incremento anual.		200		200	
	Acumulado desde 2020.	200	400	400	600	600
Biomasa.	Incremento anual.		120		120	
	Acumulado desde 2020.	140	260	260	380	380
Otras tecnologías (biogás, hidráulica, mareomotriz, etc.).	Incremento anual.		20		20	
	Acumulado desde 2020.	20	40	40	60	60

Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico.

3. Acceso y conexión a la red.

España ha establecido una regulación en materia de acceso y conexión a la red, mediante el Real Decreto 1183/2020, de 29 de diciembre, sobre acceso y conexión a las redes de transporte y distribución de electricidad.

El precitado real decreto ha establecido un procedimiento más ágil, eficiente y ordenado y fija inequívocamente un criterio de prioridad temporal para el otorgamiento de permisos. El real decreto también establece concursos de capacidad de tecnologías renovables en nuevos nodos de la red de transporte.

El Ministerio para la Transición Ecológica y el Reto Demográfico podrá convocar una serie de subastas para la capacidad de acceso en un nodo concreto de la red de transporte para nuevas instalaciones de generación eléctrica que utilicen fuentes de energía primaria renovables y para instalaciones de almacenamiento.

Recientemente se han establecido nuevas reglas para el acceso y conexión de la demanda, incluidas licitaciones de capacidad de acceso en nodos específicos de la red de transporte, por lo que el Ministerio para la Transición Ecológica y el Reto Demográfico podrá convocar una serie de subastas de capacidad de acceso a nuevas instalaciones de demanda que deseen para conectarse a la red de transporte.

De esta forma, España avanza en el proceso de descarbonización mencionado anteriormente para alcanzar la neutralidad climática en 2050, con el objetivo de tener un sistema eléctrico 100% renovable.

6.1.5 Preparación del TSO.

El punto 6.4 del PPR describe los planes de seguridad de TSO. En este punto aparece una breve mención porque algunos de los Planes cubren parcialmente actuaciones preventivas y de preparación.

Los planes de seguridad son instrumentos de colaboración entre el TSO y otros agentes del sistema y aportan diferentes soluciones en diferentes etapas de la crisis.

Los planes organizan la actuación de forma sistemática y coherente, con las diferentes situaciones que puedan surgir en el funcionamiento del sistema.

Estos planes se dividen en dos categorías diferentes:

I. Planes de Emergencia.
II. Planes de Restauración.

Aunque en su mayoría abordan la respuesta una vez producida el evento de crisis, proporcionando provisiones e información para el restablecimiento del servicio después de incidentes severos, hay una parte de este grupo de planes que cubren en parte acciones preventivas y preparatorias. El procedimiento operativo del TSO *P.O. 1.6 Establecimiento de los planes de seguridad para la operación del sistema*, contiene toda la información relacionada con los planes de seguridad. Asimismo, se destacan otros procedimientos de operación de TSO que incluyen acciones de preparación y prevención. Se fijan, por un lado, los procedimientos para pronosticar la oferta de demanda para diferentes horizontes temporales (*P.O. 2.1 Previsión de la demanda*) y, por otro lado, los valores esperados de adecuación para garantizar el funcionamiento seguro y confiable del sistema (*P.O. 2.2 Previsión de la cobertura y análisis de Seguridad del Sistema*).

6.1.6 Independencia energética y seguridad de suministro - despliegue del autoconsumo.

El autoconsumo puede aumentar la seguridad del suministro en la medida en la que:

i. Promueve la generación distribuida.
ii. Empodera a los autoconsumidores y les proporciona una seguridad adicional de suministro, ya que disminuye su dependencia de fuentes eléctricas externas.
iii. Proporciona beneficios económicos ya que el autoconsumo tiene un impacto positivo para los consumidores.

El Gobierno ha implementado la Estrategia Nacional de Autoconsumo y la Hoja de Ruta del Autoconsumo. Algunas de las últimas medidas adoptadas incluyen:

- Agilizar los trámites de autorización, estableciendo una exención de presentar garantías en instalaciones de autoconsumo inferiores a 100 kW.
- Establecer un plazo de 2 meses entre la solicitud y la operación de permisos. El incumplimiento de este plazo implica el descuento automático para los autoconsumidores en la factura de la luz.

- Consumidores acogidos a autoconsumo colectivo pueden autoconsumir a través de las redes DSO y TSO, independientemente del nivel de tensión. Anteriormente esto sólo podía realizarse en Redes de Baja Tensión (inferiores a 1 kV).
- Incremento de la distancia máxima para el autoconsumo de proximidad de instalaciones fotovoltaicas de 500m a 2 km.
- Reservar el 10% de la capacidad existente en los nodos de la red de transporte para instalaciones de autoconsumo. La misma reserva existe en la red de distribución si la instalación tiene una potencia superior a 5 MW.
- Implantación de instalaciones fotovoltaicas para autoconsumo en edificios e infraestructuras de la Administración General del Estado. Todas las administraciones públicas (estatales, autonómicas y locales) deberán elaborar un plan de despliegue del autoconsumo.

6.1.7 Ciberseguridad.

La preparación en materia de ciberseguridad se lleva a cabo en diferentes niveles: usuario final y servicios TIC.

Los usuarios finales son casi siempre el objetivo directo de los ciberataques, ya que tienen menos preparación que el personal de TIC y se convertirán más fácilmente en puntos de entrada a los servidores.

- La mejor forma de prepararse es la formación interna continua a todo el personal, y en especial a todos aquellos con responsabilidades en la toma de decisiones. Cuando los empleados saben que ciertos comportamientos y acciones son riesgosos, es más probable que los eviten.
- Los equipos de todos los servicios TIC deben preparar servicios e infraestructuras TIC para ciberataques. Su formación es una acción crucial en ciberseguridad.

El Informe sobre la Cibercriminalidad en España 2022 del Ministerio del Interior refleja que el sector energético ha sido el principal sector PIC afectado por número de incidentes, con el 37,2% del total de ataques e incidentes. Los principales incidentes que han afectado a infraestructuras críticas se encuadran en las siguientes categorías:

i. Sistemas vulnerables, con el 60,81% de las incidencias.
ii. Robo de información, con un 20,88%.
iii. Fraude, con un 6,59%, de entre los tipos de fraude con mayor relevancia, destacan:
    - Suplantación de identidad: consiste en el envío de correo electrónico personalizado, tras un análisis exhaustivo de la víctima, para que realice una transferencia a una cuenta contralada por los delincuentes, modifique la cuenta de pago de la factura de un proveedor, etc.
    - Phising: consiste principalmente en la recepción por parte de la víctima de un correo electrónico destinado a que comparta, normalmente a través de un enlace a una web fraudulenta, credenciales, datos personales, números de cuenta bancaria, datos de tarjetas de crédito o cualquier otro dato confidencial.
iv. Malware, con un 4,76%. Los tipos de malwares más relevantes son:

- Emotet: Funciona como *"downloader"* permitiendo la descarga y ejecución de otros códigos dañinos, así como la monitorización del tráfico de red, obteniendo cualquier información contenida en los navegadores de la víctima, desde credenciales de usuario hasta información bancaria.
- Mekotio: También conocido como BestaFera, representa una amenaza grave para todos aquellos usuarios que hacen uso de servicios de banca online o de criptodivisas, concretamente de Bitcoins, ya que se trata de un troyano bancario que afecta a todas las versiones del sistema operativo Windows, comprendidas entre Windows XP y Windows 10.
  Funciona como *"downloader"* permitiendo la descarga y ejecución de otros códigos dañinos, así como la monitorización del tráfico de red, obteniendo cualquier información contenida en los navegadores de la víctima.
- Flubot: Software malicioso de tipo troyano para dispositivos Android. Las campañas más habituales implicaron el envío de SMS fraudulentos que avisaban de la recepción de un paquete suplantando a diferentes empresas logísticas, como FedEx, DHL o Correos. Estos mensajes invitan al receptor a instalar una aplicación en su dispositivo móvil con el incentivo de que éste pueda conocer el paradero del paquete. Una vez que el usuario realiza la instalación de la aplicación en su dispositivo, ésta comienza a rastrear los identificadores de todas las aplicaciones que se inicien, con la capacidad de inyectar páginas superpuestas al detectar un inicio de sesión en una de las aplicaciones objetivo, de forma que el usuario se confía en que está introduciendo las credenciales en la web original cuando, en realidad, las está enviando al servidor de mando y control controlado por los operadores del código dañino.
- Anatsa: Malware de tipo troyano para dispositivos Android que ha sido analizado, en paralelo, por diferentes organizaciones asignándole diferentes nombres como: Anatsa, TeaBot o Toddler.
  Al igual que en Flubot, una vez que el usuario realiza la instalación de la aplicación en su dispositivo, ésta comienza a rastrear los identificadores de todas las aplicaciones iniciadas, con la capacidad de inyectar páginas superpuestas al detectar un inicio de sesión en una de las aplicaciones objetivo, de forma que el usuario confía en que está introduciendo las credenciales en la web original cuando, en realidad, las está enviando al servidor de mando y control controlado por los operadores del código dañino.
- Hive: Malware de tipo "*ransomware"* que implementa las funcionalidades de cifrado de la información de un equipo infectado, imposibilitando la recuperación de los datos de forma sencilla.

Teniendo en cuenta lo anterior, parte de los simulacros mencionados en el siguiente apartado y descritos en el Capítulo 9 del PPR se centran en la ciberseguridad.

6.1.8 Simulacros.

Los ejercicios de simulación son una de las mejores herramientas de preparación para cualquier tipo de crisis ya que permiten entrenar las respuestas para que en las crisis surjan de forma automática y fluida. Esto reduce el lapso entre la aparición de un problema y su solución.

Estos ejercicios se realizan periódicamente, refrescando y actualizando así la formación y conductas necesarias antes y durante una crisis. La frecuencia de estos ejercicios depende de la temática y es bianual, anual y en algunos casos bienal.

Para una descripción detallada de los diferentes ejercicios de simulación realizados en relación con el PPR español consulte el Capítulo 9 de este documento.

6.2 Comunicación.

La comunicación es fundamental en una crisis eléctrica. Cuando la información fluye rápidamente, todos los agentes relevantes actúan antes de que la crisis empeore o incluso se manifieste. Esto es relevante en todos los niveles, tanto en el ámbito público como en el sector privado.

Existen varios niveles de comunicación en el PPR:

- Comunicaciones formales:
    - A otros países y a la UE, para que los países vecinos puedan empezar a adoptar medidas preventivas antes de que la crisis cruce las fronteras o medidas paliativas para minimizar el impacto transfronterizo.
    - A los diferentes niveles de la administración pública y autoridades, para comenzar a actuar y activar equipos de respuesta a emergencias y comenzar a trabajar para la respuesta a corto y mediano plazo.
    - A los agentes y operadores del sistema eléctrico.
- Comunicaciones operativas e información proporcionada a diferentes grupos y partes interesadas.

6.2.1 Notificación formal de una alerta temprana y actualizaciones.

La "alerta temprana" en el PPR es una remisión de información concreta y confiable que indique que puede ocurrir un evento que probablemente resulte en un deterioro significativo del suministro de electricidad y que probablemente conduzca a una crisis de electricidad.

Declarar una alerta temprana es un tema relevante porque si una Autoridad Competente emite una alerta temprana (o declara una crisis de electricidad), se deberán seguir en su totalidad las medidas establecidas en el PPR.

Así, la declaración de alerta temprana es un paso fundamental en el Plan de Prevención de Riesgos español, así como en los PPR de otros Estados miembros.

En cumplimiento del apartado 1 del artículo 14 del Reglamento (UE) 2019/941, la declaración por parte de España de una disminución anticipada del PPR es el resultado de la detección de una amenaza potencial de crisis de suministro eléctrico.

Esta amenaza potencial puede manifestarse a través de:

- **Sistemas de alerta sobre condiciones meteorológicas e incendios forestales** – AEMET recopila y facilita esta información[58]. Se refiere a las condiciones climáticas y meteorológicas que pueden provocar determinadas crisis, en concreto:

    - El escenario de tormenta extrema.
    - El escenario de los incendios forestales.

    Estas mismas herramientas y sistemas también sirven para detectar otros fenómenos meteorológicos extremos, como olas de calor, tormentas de nieve y ventiscas, olas de

[58] Art. 8 del Real Decreto 186/2008, de 8 de febrero, por el que se aprueba el Estatuto de la Agencia Estatal de Meteorología, incluidas las letras a), c), e) y f).

frío e inundaciones. Si bien es muy poco probable que estos escenarios formen parte del Plan PPR, las autoridades no pueden ignorarlos y permanecerán atentos a ellos.

- **Información relativa a las reservas de combustible que apuntan a una posible escasez:** el TSO de gas detecta una cantidad insuficiente de reservas de combustible o una situación que amenaza la producción de gas natural en uno o más de sus proveedores de gas natural. Esto se lleva a cabo mediante dos vías de actuación:
    - Monitorización y control de las reservas de combustibles a nivel nacional mediante comunicación directa con los agentes pertinentes[59].
    - Mediante la recopilación de información, ya sea directamente de los propios proveedores de gas o a través de las agencias y organismos internacionales en los que participa el TSO de gas de España[60].

- **Ataques y amenazas a la ciberseguridad** - la OCC proporciona un canal permanente de alerta temprana[61] sobre vulnerabilidades, ciberamenazas y ciberataques.
  También establece canales de intercambio de información entre otros actores, públicos y privados, nacionales e internacionales y, en su caso, traslada la información técnica del incidente a las Fuerzas y Cuerpos de Seguridad del Estado para su investigación. Estos canales proporcionan información útil sobre amenazas.[62]
  Además, la OCC también pertenece al Foro CSIRT.es[63], donde coordina y colabora con los Equipos de Respuesta a Incidentes de Seguridad Informática nacionales[64].
  INCIBE-CERT también proporciona los avisos e informes periódicos en su página web[65].
- **Amenazas externas** – los diferentes cuerpos policiales y Servicios de Protección Civil recogen y facilitan esta información, a nivel nacional e internacional[66].
- **Otras amenazas** – los distintos órganos del Gobierno y la administración española, así como los gobiernos y administraciones autonómicas podrán recabar y facilitar información sobre cualquier otro tipo de riesgos, a nivel nacional e internacional.

Por tanto, cuando una evaluación de adecuación estacional o cuando cualquier otra fuente cualificada proporcione información concreta y fiable de que puede producirse una crisis eléctrica en España, la Autoridad Competente notificará una alerta temprana a las siguientes partes:

i. La CE, a través del ECG.
ii. Las Autoridades Competentes del EEMM dentro de la Región de Operación del Sistema de Europa Sudoeste (SWE SOR).
iii. Las Autoridades Competentes o autoridad equivalente de los terceros países directamente conectados al sistema eléctrico español.

La Autoridad Competente notificará a estas partes a través de todos los canales de comunicación disponibles hasta que proporcionen confirmación de la recepción.

---

[59] Art. 23 del Real Decreto 1716/2004, de 23 de julio.
[60] Art. 64 de la Ley 34/1998, de 7 de octubre.
[61] Art. 12 del Real Decreto-ley 12/2018, de 7 de septiembre.
[62] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.
[63] CSIRT: Computer Security Incident Response Team.
[64] Art. 6 del Real Decreto 207/2024, de 27 de febrero.
[65] https://www.incibe.es/incibe-cert
[66] Art. 2 del Plan Estatal General de Emergencias de Protección Civil.

Podrá contactar con ellos mediante la lista actualizada de contactos de emergencia, descrita en el artículo 14 del Reglamento de preparación ante riesgos o similar.

Una vez activa la alerta temprana, el gobierno seguirá continuamente la evolución de la situación. Utilizará la información recopilada para actualizar la declaración de alerta temprana, encontrándose en tres posibles situaciones:

- La situación se desescala y los riesgos asociados a la misma vuelven a niveles normales.
- La situación sigue siendo la misma y el nivel de preparación se mantiene en su nivel actual.
- La situación empeora y se desarrolla una crisis.

Las actualizaciones serán diferentes en cada una de estas situaciones.

6.2.2 Notificación formal de una crisis de electricidad.

Una "crisis de electricidad" es una situación presente o inminente en la que existe una escasez significativa de suministro de electricidad, según las condiciones establecidas por los Estados Miembros en sus PPR, o en la que es imposible suministrar electricidad a los clientes.

En la mayoría de los casos habrá algún tipo de alerta previa antes de que se produzca la crisis de electricidad. Una situación que da paso a una alerta temprana puede evolucionar negativamente y los impactos pueden comenzar a manifestarse o incluso empeorar. En este caso, el gobierno español notificará una crisis eléctrica.

Ante estas situaciones, el gobierno estará realizando un seguimiento de la evolución de la situación que provocó la "alerta temprana".

Sin embargo, puede desarrollarse una situación en la que no haya tiempo entre la amenaza/riesgo y la aparición de los primeros impactos negativos (y cortes de electricidad).

Tal como se describe en los capítulos dos y cinco de este PPR, la Autoridad Competente notificará la declaración de crisis de electricidad a:

i. La CE, a través del ECG.
ii. Las Autoridades Competentes del EEMM dentro de la Región de Operación del Sistema de Europa Sudoeste (SWE SOR).
iii. Las Autoridades Competentes o autoridad equivalente de los terceros países directamente conectados al sistema eléctrico español, entre los que se incluyen Andorra y Marruecos.

La Autoridad Competente notificará a estas partes a través de todos los canales de comunicación disponibles hasta que proporcionen confirmación de la recepción.

Podrá contactar con ellos mediante la lista actualizada de contactos de emergencia, descrita en el artículo 14 del Reglamento de preparación ante riesgos o similar.

6.2.3 Comunicaciones operativas en una crisis.

Una comunicación fluida entre todas las partes es una cuestión clave en circunstancias normales, pero más cuando estamos en medio de una crisis. En el PPR la comunicación es relevante en tres niveles:

i. Entre la Autoridad Competente y el TSO.
ii. Entre la Autoridad Competente y los agentes eléctricos.
iii. Entre agentes dentro del sistema eléctrico.

Comunicación entre la Autoridad Competente y el TSO.

Los canales de comunicación entre el TSO y el Ministerio para la Transición Ecológica y el Reto Demográfico son fluidos y constantes. La información fluye inmediatamente en ambas direcciones tanto a nivel directivo como a nivel operativo.

En los canales de comunicación de alto nivel el interlocutor designado por la Autoridad Competente es la persona titular de la **Dirección General de Política Energética y Minas**

La información sobre los interlocutores del TSO no se incluye por motivos de confidencialidad.

Comunicación entre la Autoridad Competente y otros agentes del sistema eléctrico.

Los canales de comunicación entre el Ministerio para la Transición Ecológica y el Reto Demográfico y otros agentes eléctricos son similares a los del TSO. La información fluye en ambas direcciones tanto a nivel directivo como a nivel operativo.

En cuestiones de operación del sistema, el TSO también podrá actuar como intermediario con otros agentes eléctricos. En relación con el funcionamiento o las reglas del mercado, la ARN también podrá impartir instrucciones y comunicarse con los agentes del sistema eléctrico.

Como antes, el interlocutor designado por la Autoridad Competente sigue siendo La persona titular de la **Dirección General de Política Energética y Minas.**

La información sobre los interlocutores de cualquiera de los agentes tampoco se incluye por cuestiones de confidencialidad.

El Ministerio tiene a su disposición sus registros administrativos a los agentes eléctricos del sector eléctrico, así como los registros de otros sectores energéticos. La ARN también puede acceder a esta información.

Comunicación entre agentes del sistema eléctrico[67].

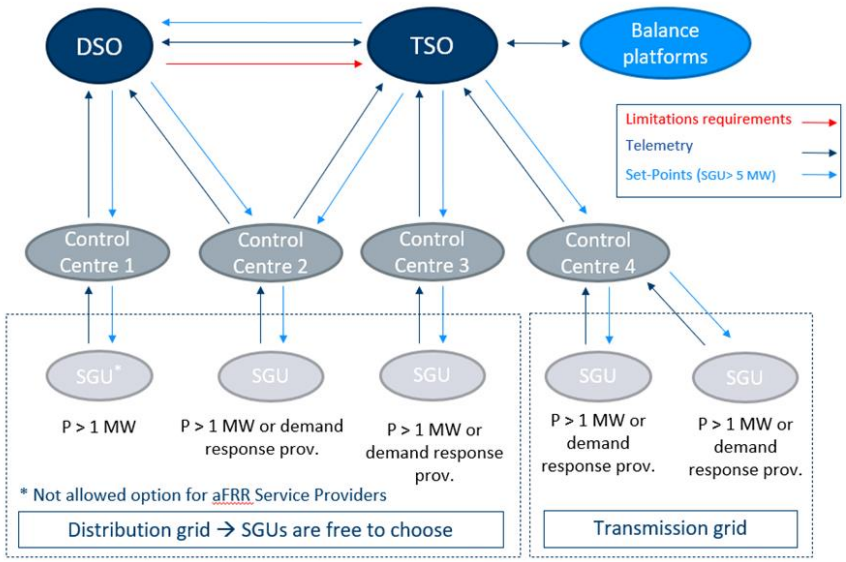
Durante la operación del sistema, incluso cuando se produce un incidente, el TSO está constantemente intercambiando datos con los diferentes agentes del sistema eléctrico mediante protocolos, plataformas y enlaces de comunicación establecidos que proporcionan la información necesaria para mantener la seguridad y la continuidad del suministro eléctrico. El TSO recibe datos de otros TSO, DSO y usuarios significativos de la red (USR), como generadores, unidades de almacenamiento e instalaciones de demanda.

[67] Los diferentes sistemas de comunicación se encuentran establecidos en los procedimientos nacionales "P.O. 9.0 Información intercambiada por el operador del Sistema", "P.O. 9.1 Intercambios de información relativa al proceso de programación" y "P.O. 9.2 Intercambio de información en tiempo real con el operador del Sistema".

Desde los DSO y otros TSO, el SO recibe datos en tiempo real de su área de observación, necesita para operar el sistema eléctrico. Los datos en tiempo real se intercambian a través de enlaces de comunicación establecidos entre el sistema de gestión de energía del TSO y los sistemas de los TSO y de otros TSO. Este intercambio incluye información de la topología, tensión y potencia activa y reactiva de los elementos de la red. Para los TSO, existe una plataforma europea adicional denominada EAS (*European Awareness System*) que permite el intercambio de datos en tiempo real sobre el estado del sistema de cada TSO. Además de los datos mencionados anteriormente, el TSO también recibe datos programados y en tiempo real de todas las UGE que tengan una capacidad de potencia activa superior a 1 MW o que participen en servicios de saldo. Esto se consigue de diferentes formas según el tipo de información que se intercambie:

1. El intercambio de datos programados se realiza a través de la plataforma de balance y mercado denominada eSIOS. Estos datos incluyen horarios de potencia activa y disponibilidades en el horizonte temporal del mercado diario e intradiario.
2. El intercambio de datos en tiempo real se realiza a través de enlaces de comunicación establecidos entre el sistema de gestión energética del TSO y los sistemas de los centros de control de generación y demanda (CC GD).

Esta información es utilizada por el TSO para lograr el equilibrio del sistema y analizar su seguridad y adecuación para garantizar la continuidad y calidad del suministro eléctrico. El siguiente diagrama muestra el esquema de intercambio de datos en tiempo real entre el TSO y los diferentes agentes.



Fuente: Red Eléctrica de España, S.A.U.

Como se puede observar en el esquema, los USR/SGU[68] conectados a la red de transporte intercambiarán datos en tiempo real directamente con el TSO a través de su CC GD (USG 4 y 5). En el caso de SGU conectados a distribución, pueden elegir cómo el CC GD proporciona sus datos en tiempo real al TSO, utilizando enlaces de comunicación directos con el TSO (SGU 3 o 2) o utilizando enlaces de comunicación con su DSO de conexión (SGU 1 o 2). En el segundo caso, los DSO intercambiarán datos de SGU con el TSO a través de sus propios enlaces de comunicación. Todos los puntos de ajuste de TSO se envían utilizando las mismas rutas de comunicación.

[68] *Significant Grid User.*

El intercambio de datos en tiempo real con el TSO está garantizado ya que todos los enlaces de comunicación están duplicados. CECOEL[69], que es el principal centro de control del TSO, que funciona las 24 horas del día, los 365 días del año, monitoriza el sistema eléctrico a través de su sistema de gestión energética, que recibe datos en tiempo real de las subestaciones transmisoras y de todos los agentes, tal y como se ha descrito anteriormente. Además, el TSO dispone de medios de comunicación de datos y voz para intercambiar información e instrucciones con los agentes del sistema eléctrico en cada momento que sea necesario.

Fuente: Red Eléctrica de España, S.A.U.

Además, cuando se produce un incidente, el TSO recoge información adicional de los diferentes agentes y elabora un informe detallado estableciendo:

1. Fecha y hora del incidente.
2. Elementos de la red de transporte o distribución observables afectados por el incidente.
3. Si están disponibles, registros de oscilaciones y registros de aquellos esquemas de protección que se activen durante el incidente.
4. En su caso, impacto en consumidores o generadores: número de instalaciones afectadas por el incidente, energía no suministrada o no generada y plazo.
5. Descripción detallada del incidente y cronología.
6. Cualquier otra información disponible.

Con toda la información disponible, no sólo el TSO sino todos los agentes pueden analizar sus respuestas para mejorar y actualizar sus procedimientos de atención de incidencias con el objetivo de minimizar su impacto en el futuro, incluidas aquellas que puedan evolucionar hacia una crisis eléctrica.

[69] Centro de Control Eléctrico de Red Eléctrica.

6.3 Activación de la coordinación.

A nivel nacional, el Gobierno coordinará todas las acciones a través del Coordinador de Crisis. Otros organismos pueden participar en esta acción de coordinación, como pueden ser:

- Comisiones Interministeriales.
- Órganos de Coordinación Administrativa.

Como se ha mencionado anteriormente, España participa en varias iniciativas de coordinación a nivel internacional que son relevantes durante una crisis eléctrica:

- El Grupo de Coordinación Eléctrica (ECG).
- ACER.
- CORESO.
- ENTSO-E.
- ENTSOG.

Los primeros pasos requieren la notificación formal de una crisis de electricidad. La Autoridad Competente lo notificará a la Comisión, a los países vecinos y a otros EEMM, siguiendo los procedimientos descritos en el punto 6.2 de este plan. Esto conducirá a la activación de órganos de coordinación también a nivel internacional.

El TSO activará la coordinación dentro del sistema español y notificará a ENTSO-E y CORESO en preparación para posibles impactos transfronterizos.

Lo notificará a los TSO franceses y portugueses y a los TSO de los terceros países que interconecten con España.

La ARN española (CNMC) también notificará a ACER que existe una crisis eléctrica (potencial o real) para que las ANR de otros Estados miembros puedan asesorar sobre las mejores prácticas y la adecuación de los procedimientos de funcionamiento del mercado adoptados en respuesta a la crisis.

6.4 Acciones correctivas.

Las acciones correctivas pueden clasificarse en tres grandes categorías: operación del sistema eléctrico, operación del mercado y acciones que quedan fuera del sector eléctrico. Muchas de estas acciones se incluyen en más de uno de estos grupos.

6.4.1 Medidas para la operación del sistema.

Las acciones correctivas sobre la operación del sistema buscan reparar y reducir los impactos una vez ocurrido un incidente. Cuando se produce un corte de suministro, las acciones correctivas incluyen dos grandes categorías. Estas categorías reflejan de qué lado de la oferta actúa la medida.

Las categorías son:

1) **Acciones en el lado de la generación:** las alternativas consideradas incluyen la generación a partir de capacidad no utilizada u ociosa. Esta acción permite una respuesta inmediata ante una disminución repentina de la generación.

2) **Acciones en el lado del consumo**: que son acciones que permiten dar una respuesta por el lado de la demanda.

Dos cuestiones son muy relevantes durante las crisis de oferta:

- ***Programas de generación y análisis de seguridad de suministro.***
  Los productores que participen en el mercado darán al TSO el cronograma de interrupciones de generación por módulos de generación, para que pueda tener en consideración esta información en el análisis de seguridad del sistema.
  Por razones de seguridad del sistema, en determinados casos el TSO podrá definir previamente y comunicar a los participantes del mercado, criterios y códigos específicos utilizados para estos desgloses de programación.
  El desglose de programas será aplicable a todas aquellas unidades de programación compuestas por más de un módulo en los distintos horizontes de programación en los que la unidad de programación haya modificado su programa.

- ***Asignación de capacidad en interconexiones internacionales.***
  En caso de incidente, incluidas crisis eléctricas, pueden producirse desviaciones en la asignación de capacidad. Si la crisis tiene impactos transfronterizos, los TSO de ambos lados de la frontera deberán resolver las desviaciones en los flujos de electricidad y las asignaciones de capacidad.
  Además, aplicarán las acciones coordinadas (deslastre de carga, etc.) que figuran en los acuerdos entre Estados miembros, y se referirán a los estudios y análisis de asignación de capacidad en el momento del incidente.

Este resumen de las acciones operativas relevantes se ve seguida de a una descripción más detallada.

Descripción de respuestas operativas inmediatas y a corto plazo.

El TSO, en colaboración con otros agentes del sistema, ha desarrollado y puesto en marcha planes de seguridad para hacer frente a las diferentes situaciones que puedan surgir en el

funcionamiento del sistema. Estos planes de seguridad proporcionan un marco de forma sistemática y coherente, que permite a todos los participantes acudir a ellos y ser conscientes de lo que deben hacer ante los diferentes incidentes y situaciones que afectan al funcionamiento del sistema, incluidos aquellos incidentes que den paso a crisis eléctricas.

Estos planes de acción se dividen en tres categorías diferentes:

I. Planes de Emergencia.
II. Planes de Reposición del Servicio.

I. Planes de Emergencia.

El objetivo de los Planes de Emergencia es minimizar el alcance y extensión de los incidentes una vez ocurridos. Esos planes serán establecidos por el TSO y podrían incluir tanto esquemas de protección automática como medidas operativas específicas.

Por un lado, los esquemas de protección automática incluyen:

a) Sistema automático de reducción de potencia y esquemas especiales de protección.

El TSO podría utilizar esquemas especiales de protección, automatismos para el disparo automático de determinadas instalaciones de generación tras una contingencia predefinida y podría utilizar un sistema automático de reducción de potencia para mantener la seguridad del sistema.

b) Sistema de control automático de subfrecuencia.

El esquema de control automático de subfrecuencia incluye la contribución del modo regulación potencia-frecuencia limitado a subfrecuencia (MRPFL-U), la contribución de los equipos de almacenamiento y un esquema automático de deslastre de cargas de subfrecuencia.

Para aquellas instalaciones de generación que no apliquen los requisitos establecidos en la Orden TED/749/2020, el esquema de control de subfrecuencia deberá coordinarse con el sistema de deslastre de carga de subfrecuencia, de modo que sólo podrán desconectarse de la red si la frecuencia baja de 48 Hz al menos 3 segundos cronometrados.

El sistema de deslastre de carga por subfrecuencia necesario será establecido por el TSO en aquellos casos en los que, debido a un incidente grave, no se pueda restablecer el equilibrio entre generación y demanda mediante las actuaciones de control previstas. Este sistema de deslastre de cargas por subfrecuencia se basará en un sistema automático, para conseguir el control de desconexión de las cargas.

Para aquellas instalaciones de generación que apliquen los requisitos establecidos en la Orden TED/749/2020 o en la norma que la sustituya, deberán permanecer conectadas y operativas dentro de los rangos de frecuencia y plazos especificados en dicha norma.

c) Sistema de control automático de sobrefrecuencia.

El sistema de control automático de sobrefrecuencia incluye el aporte del modo regulación potencia-frecuencia limitado a sobrefrecuencia (MRPFL-O) y un esquema de desconexión de generación por sobrefrecuencia.

Aquellas instalaciones de generación que apliquen los requisitos establecidos en la Orden TED/749/2020 o en la norma que la sustituya, deberán permanecer conectadas y operativas dentro de los rangos de frecuencia y plazos especificados en dicha norma, salvo que el TSO notifique un ajuste de desconexión inferior.

Por otro lado, las medidas operativas específicas incluyen:

a) Reserva de sustitución y redespacho de generación.

Las desviaciones entre generación y consumo pueden ocurrir debido a que existe una indisponibilidad y/o desvío de los equipos de generación con respecto al programa resultante del mercado y/o debido a cambios en el pronóstico de demanda y/o pronóstico de entrega para la producción de energía eólica y solar.

El artículo 3(2)(8) del Código de Red sobre Operación del Sistema define la reserva de sustitución (RR) como las reservas de energía activa disponibles para restaurar o soportar el nivel requerido de reserva de sustitución de frecuencia (FRR) para estar preparado para desequilibrios adicionales del sistema, incluyendo reservas de generación.

b) Modificación o cancelación de programas de intercambio internacional.

Las asignaciones de capacidad y dirección de los flujos de potencia activa resultarán de la diferencia entre el valor máximo teórico de la capacidad de intercambio y el margen de seguridad en estos estudios. Se consideran los siguientes criterios:

a) Las contingencias en los sistemas eléctricos vecinos incluidas en los acuerdos suscritos con sus TSO, así como las sobrecargas temporales permitidas en las interconexiones.
b) Podrá permitirse la actuación de mecanismos de disparo en líneas de interconexión siempre que el sistema eléctrico peninsular permanezca conectado al resto del sistema europeo a través de, al menos, dos líneas de la red de transporte, y de dichas líneas sea de 400 kV.

En el escenario de estudio, la generación del sistema eléctrico español y del vecino cuya interconexión es objeto de cálculo cambiarán para producir las variaciones discretas en el programa de intercambio.

La metodología utilizada será, para la interconexión España-Francia y España-Portugal, la derivada de la aplicación del artículo 21 del Reglamento (UE) 2015/1222 o del artículo 10 del Reglamento (UE) 2016/1719.

En ausencia de una metodología regional y para las interconexiones España-Marruecos y España-Andorra, los acuerdos de TSO con estos terceros países establecerán la metodología específica.

Los valores de asignación de capacidad son el resultado de aplicar un margen de seguridad al valor máximo teórico de capacidad de intercambio. Para la interconexión España-Francia y España-Portugal, este margen de seguridad derivará de la aplicación del artículo 21 del Reglamento (UE) 2015/1222 o del artículo 10 del Reglamento (UE) 2016/1719, en función del horizonte de previsión.

A falta de una metodología regional y para la interconexión España-Marruecos y España-Andorra, el margen de seguridad se fijará en los acuerdos entre TSOs.

Finalmente, la asignación de capacidad para una determinada interconexión y dirección del flujo de potencia activa resultará de la diferencia entre el valor teórico máximo de la capacidad de intercambio y el margen de seguridad.

El TSO español firmará acuerdos con los TSO de sistemas eléctricos interconectados, que determinarán también cómo calcular y compensar las desviaciones entre sistemas eléctricos.

Estos procesos de desviación aplicarán las normas comunes de liquidación vigentes y aplicables a los intercambios de pérdidas intencionadas de energía, derivadas del proceso de contención de frecuencia y rampas de variación de potencia, y a los intercambios de energía no intencionados, en aplicación de los artículos 50.3 y 51.1 del Reglamento (UE) 2017/2195.

El TSO resolverá las desviaciones entre sistemas eléctricos de acuerdo con los procedimientos operativos vigentes.

c) Servicios de control de tensión.

Las medidas de control de tensión son un servicio indispensable para realizar una operación confiable y segura del sistema.

Consiste en un conjunto de actuaciones sobre los recursos de generación y absorción de energía reactiva (generadores, reactancias, condensadores, etc.) y otros elementos de control de tensión, como transformadores con cambiadores de tomas, encaminadas a mantener las tensiones en los nodos de la red de transporte dentro de los márgenes especificados para garantizar el cumplimiento de los criterios de seguridad y calidad del suministro eléctrico.

Como medida excepcional, en caso de necesidad, el TSO podrá adoptar aquellas acciones necesarias para mantener las tensiones en los nodos de la red de transporte dentro del rango seguro, incluyendo instrucciones específicas a adoptar por los proveedores de servicios, respecto de la tensión a mantener. y/o la potencia reactiva a inyectar o consumir en cada nodo fronterizo de la red de transmisión.

El control de tensión se realiza de la siguiente manera:

a) Los generadores de energía podrán:

i. Proporcionar su capacidad máxima de generación y capacidad de absorción reactiva, mediante declaración de disponibilidad de los recursos mínimos obligatorios y suministro opcional de recursos adicionales que excedan el margen mínimo obligatorio.
ii. Funcionar como compensadores sincrónicos: estas ofertas de servicios deben ser independientes de las anteriores.

b) Los consumidores y gestores de la red de distribución podrán participar en el control de tensión mediante dos actuaciones diferentes:

i. Prestar servicios equivalentes a una generación reactiva adicional en el sistema.
ii. Proporcionar servicios equivalentes a una absorción adicional de reactivo en el sistema. Estas actuaciones se desarrollan en cada punto de conexión con la red eléctrica.

II. Planes de Reposición de Servicio.

El objetivo de los diferentes Planes de Reposición de Servicio es devolver el sistema eléctrico a su estado normal de funcionamiento tras graves incidencias que han provocado cortes de suministro.

Estos planes establecen las acciones sistemáticas para los diferentes centros de control y personal operativo local de las subestaciones en caso de un incidente generalizado.

En caso de ocurrir un incidente regional o nacional, los centros de control de los diferentes generadores, DSO y TSO retornarán el servicio, de acuerdo con las indicaciones establecidas en los correspondientes Planes de Restablecimiento, bajo la dirección del TSO.

6.4.2 Otras acciones.

Estas medidas pueden abarcar una amplia gama de cuestiones. Algunas pueden quedar fuera del ámbito del sector eléctrico, afectar también a otros sectores o participar conjuntamente en sus objetivos.

El artículo 101 de la Ley 34/1998, de 7 de octubre, otorga al Gobierno la facultad de utilizar las reservas estratégicas de gas natural en situaciones de emergencia. El gobierno también puede:

i. Limitar o modificar temporalmente el mercado del gas.
ii. Establecer obligaciones especiales en materia de existencias mínimas de seguridad de gas natural.
iii. Suspender o modificar temporalmente los derechos de acceso.
iv. Modificar las condiciones generales de regularidad en el suministro con carácter general o referido a determinadas categorías de consumidores.
v. Someter a autorización administrativa las ventas de gas natural para su consumo en el exterior.
vi. Cualesquiera otras medidas, que puedan ser recomendadas por los Organismos internacionales, de los que España sea parte o que se determinen en aplicación de aquellos convenios en que se participe.

Sin perjuicio de lo anterior, el Reglamento (UE) 2017/1938 establece la gobernanza a seguir en situaciones de escasez de gas natural. En este sentido, se pueden destacar tres documentos:

i. Documento nacional de evaluación de riesgos: analiza los riesgos que afectan a la seguridad del suministro de gas natural en España.
ii. Plan de acción preventivo, que establece las medidas necesarias para eliminar o mitigar los riesgos identificados en la evaluación nacional.
iii. Plan de emergencia, que establece las medidas para eliminar o mitigar los impactos de una interrupción del suministro.

Estos documentos establecen un marco como el de este PPR en el sector del gas.

6.5 Análisis e informe: lección aprendida.

Después de cada crisis, se realizará análisis ex-post del evento y sus consecuencias. Estos documentos incluirán propuestas y recomendaciones de mejora.

Los agentes o partes que redactarán estos documentos podrán incluir:

i. La Autoridad Competente, que realizará un análisis de la situación. Si esto no es una solución factible porque el alcance es demasiado grande, se aplicará un enfoque más compartimentado. Para ello podrá solicitar la colaboración del TSO en la elaboración del informe de evaluación o delegar la misma en el mismo.

ii. El Coordinador de Crisis o los órganos de coordinación que el gobierno active durante la crisis podrán proporcionar una visión de las acciones globales aplicadas durante la crisis, incluidas aquellas que quedan fuera de las cuestiones energéticas, y que incluyen a los ciudadanos vulnerables, la seguridad social, la ayuda a quienes han sufrido daños o pérdidas provocadas por la crisis, etc.

   El Coordinador de Crisis también podrá analizará esquemas que pueden servir como preventivos para otros impactos asociados a una crisis eléctrica, pero que no están directa e inmediatamente relacionados con la energía.

iii. El TSO podrá realizar un análisis centrado en el sector eléctrico y en las acciones adoptadas en el mismo para afrontar la crisis eléctrica. Esto puede incluir contribuciones de los diferentes agentes del sistema que participaron directamente en la crisis o de aquellos que operaron en el sistema durante la crisis, pero no sufrieron sus consecuencias negativas.

   Esta última cuestión es relevante porque ayuda hacer que los procedimientos sean ágiles y eficaces, reduciendo impactos negativos en la mayoría de los actores del sistema.

6.5.1 Evaluación ex post por parte de la Autoridad Competente.

En cumplimiento del artículo 17 del Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, la Autoridad Competente presentará un informe de evaluación ex post a la Comisión Europea y al ECG lo antes posible y, en cualquier caso, tres meses después del fin de una crisis de electricidad.

El Ministerio para la Transición Ecológica y el Reto Demográfico consultará a la Autoridad Reguladora Nacional, la Comisión Nacional de los Mercados y la Competencia (CNMC), antes de presentar el informe.

El informe ex post incluirá, al menos:

a) Una descripción del hecho que desencadenó la crisis eléctrica.
b) Una descripción de las medidas preventivas, preparatorias y mitigadoras adoptadas y una evaluación de su proporcionalidad y eficacia.
c) Una evaluación del impacto transfronterizo de las medidas adoptadas.
d) Un listado de las ayudas preparadas, con o sin activación efectiva, prestadas o recibidas de Estados miembros vecinos y terceros países.

e) El impacto económico de la crisis eléctrica y el impacto de las medidas adoptadas en el sector eléctrico en la medida permitida por los datos disponibles en el momento de la evaluación, en particular los volúmenes de energía no servida y el nivel de desconexión manual de la demanda (incluida una comparación entre el nivel de desconexión de la demanda voluntaria y forzada).
f) Razones que justifiquen la aplicación de cualquier medida no basada en el mercado.
g) Cualquier posible mejora o propuesta de mejora del PPR.
h) Una visión general de las posibles mejoras en el desarrollo de la red en los casos en que un desarrollo insuficiente de la red haya causado o contribuido a la crisis eléctrica.

El Ministerio para la Transición Ecológica y el Reto Demográfico podrá facilitar información adicional que ayude a comprender la evaluación. Además, el Ministerio responderá a cualquier solicitud específica del ECG y de la Comisión para proporcionar información adicional.

Finalmente, como autoridad competente, los representantes del Ministerio presentarán los resultados de la evaluación ex post en una reunión del ECG.

Cualquier crisis eléctrica lleva a una revisión del propio PPR. Como parte de esta revisión, los resultados del informe de evaluación ex post aparecerán en el PPR actualizado.

7. Procedimientos y acciones.

Los escenarios de Crisis de Electricidad Nacionales contempladas para el Plan Nacional de preparación son los que se han identificado en el Capítulo 3 y se resumen a continuación:

I. Pandemia

II. Tormenta extrema

III. Ciberataque a los Sistemas de Control

IV. Ciberataque a equipos críticos de control, protecciones y telecomunicaciones

V. Ataque físico a Centro Control

VI. Ataque físico a activos críticos

VII. Incendio o explosión en un activo crítico

VIII. Sabotaje por parte de personal interno

IX. Incendio forestal

X. Erupción volcánica

En este capítulo, el Plan proporciona una descripción esquemática de los diferentes escenarios que servirá como referencia para los diferentes agentes sobre qué esperar de cada situación. Dado que la mayoría de los interesados, si no todos, están familiarizados y conocen en detalle las diferentes acciones, medidas y respuestas en las que participan, estas representaciones esquemáticas proporcionarán una valiosa y sencilla lectura.

Esta descripción incluye referencias a planes, procedimientos y acciones específicos para cada uno de los escenarios utilizando la siguiente estructura:

I. Desencadenante de la crisis:

a. Detección del del desencadenante/inicio de la crisis.

b. Agentes involucrados.

II. Prevención y preparación:

a. A nivel nacional.

b. A nivel regional o bilateral.

III. Descripción de las medidas correctivas que se pueden adoptar:

Estas son medidas que no se aplican en todos y cada uno de los casos. Cada una de las acciones se llevará a cabo solo si las circunstancias concretas de la crisis lo requieren:

a. A nivel nacional.

b. A nivel regional o bilateral.

IV. Impacto.

V. Evaluación posterior y acciones de mejora.

Considerando el capítulo anterior, el procedimiento general que aplicarán todos los agentes contiene las siguientes fases:

1) Preparación del sistema, que es una fase continua que se llevará a cabo independientemente de que exista o no una crisis eléctrica real. El objetivo de esta fase es desarrollar un sistema energético que sea lo más resiliente y flexible, que facilite las acciones para prevenir y afrontar incidentes que pueden dar paso, y, de hecho, a crisis de electricidad.
   La preparación del sistema incluye sistemas de detección (como los descritos en el punto 5.1 del Plan PPR). Estos sistemas crearán conciencia sobre amenazas potenciales y sobre el desencadenante de una crisis eléctrica.

2) Declaración de alertas tempranas. Los primeros instrumentos de coordinación comienzan a funcionar tanto a nivel nacional como a nivel de la UE.
   a. El Gobierno de España alerta a sus países vecinos, incluidos Estados miembros y terceros países, así como a la Comisión de la UE.
   b. El Grupo de Coordinación Eléctrica (ECG) alerta a otros Estados miembros, incluidos los de la misma región que España.
   c. ENTSO-E y ENTSOG reciben y proporcionan información a los diferentes TSO en una misma región.

3) Dar seguimiento a la situación para ver si evoluciona hacia una crisis o no. El TSO analizará los potenciales impactos, con toda la información de que pueda disponer, y el Ministerio para la Transición Ecológica y el Reto Demográfico analizará la evolución de las amenazas al suministro energético.
   Según evolucione la situación, el Ministerio actualizará el estado e informará de tres posibles resultados:
   a. La situación y los riesgos se mantienen en su estado actual: el nivel de alerta se mantiene.
   b. La situación mejora y el riesgo disminuye: el nivel de alerta disminuye.
   c. La situación empeora y el riesgo aumenta: aumenta el nivel de alerta y, si es necesario, el gobierno declara una crisis eléctrica.

   Mientras esto ocurre, el TSO actualizará sus análisis de situación, activando las diferentes acciones preventivas y de preparación en caso de que acabe produciéndose una crisis.
   Lo mismo se aplica al resto de agentes del sistema y de la administración pública.

4) Declaración de crisis por parte de la Autoridad Competente.

5) Si las circunstancias así lo requieren, delegación de rol y/o funciones del Coordinador de Crisis.

6) La respuesta en el sector eléctrico podrá incluir, en términos genéricos, alguna de las siguientes actuaciones:
   a. Establecer contacto e interacción continuos con Operador del Sistema eléctrico.
   b. Reuniones con distintos ministerios, administraciones y órganos de coordinación para establecer las medidas relacionadas con el plan de ciberseguridad, infraestructuras críticas, catástrofes, sector eléctrico, etc.

c. Comunicación a las partes interesadas.
d. Comunicación a la Comisión y a los Estados miembros.
e. Adopción de todas las medidas necesarias, incluidas todas aquellas que se resumen para las distintas crisis en sus cuadros en los distintos apartados de este capítulo.

Finalmente, si una crisis es el resultado de una catástrofe o accidentes, las autoridades también podrán adoptar una serie de acciones fuera del sector eléctrico que incluyen:

1) Activación de los Servicios de Emergencia y Seguridad Pública: son las medidas adoptadas para atender adecuadamente el incidente, así como el rescate y salvamento de las víctimas.
2) Activación de Servicios de Salud: buscan asegurar la recepción en establecimientos médicos de las víctimas; incluyen primeros auxilios, clasificación de los heridos y traslado a centros hospitalarios adecuados.
3) Activación de Servicios Sociales: estas medidas buscan proporcionar socorro y asistencia a las víctimas y su posible traslado a centros de acogida.
4) Activación de Servicios de Seguridad: estas medidas podrán incluir el cercamiento de la zona afectada; el control y organización de accesos y salidas; mantenimiento del orden y la seguridad interior; vigilancia y gestión del tráfico; la evacuación de personas, víctimas en peligro o incluso bienes.
5) Activación de Servicios Técnicos: estas medidas buscarán garantizar la mejor operatividad de las actuaciones y la rehabilitación inmediata de los servicios públicos esenciales.

Durante la crisis, las distintas autoridades mantendrán un análisis continuo de su impacto y su evolución. Esto requerirá comunicación e interacción constante con el TSO de electricidad.

Por último, una vez finalizada la crisis, la Autoridad Competente notificará a las diferentes partes interesadas que se ha resuelto y se iniciará una evaluación ex post de ésta. Esta evaluación busca extraer lecciones relevantes de la experiencia adquirida y acciones de mejora para futuras crisis, en caso de que alguna vez se produzcan.

7.1 Escenario de pandemia.

Una pandemia es epidemia que se ha extendido por varios países, continentes o todo el mundo y que, generalmente, afecta a un gran número de personas[70]. Las pandemias son internacionales por naturaleza. Evolucionan a partir de brotes infecciosos cuando la enfermedad se descontrola y no permanece en una zona concreta.

Desencadenante/suceso inicial:

El escenario se iniciaría con la propagación internacional de una enfermedad. El personal operativo de TSO podría estar infectado. Podrían producirse infecciones, entre otros, en las plantillas de personal de las centrales eléctricas, instalaciones de transporte y distribución de energía eléctrica, centros de control, etc., lo que podría provocar una falta de personal.

Brote de una enfermedad contagiosa (potencial primera etapa de una pandemia)

El desencadenante de una pandemia serán los primeros casos declarados de una enfermedad infecciosa:

a) En territorio nacional. El Ministerio de Sanidad recibe su información de las distintas Autoridades Sanitarias de cada una de las Comunidades Autónomas[71].
b) En suelo extranjero[72]. El gobierno español puede recibir información relativa al brote[73]:
    a. Directamente de las autoridades del país donde aparecen los primeros casos.
    b. Indirectamente de cualquiera de los organismos internacionales a los que pertenece, entre las que se encuentra la Organización Mundial de la Salud (OMS).

Estas dos situaciones requieren diferentes acciones de seguimiento.

Cuando aparezcan los primeros casos en suelo nacional, la primera actuación del Ministerio de Sanidad (y resto de Autoridades Sanitarias) será evaluar el brote infeccioso, considerando:

a) Cuál es la enfermedad infecciosa.
b) Cómo de contagiosa es, considerando:
    a. Velocidad de contagio (días en que la enfermedad se manifiesta considerando el momento en que el paciente estuvo expuesto por primera vez a la enfermedad).
    b. Virulencia de la enfermedad (número de personas que un solo paciente puede infectar).
c) Para analizar esto, el ministerio podrá utilizar datos históricos si están disponibles. Si no hay datos disponibles, se utilizarán las mejores estimaciones proporcionadas por los expertos en salud.
d) ¿Existe cura o qué otras medidas paliativas se pueden aplicar a las personas infectadas?

---

[70] Según el documento "Covid-19 Glosario sobre brotes y epidemias: Un recurso para periodistas" de Organización Panamericana de la Salud la afiliada a la Organización Mundial de la Salud (OMS).
[71] A través del Centro de Coordinación de Alertas y Emergencias Sanitarias. Art. 4.8.b) del Real Decreto 735/2020, de 4 de agosto.
[72] A través de los órganos y unidades establecidos entre otros en los art. 3.1.e), 4.6, 4.7.a), c) y j) del Real Decreto 735/2020, de 4 de agosto.
[73] La coordinación internacional se encuentra habilitada en el art. 39.1.a) y b) de la Ley 33/2011, de 4 de octubre, de Salud Pública.

El Gobierno español notificará a sus países vecinos y a las instituciones internacionales a las que pertenece que hay un brote[74].

Cuando los primeros casos aparezcan en suelo extranjero, la primera actuación del Ministerio de Sanidad (y del resto de Autoridades Sanitarias) será valorar el brote a partir de la información proporcionada por el país vecino o las instituciones internacionales.

El gobierno se preparará[75] para el brote y su evolución:

i. Informando directamente de que existe un brote a todas las autoridades sanitarias, hospitales, unidades de primera atención y respuesta, etc., que puedan verse implicadas.
ii. Revisando protocolos de tratamiento, incluidos los equipos de primera respuesta, cuidados intensivos, etc.
iii. Revisando el stock de suministros médicos disponibles, incluidos los insumos de profilaxis sanitaria utilizados para higiene general, aislamiento, sacrificio, destrucción de material virulento.
iv. Revisando el stock de vacunas disponible.

Del brote a la epidemia y a la pandemia

Un brote se produce cuando hay es dos o más casos asociados epidemiológicamente entre sí. La existencia de un caso único bajo vigilancia en una zona donde no existía el padecimiento se considera también un brote. Un brote sucede por el aumento inusual del número de casos de una enfermedad más allá de lo normal. puede tener una diseminación localizada en un espacio específico (por ejemplo, una comunidad, un pueblo, un barco, una institución cerrada) o extenderse a varios países. Puede durar unos días, varias semanas o varios años.[76]

Los brotes de enfermedades infecciosas no son necesariamente la primera etapa de una epidemia ni de una pandemia. Un brote no evolucionará necesariamente hacia una epidemia o una pandemia, siempre que se pueda contener.

Una epidemia es un aumento inusual del número de casos de una enfermedad determinada en una población específica, en un período determinado. Los términos “brote” y “epidemia” se usan a menudo indistintamente. En general, una epidemia puede ser considerada como la consolidación simultánea de múltiples brotes en una amplia zona geográfica y, generalmente, implica la ocurrencia de un gran número de casos nuevos en poco tiempo, mayor al número esperado[77]).

Finalmente, una pandemia cumple dos condiciones:

---

[74] La Orden SCO/564/2004, de 27 de febrero, por la que se establece el sistema de coordinación de alertas y emergencias de Sanidad y Consumo establece en la letra d) de su art. Primero.3 que el SICAS del Ministerio de Salud Servir de apoyo al plan de respuesta de salud pública para alertas por riesgos extraordinarios biológicos, químicos, alimentarios, radiológicos y nucleares del Sistema Nacional de Salud, así como a las Administraciones y organismos nacionales, autonómicos, comunitarios o internacionales competentes en la gestión de situaciones de crisis y catástrofes.

[75] Como parte de los planteamientos estratégicos especificados en las letras a) y d) del art. 3 de la Orden SCO/564/2004, de 27 de febrero.

[76] Según el documento “Covid-19 Glosario sobre brotes y epidemias: Un recurso para periodistas” de Organización Panamericana de la Salud la afiliada a la Organización Mundial de la Salud (OMS).

[77] Según el documento “Covid-19 Glosario sobre brotes y epidemias: Un recurso para periodistas” de Organización Panamericana de la Salud la afiliada a la Organización Mundial de la Salud (OMS).

i. Que la enfermedad afecte a más de un país, e incluso a más de un continente.
ii. Que los casos de cada país ya no sean importados sino transmitidos a través de la comunidad.

La cuestión de cuán contagiosa es una enfermedad puede no estar clara desde el principio, ya que las mutaciones en el patógeno introducen variaciones con respecto a brotes anteriores. Considerando esto, el gobierno activará medidas de contención con los siguientes objetivos:

i. Aislar el brote.
ii. Prevenir la propagación de la enfermedad.
iii. Frenar la propagación de la enfermedad.

El gobierno revisará continuamente estas medidas para responder mejor a la situación.

Finalmente, la Organización Mundial de la Salud (OMS) es la institución que declara oficialmente una pandemia cuando más de un continente sufre la enfermedad y hay transmisión comunitaria dentro de los países. Sin embargo, antes de esta declaración, los países se habían preparado para la enfermedad y habían actuado antes de esta declaración formal y, en cooperación con la OMS, habían trabajado para planificar, preparar y responder de manera coordinada.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias están cumplido, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

Para que una pandemia sea considerada una crisis eléctrica, no es esencial alcanzar un número determinado de casos confirmados, ni siquiera dentro del propio sector eléctrico. La situación se convierte en crisis cuando el sistema no puede dar una respuesta adecuada a las diferentes circunstancias y funcionar adecuadamente.

La falta de personal en el sistema eléctrico puede suponer una reducción importante de la mano de obra disponible. Esto podría tener un efecto en cascada sobre los proveedores y contratistas, así como sobre los consumidores intermedios. Si el número de casos confirmados en el sistema eléctrico es lo suficientemente grande, la crisis será más relevante y de mucho mayor alcance. Esto es más relevante cuando le sucede al personal de TSO y DSO y/o a los empleados de los centros de control del sistema.

Las acciones preventivas son fundamentales, y la batería de medidas posibles incluye que:

- Los agentes podrían preparar y aislar al personal, estableciendo diferentes equipos de trabajo (principal y reserva) para cada turno. Estos equipos deberán estar aislados entre sí y deberán tomar medidas sanitarias extraordinarias para evitar contagios y someterse a controles adicionales.
- Si es posible, diferentes equipos trabajarían en diferentes lugares.
- Los agentes deben aumentar las medidas de limpieza y desinfección en todos los lugares donde haya personal presente.

- El almacenamiento de reservas de combustible a nivel nacional puede convertirse en una prioridad.
- El almacenamiento de reservas de combustible en cada instalación individual puede convertirse en un factor decisivo, contribuyendo a reducir la necesidad de suministro externo a muy corto plazo[78].
- El sistema de transporte debe estar preparado para abastecer las instalaciones desde las zonas de reserva del país a cada planta de generación que lo requiera.

Otras Consideraciones.

Los impactos que previsiblemente pueden producirse por este tipo de crisis son esencialmente dos:

- Hay menos personal de mantenimiento que pueden resolver incidencias.
- Incrementan la probabilidad de crisis de electricidad por retrasos en la resolución de una incidencia en un elemento crítico de la red (por falta de personal) y que derive en un fallo múltiple.

Al considerar los impactos transfronterizos de este tipo de crisis, lo más probable es que otros Estados miembros (incluidos aquellos de la región en la que se incluye España) se encuentren en una situación idéntica o muy similar.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando los TSO vecinos pueden brindar apoyo.

Así, se pueden tomar algunas de las siguientes acciones:

- Realizar intercambios de apoyo de energía activa con TSO vecinos.
- Aplicar los procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar los procedimientos de soporte de los sistemas español y portugués tras incidencias.

Como referencias más recientes de este tipo de crisis se pueden citar la Gripe A de 2009 y más recientemente la Covid-19.

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
Comunicación a través de organismos oficiales, que como se indicaba anteriormente, incluyen el Ministerio de Sanidad[79].
Agentes implicados

[78] El P.O. 9: «Información intercambiada por el operador del sistema» establece esto como parte del contenido de la base de datos de información que debe tener el Operador del Sistema de las Unidades térmicas de régimen ordinario en su Anexo I en el punto 8 correspondiente a estas instalaciones.

[79] Ente otros a través de la Centro de Coordinación de Alertas y Emergencias Sanitarias – Art. Cuarto, de la Orden SCO/564/2004, de 27 de febrero.

Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSOs), Empresas de generación, Organismos oficiales.

II. PREVENCIÓN Y PREPARACIÓN

Medidas preventivas a nivel nacional

En una crisis en la que la movilidad puede verse gravemente limitada, la preparación debe abordar al menos tres vías de acción clave:

- Preparación del TSO.
- Informar al TSO sobre las reservas de combustible disponibles para la generación de electricidad.
- Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Preparar y aislar al personal.
- Aislamiento de los Centros de Control: reorganización de turnos evitando el contacto entre los diferentes Centros de Control y entre los diferentes turnos.
- Limitar la presencia física del personal.
- Aumentar las medidas de limpieza y desinfección.
- Dar la necesaria priorización a las tareas de operación y de los trabajos en campo.
- Fortalecer la coordinación entre los diferentes agentes: estableciendo diferentes escenarios y, en función de estos, llevar a cabo una reasignación de tareas.
- Reunir material de emergencia y víveres en los centros de control.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Las acciones que se pueden tomar durante la crisis incluyen las siguientes. La adopción de estas acciones dependerá de las características específicas de la crisis y de los impactos que pueda tener en los sistemas eléctricos.

a) Medidas relacionadas con la operación del sistema:

- En función de la crisis de suministro eléctrico que se pueda producir, el Operador del Sistema llevará a cabo las medidas incluidas en los Procedimientos de Operación para los distintos estados de emergencia del sistema (alerta, emergencia, reposición).
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Movilización de reservas disponibles de fuentes de energía para la generación de electricidad en caso de estado de alerta/emergencia del sistema. El uso para generación eléctrica se hará sin perjuicio de otros usos regulados de estas reservas (reservas de agua y gas natural para usos distintos al eléctrico, como

abastecimiento de agua e industria) y quedando bajo el criterio del operador del sistema y supervisión de las autoridades.

b) Otras medidas:

La aplicación del protocolo de actuación recoge diferentes escenarios ante imposibilidad o limitación de movilidad, donde se contemplan: organización de turnos, alojamientos, suministros e instalaciones.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimiento de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimiento de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.2 Escenario de tormenta extrema.

Desencadenante/suceso inicial:

Las tormentas son fenómenos meteorológicos naturales. Considerando el área geográfica de España y la Península Ibérica, no se pueden descartar impactos a nivel regional.

El desencadenante en este tipo de crisis del sector eléctrico puede ser un fuerte temporal de viento, o cualquier tipo de tormenta, incluidas las de nieve. Como tal, es previsible que este evento pueda dar lugar a una pérdida significativa de suministro y que se caracteriza por una caída de apoyos, afectando a otros elementos del sistema eléctrico.

Antes de la tormenta (potencial primera etapa de un evento climático extremo).

AEMET analiza la información meteorológica de la que dispone. Si hay potencial tormenta, emitirá un aviso que llegará no sólo a los agentes eléctricos sino también a la ciudadanía[80].

Una vez que AEMET haya emitido un aviso de posible mal tiempo, los equipos de seguridad de todas las instalaciones afectadas podrían realizar alguna de las siguientes actuaciones si las circunstancias así lo requieren:

- Acoplamiento de líneas para aumentar el mallado de red y evitar la formación de manguitos de hielo en líneas desacopladas.
- Valorar la devolución de descargos y la reposición de elementos.
- Realizar una gestión de la generación existente (Acoplar grupos, gestión de indisponibilidades de grupos).
- Implementar la anulación reenganches, desplazamiento personal para identificación de líneas afectadas y apertura líneas.

Además, se hace necesaria la preactivación de diferentes recursos para gestionar la crisis una vez materializada: personal de campo, grupos electrógenos, medios de grupos de repostaje, medios especiales de acceso como quads, helicópteros, etc.

Esto adquiere especial relevancia en el caso de los servicios de limpieza de vías de las Comunidades Autónomas[81] y municipios[82] en el ámbito de sus respectivas competencias, así como para la UME[83] y el Sistema de Seguridad Nacional[84].

También hay que considerar el posible impacto en el sistema de telecomunicaciones provocado por la pérdida de suministro de antenas y repetidores durante un largo periodo para proceder a la planificación de la instalación de grupos electrógenos, así como a su repostaje.

La AEMET deberá revisar continuamente sus predicciones meteorológicas[85] y hacer un seguimiento de la evolución de las condiciones meteorológicas, actualizando el nivel de alerta según sea necesario[86].

---

[80] Art. 8, letra a) del Estatuto de la Agencia Estatal de Meteorología, aprobado por el Real Decreto 186/2008, de 8 de febrero

[81] Recogidas en sus respectivos estatutos de autonomía.

[82] Art. 26 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

[83] Art. Tercero.1.a) del Protocolo de Intervención de la Unidad Militar de Emergencias.

[84] Título II de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

[85] Art. 8, letras o) y f) del Estatuto de la Agencia Estatal de Meteorología.

[86] Art. 8, letra a) del Estatuto de la Agencia Estatal de Meteorología.

En esta situación conviene asegurar previamente la disponibilidad de combustible para los grupos electrógenos, así como su traslado a los puntos de consumo.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) y los criterios de seguridad ante contingencias se encuentran dentro de los márgenes normales de operación, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

La debilidad en el sistema puede aparecer por cualquiera de las siguientes razones:

- Daños físicos u operativos en elementos del sistema eléctrico.
- Que se produzcan cortes de mercado.
- Por daños en los cables de fibra óptica.
- Que se produzca una pérdida de control remoto en el funcionamiento del sistema eléctrico.

Con la posible excepción de los cortes de mercado, estas situaciones probablemente se producirían sólo si la tormenta fuera tan grande que se acumulara una gran cantidad de nieve, bloqueando las carreteras. Esto dificultaría o impediría que el personal del sector eléctrico se desplazara a sus lugares de trabajo o que los camiones de suministro de combustible llegaran a las plantas de generación.

Incluso si la tormenta es un evento mayor, los Servicios de Emergencia cuentan con flotas de vehículos para el mantenimiento de carreteras y calles, incluidos quitanieves y vehículos auxiliares.

Otras Consideraciones.

En este escenario de crisis, es probable que la acumulación de nieve dificulte el acceso para reparar las infraestructuras y equipos dañados. La caída de árboles en caminos y pistas forestales también puede dificultar el acceso a las instalaciones. Las lluvias torrenciales también pueden causar graves daños a la red de carreteras y provocar deslizamientos de tierra.

Los impactos que previsiblemente se pueden dar como consecuencia de este tipo de crisis son fundamentalmente:

- Daños físicos u operativos en elementos del sistema eléctrico.
- Que tengan lugar cortes de suministro locales.
- Que se produzcan afectaciones en los cables de fibra óptica.
- Que se produzca una pérdida de telemando en la operación del sistema eléctrico.
- Que se produzca una pérdida del control remoto en la operación de algunas subestaciones del sistema eléctrico, que es un evento localizado.
- Que tenga lugar la pérdida de comunicaciones de voz y datos a través de señal móvil que podría afectar al personal de campo y a la comunicación de los Centros de Control con los equipos de trabajo.
- Que sea imposible sustituir turnos de operación.

En lo que se refiere al impacto transfronterizo de este tipo de crisis, se considera previsible que el temporal también pueda afectar a países de la zona Oeste de Europa. En este sentido se asumen posibles pérdidas de líneas de interconexión y, por tanto, una potencial reducción de capacidad de intercambio con Francia y Portugal.

Para evitar impactos transfronterizos, el TSO evaluará si es necesaria la adaptación de los programas de intercambio con los Estados miembros vecinos, así como con países terceros vecinos. La necesidad de adaptar o no los programas de intercambio dependerá de cada situación.

Así, podrán adoptarse algunas de las siguientes actuaciones si las circunstancias lo requieren:

- Llevar a cabo intercambios de apoyo de energía activa con los TSO vecinos.
- Aplicar los procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar los procedimientos de soporte de los sistemas español y portugués tras incidencias.

Como referencias más recientes de este tipo de crisis se pueden citar el Ciclón Klaus (2009), el Temporal Gloria (2020) y Filomena (2021).

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS
Detección Inicio Crisis
Información o alertas meteorológicas (AEMET)[87].
Agentes implicados
Se han identificado los siguientes agentes que pueden estar implicados: Red Eléctrica de España, S.A.U., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Organismos oficiales (Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC, Ministerios, Unidad Militar de Emergencias (UME).
II. PREVENCIÓN Y PREPARACIÓN
Medidas preventivas a nivel nacional
En una crisis de esta naturaleza, la preparación debe abordar al menos cuatro líneas de actuación clave: • Alertas meteorológicas en caso de fenómenos meteorológicos adversos. • Preparación del TSO. • Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad. • Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

[87] Art. 8 del Estatuto de la Agencia Estatal de Meteorología.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Acoplamiento de líneas para aumentar el mallado de red y evitar la formación de manguitos de hielo en líneas desacopladas.
- Valorar la devolución de descargos y la reposición de elementos.
- Realizar una gestión de la reserva de generación existente (acoplar grupos, gestión de indisponibilidades de grupos).
- Implementar la anulación reenganches, desplazamiento personal para identificación de líneas afectadas y apertura líneas.
- Activación previa de los recursos necesarios para gestionar la crisis (personal de campo, grupos electrógenos, medios de grupos de repostaje, medios de acceso especiales como motos de nieve, helicópteros, etc.).
- Analizar los posibles impactos en el sistema de telecomunicaciones provocados por la pérdida de suministro de antenas y repetidores durante un largo periodo para proceder a la planificación de la instalación de grupos electrógenos, así como a su repostaje).
- Garantizar la disponibilidad de combustible para los grupos electrógenos, así como su traslado a los puntos de consumo.

Medidas preventivas a nivel regional

Llevar a cabo la adaptación de los programas de intercambio con los Estado Miembros vecinos, así como con países terceros vecinos.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático de control de sobrefrecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- La aplicación del protocolo de actuación recoge diferentes escenarios ante imposibilidad o limitación de movilidad, donde se contemplan: organización de turnos, alojamientos, suministros e instalaciones.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimiento de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimiento de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.3 Escenario de ciberataque a los sistemas de control.

Desencadenante/suceso inicial:

Los ciberataques son incidentes intencionados. Teniendo en cuenta su gravedad y objetivos, no sólo no se pueden descartar impactos marcados a nivel regional, sino que su impacto transfronterizo es ciertamente plausible.

En este escenario, el suceso inicial de este tipo de crisis en el sector eléctrico es un ciberataque a equipos críticos de control, protecciones y telecomunicaciones. Este ataque se manifestaría en una denegación de servicio, en intentos de acceso ilegal o en la manipulación de la información utilizada por los sistemas de control. En última instancia, esto provocaría problemas en el funcionamiento del sistema.

Antes del ciberataque.

Al igual que en el escenario anterior, una serie de acciones permiten al sistema prepararse frente a ciberataques. Cuanto más integrales y exhaustivas sean estas acciones, mejor preparado estará el sistema y mejor será la respuesta.

La planificación ocupa el primer lugar en la respuesta a los ciberataques. Una planificación adecuada es fundamental y el personal debe actualizar sus conocimientos sobre temas de ciberseguridad, amenazas y comportamientos adecuados para evitar que las amenazas se materialicen en ciberataques.

Estas acciones incluyen también un análisis continuo de los riesgos potenciales, dando seguimiento a la actividad de ciberataques en el país y en otros países. INCIBE[88] y la OCC[89] proporcionarán información útil y actualizaciones en el menor tiempo posible.

Los principales incidentes que han afectado a infraestructuras críticas se encuadran en las siguientes categorías:

i. Sistemas vulnerables.
ii. Malware, que incluye los malware Emotet, Mekotio, Flubot, Anatsa y Hive.
iii. Robo de información.
iv. Fraude, que incluye robo de identidad (fraude de CEO) y phishing.

Considerando esto, el personal de ciberseguridad de los Sistemas de Control deberá:

- Realizar la monitorización de accesos y de sistemas.
- Definir y revisar los diferentes niveles de aislamiento de las redes IT/OT de los agentes implicados en una amenaza de ciberataque.
- Desarrollo seguro de aplicaciones operativas.
- Llevar a cabo la implantación de medidas y controles anti-intrusión.
- Controlar de accesos de personas y vehículos (incluye autenticación) a las diferentes instalaciones, evitando intrusiones contra ataques in situ.
- Realizar la instalación y configuración segura, protección frente a malware.
- Aplicar y revisar la gestión de privilegios.

[88] Proporciona los avisos e informes periódicos en su página de Internet https://www.incibe.es/incibe-cert

[89] Art. 4.4 del Real Decreto 43/2021, de 26 de enero.

Los usuarios finales son casi siempre el objetivo directo de los ciberataques, ya que tienen menos preparación que el personal de TIC y se convierten más fácilmente en puntos de entrada de facto a los servidores.

- La mejor forma de prepararse es la formación interna continua a todo el personal, y en especial a todos aquellos con responsabilidades en la toma de decisiones. Cuando los empleados saben que ciertos comportamientos y acciones entrañan riesgos, es más probable que los eviten.
- Los equipos de todos los servicios TIC deben preparar servicios e infraestructuras TIC para ciberataques. Su formación es una acción crucial en materia de ciberseguridad.

Otros agentes tendrán que llevar a cabo otras respuestas relevantes. Los operadores deberán prepararse para una serie de acciones que incluyen:

- Disponer y operar elementos de respaldo. Esto no sólo abarca tener físicamente activos que sirvan como respaldo, sino también activarlos (mantenerlos en stand-by si es necesario) y activar equipos de trabajo y personal de respaldo para operar estos elementos de respaldo.
  Es fundamental que estos elementos de respaldo estén tanto online como offline. De esta manera, la operación puede continuar incluso en las condiciones más catastróficas del ciberataque.
- En el peor de los casos, los centros de control dejarán de funcionar o quedarán bajo el control de los atacantes. En este caso, la respuesta requerirá aislar el centro de control u operación afectado y un centro alternativo deberá asumir las actuaciones que estaba llevando a cabo antes del ataque. El personal de los centros de operaciones redundantes deberá estar en alerta, listo para comenzar a trabajar cuando sea necesario.
- En el caso de centros redundantes, estos deberán disponer de capas de seguridad redundantes o garantizar que los ciberataques no puedan llegar a ellos al mismo tiempo que a los centros de control principales, manteniendo los equipos apagados o aislados de la red externa.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias están cumplido, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

Una vez producido el ciberataque, la diferente decisión y operación activará una serie de respuestas. Estos incluyen desde la revisión de privilegios de acceso hasta el traspaso de la operación activa del sistema a los Centros de Control u Operación secundarios o redundantes, los cuales contarán con un equipo de trabajo independiente.

Fuera del sector eléctrico, las autoridades procederán a la Declaración de Aplicabilidad.

Una vez producido el ciberataque se activará la comunicación entre el centro de control, el OCC y el Centro de Respuesta a Incidentes de Seguridad para ciudadanos y empresas (INCIBE-CERT)[90].

Estas mismas entidades aplicarán el Plan de Continuidad en caso de indisponibilidad de activos tecnológicos.

Otras Consideraciones.

Los impactos que se pueden presentar a causa de este tipo de crisis son fundamentalmente que:

- Se produzcan múltiples disparos de posición simultáneos en varias subestaciones críticas.
- Se produzcan disparos no planificados o previstos en las unidades de generación.
- Exista una pérdida operativa en el mercado eléctrico.
- Que resulte imposible operar los activos desde el Centro de Control afectado.
- Que se produzca un apagón parcial o total.

Sobre los impactos transfronterizos de este tipo de crisis, es probable que un ciberataque a los Centros de Control pueda afectar también a nuestros países vecinos. Este impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión si se tratara de activos afectados.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando los TSO vecinos pueden brindar apoyo. Así, se pueden tomar algunas de las siguientes acciones:

- Realizar intercambios de apoyo de energía activa con TSO vecinos.
- Aplicar los procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar los procedimientos de soporte de los sistemas español y portugués tras incidencias.

La referencia más reciente a este tipo de crisis es el ciberataque a la red eléctrica de Ucrania (2015).

Las principales características de este escenario de crisis y las acciones a tomar ante él se muestran a continuación:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
Agentes que pueden detectar el suceso inicial: • La Oficina de Coordinación de Ciberseguridad (OCC) a través de la declaración del nivel máximo de alerta[91]. • INCIBE-CERT[92]. • El Centros de Operaciones de Seguridad (SOC) de Red Eléctrica de España, S.A o el SOC de otros agentes (como los DSO) podrían detectar la crisis y comunicar e iniciar la coordinación mediante INCIBE-CERT.

[90] Art. 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.
[91] Art. 4.4 del Real Decreto 43/2021, de 26 de enero.
[92] Art. 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

Agentes implicados

Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales Centro Nacional Protección de Infraestructuras y Ciberseguridad (CNPIC), Instituto Nacional de Ciberseguridad (INCIBE), Oficina de Coordinación de Ciberseguridad (OCC), Ministerios.

II. PREVENCIÓN Y PREPARACIÓN

Medidas preventivas a nivel nacional

Las medidas que se pueden tomar antes de la crisis se incluyen:

- Ciberseguridad.
- Preparación del TSO.
- Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad.
- Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Realizar análisis de riesgos potenciales.
- Definir y revisar los diferentes niveles de aislamiento de las redes IT/OT de los agentes implicados en una amenaza de ciberataque.
- Establecer una planificación y aplicarla.
- Realizar un control de accesos y sistemas.
- Desarrollo seguro de aplicaciones operativas.
- Llevar a cabo la implementación de medidas y controles anti-intrusión.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Instalación y configuración seguras de protección contra malware.
- Aplicar y revisar la gestión de privilegios.
- Disponer de elementos de back up, tanto on-line como off-line.
- Tener un Centro de Control redundante en activo.
- Proporcionar formación adecuada del personal y actividades pedagógicas, para evitar vulnerabilidades y comportamientos de riesgo.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Proceder a la Declaración de Aplicabilidad (SoA)[93]. El SoA es un documento que incluye la lista completa de los controles de seguridad de la información evaluable amenazada por ciberataques.
  Una vez que la instalación/entidad realiza el análisis y evaluación de los ciber-riesgos, la organización debe definir las respuestas y las medidas de seguridad a tomar para mitigarlos. El SoA es el documento donde aparecen los controles de seguridad a aplicar.
- Comunicación con el OCC y con el Centro de Respuesta a Incidentes de Seguridad para ciudadanos y empresas, que pasa a denominarse INCIBE-CERT de referencia[94].
- Aplicación del Plan Continuidad ante indisponibilidad de activos tecnológicos.
- Para poder contener el ciberataque y permitir que el sistema siga funcionando, los operadores de servicios esenciales como los DSO han diseñado un conjunto de medidas de aislamiento que permiten reducir la exposición de la empresa para mantener los procesos críticos (operación de la red).

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.

[93] Norma ISO 27001, de Sistemas de Gestión de Seguridad de la Información (SGSI) y actualizaciones.
[94] Art. 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.4 Escenario de ciberataque a los equipos críticos de control, protecciones y telecomunicaciones

Desencadenante/suceso inicial:

Tal y como se menciona en el escenario anterior, los ciberataques son incidentes intencionados. Teniendo en cuenta su gravedad y objetivos, no sólo no se pueden descartar impactos marcados a nivel regional, sino que su impacto transfronterizo es ciertamente plausible.

En este escenario, el suceso inicial de este tipo de crisis en el sector eléctrico es un ciberataque a equipos críticos de control, protecciones y telecomunicaciones. Este ataque se manifestaría en una denegación de servicio, en intentos de acceso ilegal o en la manipulación de la información utilizada por los sistemas de control. En última instancia, esto provocaría problemas en el funcionamiento del sistema.

Antes del ciberataque.

Hay una serie de acciones permiten al sistema prepararse frente a ciberataques. Cuanto más integrales y exhaustivas sean estas actuaciones, mejor preparado estará el sistema y mejor será la respuesta.

La planificación ocupa el primer lugar en la respuesta a los ciberataques. Una planificación adecuada es fundamental y el personal debe actualizar sus conocimientos sobre temas de ciberseguridad, amenazas y comportamientos adecuados para evitar que las amenazas se materialicen en ciberataques.

Estas acciones incluyen también un análisis continuo de los riesgos potenciales, dando seguimiento a la actividad de ciberataques en el país y en otros países. INCIBE[95] y la OCC[96] proporcionarán información útil y actualizaciones en el menor tiempo posible.

Los principales incidentes que han afectado a infraestructuras críticas se encuadran en las siguientes categorías:

v. Sistemas vulnerables.
vi. Malware, que incluye los malware Emotet, Mekotio, Flubot, Anatsa y Hive.
vii. Robo de información.
viii. Fraude, que incluye robo de identidad (fraude de CEO) y phishing.

Considerando esto, el personal de ciberseguridad de los Sistemas de Control deberá:

- Realizar la monitorización de accesos y de sistemas.
- Definir y revisar los diferentes niveles de aislamiento de las redes IT/OT de los agentes implicados en una amenaza de ciberataque.
- Desarrollo seguro de aplicaciones operativas.
- Llevar a cabo la implantación de medidas y controles anti-intrusión.
- Controlar de accesos de personas y vehículos (incluye autenticación) a las diferentes instalaciones, evitando intrusiones contra ataques in situ.
- Realizar la instalación y configuración segura, protección frente a malware.

[95] Proporciona los avisos e informes periódicos en su página de Internet https://www.incibe.es/incibe-cert
[96] Art. 4.4 del Real Decreto 43/2021, de 26 de enero.

- Aplicar y revisar la gestión de privilegios.

Los usuarios finales son casi siempre el objetivo directo de los ciberataques.

- La mejor forma de prepararse es la formación interna continua a todo el personal, y en especial a todos aquellos con responsabilidades en la toma de decisiones. Cuando los empleados saben que ciertos comportamientos y acciones son riesgosos, es más probable que los eviten.
- Los equipos de todos los servicios TIC deben preparar servicios e infraestructuras TIC para ciberataques. Su formación es una acción crucial en ciberseguridad.

Otros agentes tendrán que llevar a cabo otras respuestas relevantes. Los operadores deberán prepararse para una serie de acciones que incluyen:

- Disponer y operar elementos de respaldo. Esto no sólo abarca tener físicamente activos que sirvan como respaldo, sino también activarlos (mantenerlos en stand-by si es necesario) y activar equipos de trabajo y personal de respaldo para operar estos elementos de respaldo.
  Es fundamental que estos elementos de respaldo estén tanto online como offline. De esta manera, la operación puede continuar incluso en las condiciones más catastróficas del ciberataque.
- En el peor de los casos, los centros de control dejarán de funcionar o quedarán bajo el control de los atacantes. En este caso, la respuesta requerirá aislar el centro de control u operación afectado y un centro alternativo deberá asumir las actuaciones que estaba llevando a cabo antes del ataque. El personal de los centros de operaciones redundantes deberá estar en alerta, listo para comenzar a trabajar cuando sea necesario.
- En el caso de centros redundantes, estos deberán disponer de capas de seguridad redundantes o garantizar que los ciberataques no puedan llegar a ellos al mismo tiempo que a los centros de control principales, manteniendo los equipos apagados o aislados de la red externa.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

Una vez producido el ciberataque, la diferente decisión y operación activará una serie de respuestas. Estos incluyen desde la revisión de privilegios de acceso hasta el traspaso de la operación activa del sistema a los Centros de Control u Operación secundarios o redundantes, los cuales contarán con un equipo de trabajo independiente.

Fuera del sector eléctrico, las autoridades procederán a la Declaración de Aplicabilidad.

Una vez producido el ciberataque se activará la comunicación entre el centro de control, el OCC y el Centro de Respuesta a Incidentes de Seguridad para ciudadanos y empresas (INCIBE-CERT)[97].

Estas mismas entidades aplicarán el Plan de Continuidad en caso de indisponibilidad de activos tecnológicos.

Otras Consideraciones.

Los impactos que se pueden presentar a causa de este tipo de crisis son fundamentalmente que:

- Se produzcan disparos de líneas eléctricas.
- Se produzcan disparos no planificados o previstos en las unidades de generación.
- Exista una pérdida operativa en el mercado eléctrico.
- Que resulte imposible operar los activos desde el Centro de Control afectado.
- Que se produzca un apagón parcial o total.

Sobre los impactos transfronterizos de este tipo de crisis, es probable que un ciberataque a equipos críticos de control, protecciones y telecomunicaciones pueda afectar también a nuestros países vecinos. Este impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión si se tratara de activos afectados.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando los TSO vecinos pueden brindar apoyo. Así, se pueden tomar algunas de las siguientes acciones:

- Realizar intercambios de apoyo de energía activa con TSO vecinos.
- Aplicar los procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar los procedimientos de soporte de los sistemas español y portugués tras incidencias.

La referencia más reciente a este tipo de crisis es el ciberataque a la red eléctrica de Ucrania (2015).

Las principales características de este escenario de crisis y las acciones a tomar ante él se muestran a continuación:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
Agentes que pueden detectar el suceso inicial: • La Oficina de Coordinación de Ciberseguridad (OCC) a través de la declaración del nivel máximo de alerta[98]. • INCIBE-CERT. • El Centros de Operaciones de Seguridad (SOC) de Red Eléctrica de España, S.A o el SOC de otros agentes (como los DSO) podrían detectar la crisis y comunicar e iniciar la coordinación mediante INCIBE-CRET.
Agentes implicados

[97] Art. 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.
[98] Art. 4.4 del Real Decreto 43/2021, de 26 de enero.

Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales Centro Nacional Protección de Infraestructuras y Ciberseguridad (CNPIC), Instituto Nacional de Ciberseguridad (INCIBE), Oficina de Coordinación de Ciberseguridad (OCC), Ministerios).

II. PREVENCIÓN Y PREPARACIÓN

Medidas preventivas a nivel nacional

Las medidas que se pueden tomar antes de la crisis se incluyen:

- Ciberseguridad.
- Preparación del TSO.
- Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad.
- Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Seguridad física y electrónica perimetral.
- Establecer y aplicar las medidas de Protección del puesto de trabajo.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Llevar a cabo registros de usuarios de los centros de control.
- Aplicar y revisar la gestión de privilegios.
- Definir y revisar los diferentes niveles de aislamiento de las redes IT/OT de los agentes implicados en una amenaza de ciberataque.
- Disponer de elementos de back up, tanto on-line como off-line.
- Tener un Centro de Control redundante en activo.
- Proporcionar formación adecuada del personal y actividades pedagógicas, para evitar vulnerabilidades y comportamientos de riesgo.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Proceder a la Declaración de Aplicabilidad (SoA)[99]. El SoA es un documento que incluye la lista completa de los controles de seguridad de la información evaluable amenazada por ciberataques.
  Una vez que la instalación/entidad realiza el análisis y evaluación de los ciber-riesgos, la organización debe definir las respuestas y las medidas de seguridad a tomar para mitigarlos. El SoA es el documento donde aparecen los controles de seguridad a aplicar.
- Comunicación con el OCC y con el Centro de Respuesta a Incidentes de Seguridad para ciudadanos y empresas pasa a denominarse INCIBE-CERT de referencia[100].
- Aplicación del Plan Continuidad ante indisponibilidad de activos tecnológicos.
- Para poder contener el ciberataque y permitir que el sistema siga funcionando, los operadores de servicios esenciales como los DSO han diseñado un conjunto de medidas de aislamiento que permiten reducir la exposición de la empresa para mantener los procesos críticos (operación de la red).

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.

[99] Norma ISO 27001, de Sistemas de Gestión de Seguridad de la Información (SGSI) y actualizaciones.
[100] Art. 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.5 Escenario de ataque físico al Centro de Control

Desencadenante/suceso inicial:

Los ataques físicos a instalaciones e infraestructura son incidentes intencionales. Considerando su gravedad y objetivos, no sólo no se pueden descartar impactos marcados a nivel regional, sino que también es bastante posible su impacto transfronterizo.

En este escenario, el hecho iniciador de este tipo de crisis en el sector eléctrico es un ataque físico a un Centro de Control Principal, a un Centro de Control de Respaldo o simultáneamente a centros de ambos tipos.

Antes del ataque físico.

Al igual que ocurre con los escenarios de ciberataque, hay una serie de acciones que preparan a los centros de control frente a ataques físicos. Cuanto más integrales y exhaustivas sean estas actuaciones, mejor preparado estará el sistema y mejor será la respuesta.

La planificación ocupa el primer lugar en la respuesta de seguridad. Una planificación adecuada es fundamental y el personal debe actualizar sus conocimientos sobre las amenazas y el comportamiento adecuado para evitar que los riesgos se materialicen en ataques dañinos.

Estas acciones incluyen también un análisis continuo de los riesgos potenciales, dándoles seguimiento tanto en el país como en otros países. Las diferentes fuerzas policiales, el CNPIC[101] e incluso el INCIBE[102] y la OCC[103] pueden proporcionar y proporcionarán información y actualizaciones útiles en el menor tiempo posible.

Considerando esto, los servicios de seguridad en los Sistemas de Control deben realizar las siguientes acciones:

- Realizar seguridad física y electrónica perimetral.
- Establecer y aplicar las medidas de Protección del puesto de trabajo.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Llevar a cabo registros de usuarios de los centros de control.

Si aparecen amenazas, el centro de control siempre puede solicitar ayuda a las fuerzas policiales. De este modo, la policía refuerza la seguridad y disminuye la probabilidad de un ataque físico. Se activa la coordinación entre los cuerpos policiales estatales o autonómicos y los servicios de seguridad del centro de control, actuando cada sujeto dentro de sus capacidades y trabajando juntos para evitar el potencial ataque.

Cuando exista amenaza, los interesados activarán Planes de Protección Específicos de los Centros de Control. El punto de contacto en el Ministerio del Interior es el CNPIC[104] y habrá comunicaciones con las Fuerzas de Seguridad del Estado (FCSE).

---

[101] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.
[102] Proporciona los avisos e informes periódicos en su página de Internet https://www.incibe.es/incibe-cert
[103] Art. 4.4 del Real Decreto 43/2021, de 26 de enero.
[104] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.

Otros agentes tendrán que llevar a cabo otras respuestas relevantes. Tendrán que prepararse para una serie de acciones que podrían incluir, si las circunstancias lo requieren:

- Disponer y operar elementos de respaldo. Esto no sólo requiere tener físicamente activos que sirvan como respaldo, sino también activarlos (mantenerlos en stand-by si es necesario) y activar equipos de trabajo y personal de respaldo para operar estos elementos de respaldo.
- En el peor de los casos, los centros de control dejarán de funcionar o quedarán bajo el control de los atacantes. En este caso, la respuesta requerirá aislar el centro de control u operación afectado y un centro alternativo deberá asumir las actuaciones que estaba llevando a cabo antes del ataque. El personal de los centros de operaciones redundantes deberá estar en alerta, listo para comenzar a trabajar cuando sea necesario.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

Una vez que se produzca el ataque físico, los Centros de Operaciones de Seguridad (SOC) activarán una serie de respuestas. Estos incluyen desde la revisión de privilegios de acceso hasta el traslado de la operación activa del sistema al Centro de Control secundario o redundante, el cual contará con un equipo de trabajo independiente.

Cuando el ataque es potencial, en caso de que se produzca un incidente, el Centro de Control siempre puede solicitar ayuda a las fuerzas policiales.

De hecho, las policías estatales y autonómicas (FCSE) activarán los Planes de Apoyo Operativo. De esta forma, la policía refuerza no sólo la seguridad sino también la respuesta al ataque. Se activa la coordinación entre los cuerpos policiales estatales o autonómicos y los servicios de seguridad del centro de control, actuando cada sujeto dentro de sus capacidades y trabajando conjuntamente para controlar la situación, contenerla y finalmente desactivarla.

El CNPIC[105] también actuará como punto de contacto ante el Ministerio del Interior sobre la operación de infraestructuras críticas y los planes de apoyo.

Finalmente, se producirá la activación del Protocolo de Comunicaciones SES-OCC-FCSE (Secretaría de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad - Fuerzas y Cuerpos de Seguridad del Estado)[106] para coordinar todos los esfuerzos hacia la solución de la crisis.

Otras Consideraciones.

Los impactos que presentan mayor probabilidad de ocurrir debido a este tipo de crisis son:

[105] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.
[106] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- Que resulte imposible operar los activos desde el Centro de Control afectado.
- Que se produzca un apagón parcial o total.

Sobre los impactos transfronterizos de este tipo de crisis, es probable que un ataque físico a los Centros de Control pueda afectar también a nuestros países vecinos. Este impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión si se tratara de activos afectados.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando los TSO vecinos pueden brindar apoyo. Así, se pueden tomar algunas de las siguientes acciones:

- Realizar intercambios de apoyo de energía activa con TSO vecinos.
- Aplicar los procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar los procedimientos de soporte de los sistemas español y portugués tras incidencias.

A fecha de hoy no se tiene una referencia para este tipo de crisis.

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
La Unidad de Seguridad Física de Red Eléctrica de España, S.A.U. y las unidades de seguridad física de otros agentes (como los DSO) pueden detectar la crisis, comunicarse y coordinarse con otros agentes.
Agentes implicados
Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales Centro Nacional Protección de Infraestructuras y Ciberseguridad (CNPIC), Instituto Nacional de Ciberseguridad (INCIBE), Oficina de Coordinación de Ciberseguridad (OCC), Ministerios).
II. PREVENCIÓN Y PREPARACIÓN
Medidas preventivas a nivel nacional
Las medidas que se pueden tomar antes de la crisis se incluyen: • Protección de infraestructuras. • Preparación del TSO. • Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad. • Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Seguridad física y electrónica perimetral.
- Establecer y aplicar las medidas de Protección del puesto de trabajo.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Llevar a cabo registros de usuarios de los centros de control.
- Aplicar y revisar la gestión de privilegios.
- Disponer de elementos de back up.
- Tener un Centro de Control redundante en activo.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Activación del Protocolo de Comunicaciones SES-OCC-FCSE[107] (Secretaria de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad – Fuerzas y Cuerpos de Seguridad del Estado).

[107] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.

- Aplicación de los Planes seguridad del Operador[108]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC.
- Aplicación de los Planes de Protección Específicos[109]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el CNPIC y también habrá comunicaciones con las Fuerzas y cuerpos de Seguridad del Estado (FCSE)
- Aplicación de los Planes de Apoyo Operativos[110]. Las acciones de despliegue serán realizadas por las FCSE.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

[108] Art. 16 y Capítulo III del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
[109] Art. 16 y Capítulo IV del Real Decreto 704/2011, de 20 de mayo.
[110] Art. 16 y Capítulo V del Real Decreto 704/2011, de 20 de mayo.

7.6 Escenario de ataque físico a activos críticos

Desencadenante/suceso inicial:

Tal y como se ha comentado anteriormente para los ataques físicos a uno o más Centros de Control, los ataques físicos a instalaciones e infraestructuras son incidentes intencionados. Considerando su gravedad y objetivos, no sólo no se pueden descartar impactos marcados a nivel regional, sino que es posible su impacto transfronterizo.

El Inventario Nacional de los Activos Críticos Nacionales (INACN) es el registro que contiene información completa y actualizada de los Bienes Críticos Nacionales ubicados en el territorio español. Como se mencionó, esta lista incluye algunos activos del sector eléctrico.

En este escenario, el desencadenante de este tipo de crisis en el sector eléctrico es un ataque físico a uno o más activos críticos, incluyendo subestaciones, líneas, grupos de generación, centros de datos, etc.

Antes del ataque físico.

Al igual que ocurre con los escenarios de ciberataque y ataque físico a los centros de control, hay una serie de acciones que preparan a los centros de control frente a ataques físicos. Cuanto más integrales y exhaustivas sean estas actuaciones, mejor preparado estará el sistema y mejor será la respuesta.

La planificación ocupa el primer lugar en la respuesta de seguridad. Una planificación adecuada es fundamental y el personal debe actualizar sus conocimientos sobre las amenazas y el comportamiento adecuado para evitar que los riesgos se materialicen en ataques dañinos.

Estas acciones incluyen también un análisis continuo de los riesgos potenciales, dándoles seguimiento tanto en el país como en otros países. Las diferentes fuerzas policiales, el CNPIC[111] e incluso el INCIBE[112] y la OCC[113] pueden proporcionar y proporcionarán información y actualizaciones útiles en el menor tiempo posible.

Considerando esto, los servicios de seguridad en los Sistemas de Control deben realizar las siguientes acciones:

- Realizar seguridad física y electrónica perimetral.
- Establecer y aplicar las medidas de Protección del puesto de trabajo.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Llevar a cabo registros de usuarios de los centros de control.

Si aparecen amenazas, el centro de control siempre puede solicitar ayuda a las fuerzas policiales. De este modo, la policía refuerza la seguridad y disminuye la probabilidad de un ataque físico. Se activa la coordinación entre los cuerpos policiales estatales o autonómicos y los servicios de seguridad del centro de control, actuando cada sujeto dentro de sus capacidades y trabajando juntos para evitar el potencial ataque.

---

[111] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.

[112] Proporciona los avisos e informes periódicos en su página de Internet https://www.incibe.es/incibe-cert

[113] Art. 4.4 del Real Decreto 43/2021, de 26 de enero.

Cuando exista amenaza, los interesados activarán Planes de Protección Específicos de los Centros de Control. El punto de contacto el Ministerio del Interior es el CNPIC[114] y habrá comunicaciones con las Fuerzas de Seguridad del Estado (FCSE).

Otros agentes tendrán que llevar a cabo otras respuestas relevantes. Tendrán que prepararse para una serie de actuaciones que podrán poner en funcionamiento determinados equipos o elementos de respaldo.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

Cuando el ataque es potencial, en caso de que se produzca un incidente, el Centro de Control siempre puede solicitar ayuda a las fuerzas policiales.

De hecho, las policías estatales y autonómicas (FCSE) activarán los Planes de Apoyo Operativo. De esta forma, la policía refuerza no sólo la seguridad sino también la respuesta al ataque. Se activa la coordinación entre los cuerpos policiales estatales o autonómicos y los servicios de seguridad del centro de control, actuando cada sujeto dentro de sus capacidades y trabajando conjuntamente para controlar la situación, contenerla y finalmente desactivarla.

El CNPIC también actuará como punto de contacto con el Ministerio del Interior sobre la operación de infraestructuras críticas y los planes de apoyo.

Finalmente, se producirá la activación del Protocolo de Comunicaciones SES-OCC-FCSE (Secretaría de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad - Fuerzas y Cuerpos de Seguridad del Estado)[115] para coordinar todos los esfuerzos hacia la solución de la crisis.

Otras Consideraciones.

Los impactos que es más probable que ocurran debido a este tipo de crisis son fundamentalmente daños a activos críticos.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando los TSO vecinos pueden brindar apoyo. Así, se pueden tomar las siguientes acciones:

- Realizar intercambios de apoyo de energía activa con TSO vecinos.
- Aplicar los procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar los procedimientos de soporte de los sistemas español y portugués tras incidencias.

[114] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.
[115] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.

A fecha de hoy no se tiene una referencia para este tipo de crisis.

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS

Detección de la Crisis/Evento desencadenante

La Unidad de Seguridad Física de Red Eléctrica de España, S.A.U. y las unidades de seguridad física de otros agentes pueden detectar la crisis, comunicarse y coordinarse con el CNPIC y otros agentes.

Agentes implicados

Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales Centro Nacional Protección de Infraestructuras y Ciberseguridad (CNPIC), Instituto Nacional de Ciberseguridad (INCIBE), Oficina de Coordinación de Ciberseguridad (OCC), Ministerios).

II. PREVENCIÓN Y PREPARACIÓN

Medidas preventivas a nivel nacional

Las medidas que se pueden tomar antes de la crisis se incluyen:

- Protección de infraestructuras.
- Preparación del TSO.
- Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad.
- Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Seguridad física y electrónica perimetral.
- Establecer y aplicar las medidas de Protección del puesto de trabajo.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Llevar a cabo registros de usuarios de los centros de control.
- Aplicar y revisar la gestión de privilegios.
- Disponer de elementos de back up.
- Tener un Centro de Control redundante en activo.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Activación del Protocolo de Comunicaciones SES-OCC-FCSE[116] (Secretaría de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad – Fuerzas y Cuerpos de Seguridad del Estado).
- Aplicación de los Planes seguridad del Operador[117]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC.
- Aplicación de los Planes de Protección Específicos[118]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el CNPIC y también habrá comunicaciones con las Fuerzas y cuerpos de Seguridad del Estado (FCSE).
- Aplicación de los Planes de Apoyo Operativos[119]. Las acciones de despliegue serán realizadas por las FCSE.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.

[116] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.
[117] Art. 16 y Capítulo III del Real Decreto 704/2011, de 20 de mayo.
[118] Art. 16 y Capítulo IV del Real Decreto 704/2011, de 20 de mayo.
[119] Art. 16 y Capítulo V del Real Decreto 704/2011, de 20 de mayo.

- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.7 Escenario de incendio o explosión en un activo crítico

Desencadenante/suceso inicial:

A diferencia de las crisis provocadas por ataques físicos, los escenarios de incendios o explosiones en activos, instalaciones e infraestructuras son situaciones en las que el incidente no es necesariamente intencionado. Como en los casos de ataques deliberados y considerando su gravedad y objetivos, las autoridades no pueden descartar impactos marcados a nivel regional, siendo también posible el impacto transfronterizo de este evento. Esta posibilidad puede darse si el incidente se produce cerca de la interconexión.

En este escenario, el desencadenante de este tipo de crisis del sector energético es un incendio o una explosión no intencionados en un activo crítico. Es poco probable que se produzca algún tipo de alerta temprana, ya que estos acontecimientos son repentinos y generalmente impredecibles.

Antes del incidente de incendio/explosión.

La preparación y la prevención ocupan el primer lugar en respuesta a estos incidentes.

Si bien la planificación no es una cuestión determinante, sí ayuda a mitigar las consecuencias. Además, es relevante en la prevención. Unos planes de mantenimiento adecuados previenen estos accidentes, al reducir su probabilidad.

El mantenimiento preventivo y predictivo reduce la probabilidad de incendios y accidentes en activos críticos.

El mantenimiento preventivo se realiza independientemente del estado en el que se encuentre el activo, ya que su principal objetivo es realizar revisiones para evitar averías y, en consecuencia, paradas de las máquinas.

El mantenimiento preventivo se realiza de forma programada y se realiza periódicamente (las revisiones periódicas pueden variar según la máquina), cuando se producen determinados eventos o la máquina alcanza un determinado número de usos. Los técnicos establecen estos hitos considerando la vida útil promedio o esperada del activo correspondiente. Para controlar tiempos y recursos para el mantenimiento, muchos técnicos utilizan programas de gestión en sus empresas.

Por otro lado, el mantenimiento predictivo responde a una serie de condiciones, relacionadas con las condiciones físicas u operativas de los activos. A diferencia del mantenimiento preventivo, no utiliza estadísticas ni fechas predefinidas. El objetivo de este tipo de mantenimiento es prevenir cualquier avería mediante pruebas, seguimiento y análisis continuo. Cuando los técnicos detectan cualquier condición o desgaste que pueda provocar una avería, se enciende una bandera de advertencia y se realiza el mantenimiento.

La mejor estrategia es utilizar ambas técnicas de mantenimiento, incluido por supuesto el mantenimiento correctivo.

Además, los agentes deberán prepararse para una serie de acciones que incluyen principalmente contar con y operar elementos de respaldo. Esto no sólo abarca tener físicamente activos que sirvan como respaldo, sino también activarlos (mantenerlos en stand-by si es necesario) y activar equipos de trabajo y personal de respaldo para operar estos elementos de respaldo.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

En caso de que se produzca un incidente como un incendio o una explosión en cualquiera de los activos críticos, el centro de control siempre puede solicitar ayuda a las fuerzas policiales y a los servicios de emergencia. Esto es algo muy diferente porque sólo sucedería si la naturaleza no intencional del incidente sigue sin estar clara, y sólo hasta que se aclare la duda.

El CNPIC también actuará como punto de contacto el Ministerio del Interior[120] sobre la operación de infraestructuras críticas y los planes de apoyo.

Finalmente, se producirá la activación del Protocolo de Comunicaciones SES-OCC-FCSE (Secretaría de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad - Fuerzas y Cuerpos de Seguridad del Estado)[121] para coordinar todos los esfuerzos hacia la solución de la crisis.

Otras Consideraciones.

Los impactos que es más probable que se produzcan por este tipo de incidentes son fundamentalmente:

En el caso de este escenario, el desencadenante en este tipo de crisis del sector eléctrico es un Incendio o una explosión no intencionados en un activo crítico. Los impactos que es más probable que se pueden dar como consecuencia de este tipo de incidentes son fundamentalmente:

- Que haya daños en activos críticos.
- Que se produzca una pérdida operativa del mercado eléctrico local.

En lo que se refiere al impacto transfronterizo de este tipo de crisis, se considera probable que un incidente en el que tenga lugar una incidencia o explosión en alguno de los activos críticos también pueda afectar a nuestros países vecinos. Este impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión, si son estos los activos que han sufrido el incendio o la explosión o están próximos a dichos activos o están conectados a ellos.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando los TSO vecinos pueden brindar apoyo. Así, se pueden tomar algunas de las siguientes acciones:

- Realizar intercambios de apoyo de energía activa con TSO vecinos.
- Aplicar procedimientos de soporte de los sistemas español y francés tras incidencias.
- Aplicar procedimientos de soporte de los sistemas español y portugués tras incidencias.

[120] Art. 7.a) del Real Decreto 704/2011, de 20 de mayo.
[121] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.

A fecha de hoy tampoco se tiene una referencia para este tipo de crisis en la Unión Europea.

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
La Unidad de Seguridad Física de Red Eléctrica de España, S.A.U. y las unidades de seguridad física de otros agentes pueden detectar la crisis, comunicarse y coordinarse con el CNPIC y otros agentes.
Agentes implicados
Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC, Instituto Nacional de Ciberseguridad INCIBE, Oficina de Coordinación de Ciberseguridad (OCC), Ministerios).
II. PREVENCIÓN Y PREPARACIÓN
Medidas preventivas a nivel nacional
Las medidas que se pueden tomar ante la crisis incluyen contar con elementos y equipos de respaldo.
Medidas preventivas a nivel regional
No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.
III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS
Medidas para atenuar la crisis a nivel nacional
Entre las medidas que se pueden tomar antes de la crisis se incluyen: • Protección de infraestructuras. • Preparación del TSO. • Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad. • Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas. Entre las medidas a adoptar durante la crisis se incluyen las siguiente: a) Medidas relacionadas con la operación del sistema: • Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.

- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Activación del Protocolo de Comunicaciones SES-OCC-FCSE[122] (Secretaria de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad – Fuerzas y Cuerpos de Seguridad del Estado).
- Aplicación de los Planes Seguridad del Operador[123]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC.
- Aplicación de los Planes de Protección Específicos[124]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el CNPIC y también habrá comunicaciones con las Fuerzas y cuerpos de Seguridad del Estado (FCSE).
- Aplicación de los Planes de Apoyo Operativos[125]. Las acciones de despliegue serán realizadas por las FCSE.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

[122] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.
[123] Art. 16 y Capítulo III del Real Decreto 704/2011, de 20 de mayo.
[124] Art. 16 y Capítulo IV del Real Decreto 704/2011, de 20 de mayo.
[125] Art. 16 y Capítulo V del Real Decreto 704/2011, de 20 de mayo.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.8 Escenario de sabotaje por parte de personal interno

Desencadenante/suceso inicial:

Al igual que ocurre con los ataques físicos a uno o más Centros de Control o los ataques físicos a activos críticos, los sabotajes por parte del personal interno son incidentes intencionados. Considerando su gravedad y objetivos, no sólo no se pueden descartar impactos marcados a nivel regional, sino que es posible su impacto transfronterizo.

En este escenario, el hecho iniciador de este tipo de crisis en el sector eléctrico es una manipulación intencional de sistemas críticos por parte de personal interno bajo amenaza o soborno.

Antes del sabotaje.

En respuesta a estos incidentes, lo primero que se puede hacer es cierta preparación y prevención.

Cada vez que aparece un indicador de advertencia, los equipos de seguridad de todas las instalaciones afectadas deben:

- Seguridad física y electrónica perimetral.
- Establecer y aplicar las medidas de Protección del puesto de trabajo.
- Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión.
- Llevar a cabo registros de usuarios de los centros de control.
- Aplicar y revisar la gestión de privilegios.
- Disponer de elementos de back up.
- Tener un Centro de Control redundante en activo.
- Identificar maniobras con gran impacto en la red para que requieran doble validación. Esto evita que un solo usuario los ejecute de forma independiente. Esto proporciona cobertura en caso de sabotaje o error humano.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico.*

Crisis.

Una vez ha tenido lugar el sabotaje, los diferentes Centros de Operaciones activarán una serie de respuestas. Estas incluyen acciones que van desde la revisión de los privilegios de acceso hasta el traslado de la operación activa del sistema a los centros de control secundarios o redundantes, que contarán con un equipo de trabajo independiente.

Si el suceso tiene lugar en las instalaciones del TSO, la Unidad de Seguridad Física de Red Eléctrica liderará la respuesta.

Al igual que cuando se produce un ataque (ya sea cibernético o físico), en caso de que se produzca un incidente como un incendio o una explosión en cualquiera de los activos críticos, el

centro de control siempre puede solicitar ayuda a las fuerzas policiales y a los servicios de emergencia.

De hecho, las policías estatales y autonómicas (FCSE) activarán los Planes de Apoyo Operativo[126]. De esta forma, la policía refuerza no sólo la seguridad sino también la respuesta al ataque. Se activa la coordinación entre los cuerpos policiales estatales o autonómicos y los servicios de seguridad del centro de control, cada sujeto actuando dentro de sus capacidades y trabajando juntos para controlar la situación, contenerla y finalmente desactivarla.

El CNPIC[127] también actuará como punto de contacto ante el Ministerio del Interior sobre la operación de infraestructuras críticas y los planes de apoyo.

Por último, se producirá la activación del Protocolo de Comunicaciones SES-OCC-FCSE (Secretaría de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad - Fuerzas y Cuerpos de Seguridad del Estado)[128] para coordinar todos los esfuerzos hacia la solución de la crisis.

Otras Consideraciones.

Los impactos que es más probable que se pueden dar como consecuencia de este tipo de crisis son fundamentalmente:

- Que tenga lugar la apertura múltiple de elementos de la red de transporte o distribución de energía eléctrica.
- Que se produzcan disparos de grupos de generación.

El impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión si se tratara de activos afectados.

Los impactos transfronterizos son una cuestión relevante. El TSO siempre puede afrontar mejor los daños a un activo crítico cuando depende de los TSO vecinos. Así, algunas de las siguientes acciones:

- Aplicar Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Aplicar los procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Aplicar los procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

Tal y como se establecía para los ataques físicos a uno o más Centros de Control o los ataques físicos a activos críticos, los sabotajes por parte de personal interno son incidentes intencionados. Teniendo en cuenta su gravedad y sus objetivos, no solo no se no se pueden descartar impactos marcados a nivel regional, sino que no el impacto transfronterizo de los mismo es también posible.

En el caso de este escenario, el desencadenante en este tipo de crisis del sector eléctrico es una manipulación intencionada de los sistemas críticos por parte de personal interno bajo amenaza o soborno.

[126] Art. 16 y Capítulo V del Real Decreto 704/2011, de 20 de mayo.
[127] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.
[128] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.

En lo que se refiere al impacto transfronterizo de este tipo de crisis, se considera probable que un ataque físico a uno o más activos críticos (en caso de ser coordinado), también pueda afectar a nuestros países vecinos. Este impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión, si son estos los activos que han sufrido el incidente.

A fecha de hoy no se tiene una referencia para este tipo de crisis en la Unión Europea.

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
La Unidad de Seguridad Física de Red Eléctrica de España, S.A.U. y las unidades de seguridad física de otros agentes pueden detectar la crisis, comunicarse y coordinarse con otros agentes y partes interesadas.
Agentes implicados
Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC, Instituto Nacional de Ciberseguridad INCIBE, Oficina de Coordinación de Ciberseguridad (OCC), Ministerios).
II. PREVENCIÓN Y PREPARACIÓN
Medidas preventivas a nivel nacional
Entre las medidas que se pueden tomar antes de la crisis se incluyen: • Protección de infraestructuras. • Preparación del TSO. • Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad. • Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas. Entre las medidas que se pueden tomar antes de la crisis se incluyen: • Seguridad física y electrónica perimetral. • Establecer y aplicar las medidas de Protección del puesto de trabajo. • Realizar un control de accesos de personas y vehículos (incluye autenticación) a los activos críticos en cuestión. • Llevar a cabo registros de usuarios de los centros de control. • Aplicar y revisar la gestión de privilegios. • Disponer de elementos de back up. • Tener un Centro de Control redundante en activo.

- Identificar maniobras con gran impacto en la red para que requieran doble validación. Esto evita que un solo usuario los ejecute de forma independiente. Esto proporciona cobertura en caso de sabotaje o error humano.

Medidas preventivas a nivel regional

Llevar a cabo la adaptación de los programas de intercambio con los Estado Miembros vecinos, así como con países terceros vecinos.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Activación del Protocolo de Comunicaciones SES-OCC-FCSE[129] (Secretaria de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad – Fuerzas y Cuerpos de Seguridad del Estado).
- Aplicación de los Planes de Seguridad del Operador[130]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC.
- Aplicación de los Planes de Protección Específicos[131]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el CNPIC y también habrá comunicaciones con las Fuerzas y cuerpos de Seguridad del Estado (FCSE).
- Aplicación de los Planes de Apoyo Operativos[132]. Las acciones de despliegue serán realizadas por las FCSE.

[129] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.
[130] Art. 16 y Capítulo III del Real Decreto 704/2011, de 20 de mayo
[131] Art. 16 y Capítulo IV del Real Decreto 704/2011, de 20 de mayo
[132] Art. 16 y Capítulo V del Real Decreto 704/2011, de 20 de mayo.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.9 Escenario de incendio forestal

Desencadenante/suceso inicial:

Los escenarios de incendios forestales son situaciones en las que el incidente no es necesariamente intencionado. Sin embargo, considerando su gravedad, es posible que se produzcan graves impactos a nivel regional.

En este escenario, el hecho iniciador de este tipo de crisis en el sector eléctrico es un incendio forestal que puede afectar al funcionamiento de instalaciones/activos críticos o, en su caso, estratégicos para el funcionamiento del sistema.

Antes del incendio forestal.

La preparación y la prevención son esenciales en respuesta a estos incidentes.

Los equipos de trabajo podrán realizar operaciones de limpieza forestal y desmonte alrededor de líneas e infraestructuras eléctricas en o cerca de los bosques.

Se hace necesaria una activación previa de los recursos para gestionar la crisis una vez que se materialice (personal de campo, grupos electrógenos, medios de reabastecimiento de combustible, medios especiales de acceso y extinción de incendios como aviones y helicópteros de extinción de emergencia, etc.).

También hay que considerar el posible impacto en el sistema de telecomunicaciones (voz y datos) provocado por la pérdida de suministro de antenas y repetidores durante un largo periodo (planificación de la instalación de grupos electrógenos y su repostaje).

En su caso, podría resultar necesario asegurar la disponibilidad de combustible para los grupos electrógenos, así como su traslado a los puntos de consumo.

Cada vez que aparece un indicador de advertencia, los equipos de seguridad de todas las instalaciones afectadas deben:

- Cancelar recierres de líneas/unidades.
- Realizar asignación de personal para identificar líneas afectadas y líneas abiertas.
- Los equipos de trabajo deben realizar continuamente operaciones de limpieza forestal y desmonte alrededor de líneas e infraestructuras eléctricas en o cerca de los bosques.
- Los Servicios de Emergencia deberán preparar las flotas de vehículos para la extinción de incendios.

Además, las autoridades y agentes del sistema eléctrico deben anticipar una evolución negativa de la crisis y prepararse para los peores escenarios.

Condición inicial del sistema antes del evento desencadenante.

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico.

Crisis.

Una vez que los servicios de Protección contra Incendios de las correspondientes Comunidades Autónomas detectan un incendio forestal, la respuesta debe ser inmediatas si este alcanza un Índice de Gravedad Potencial 2[133] o superior. En el peor de los casos, la UME podría participar en la extinción de los incendios forestales[134].

En caso de que se produzca un incendio forestal, el Centro de Control del Sistema siempre puede solicitar ayuda a las fuerzas policiales y a los servicios de emergencia.

El CNPIC[135] podrá actuar como punto de contacto con el Ministerio del Interior sobre la operación de infraestructuras críticas y los planes de soporte, en caso de que los activos críticos sufran daños o estén amenazados a causa del incendio.

Esta situación excepcional puede dar paso a que se produzca la activación del Protocolo de Comunicaciones SES-OCC-FCSE (Secretaría de Estado de Seguridad – Oficina de Coordinación de Ciberseguridad - Fuerzas y Cuerpos de Seguridad del Estado)[136] para coordinar todos los esfuerzos encaminados a la solución de la crisis.

El posible impacto en el sistema eléctrico se ve algo atenuado por el hecho de que España es un país muy grande y los incendios son eventos locales. Aunque el incendio forestal evolucione hasta convertirse en un evento mayor, los Servicios de Emergencia disponen de flotas de vehículos para hacer frente a la situación.

El Ministerio para la Transición Ecológica y el Reto Demográfico cuenta con las Brigadas de Refuerzo contra Incendios Forestales.

Las brigadas BRIF son unidades helitransportadas de personal de extinción de incendios altamente especializado. Prestan un servicio de apoyo a las comunidades autónomas, pudiendo actuar en cualquier lugar del territorio nacional, incluida Canarias[137].

Algunas acciones preventivas son esenciales en aquellas zonas donde se produce el incendio forestal:

- Los Servicios de Emergencia deberán preparar las flotas de vehículos para la extinción de incendios.
- El sistema de transporte debe estar preparado para abastecer las instalaciones desde las zonas de reserva del país a cada planta de generación que lo requiera.

Además, el TSO podrá cancelar los cierres de líneas/unidades y realizar la asignación de personal para identificar las líneas afectadas y las líneas abiertas.

Otras Consideraciones.

Los impactos que podrían presentarse a causa de este tipo de crisis son fundamentalmente:

---

[133] Anexo I del Real Decreto 893/2013, de 15 de noviembre, por el que se aprueba la Directriz básica de planificación de protección civil de emergencia por incendios forestales.
[134] Art. Tercero.1, letra b) del Protocolo de Intervención de la Unidad Militar de Emergencias, aprobado por el Real Decreto 1097/2011, de 22 de julio.
[135] Art. 7.a) del Reglamento de Protección de Infraestructuras Criticas.
[136] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.
[137] https://www.miteco.gob.es/es/biodiversidad/temas/incendios-forestales/extincion/brif.html

- Que existan daños en activos críticos o estratégicos.
- La indisponibilidad de instalaciones/activos críticos o estratégicos se produce a causa del incendio.

Al analizar los impactos transfronterizos de este tipo de crisis, es posible que se produzcan incendios que afecten a España y Portugal o a España y Francia al mismo tiempo. Este impacto transfronterizo se manifestaría fundamentalmente en pérdidas de las líneas de interconexión, si fueran estos los activos afectados por el incendio.

Así, se pueden tomar algunas de las siguientes acciones:

- La aplicación de intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- La aplicación de los procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- La aplicación de los procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

Como referencia más reciente de este tipo de crisis se puede citar el incendio en los Pirineos Orientales debajo de las líneas de interconexión eléctrica del 24 de julio de 2021 en Francia que derivó en el desacoplamiento del sistema eléctrico español-portugués del sistema europeo.

Las principales características de este escenario de crisis y las acciones que se adoptarán en el mismo son las siguientes:

I. DESENCADENANTE DE LA CRISIS
Detección de la Crisis/Evento desencadenante
Los servicios de Protección contra incendios de la Comunidades Autónomas correspondientes.
Agentes implicados
Se han identificado los siguientes agentes implicados: Red Eléctrica de España, S.A., los Gestores de la Red de Distribución (DSO), Empresas de generación, Fuerzas y Cuerpos de Seguridad del Estado (FCSE), Servicios de Protección contra incendios, Unidad Militar de Emergencias (UME), Organismos oficiales (Centro Nacional Protección de Infraestructuras y Ciberseguridad (CNPIC)), Ministerios.
II. PREVENCIÓN Y PREPARACIÓN
Medidas preventivas a nivel nacional
Entre las medidas que se pueden tomar antes de la crisis se incluyen: • Protección de infraestructuras. • Preparación del TSO. • Contar con reservas de combustible suficientes para evitar restricciones en determinados usos o aplicaciones de estos combustibles, incluido el uso para la generación de electricidad. • Asegurar una adecuada preparación de la red y del sistema eléctrico, lo que permite un mejor manejo de las crisis eléctricas.

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Cancelar recierres de líneas/unidades.
- Realizar asignación de personal para identificar líneas afectadas y líneas abiertas.
- Los equipos de trabajo deben realizar continuamente operaciones de limpieza forestal y desmonte alrededor de líneas e infraestructuras eléctricas en o cerca de los bosques.
- Los Servicios de Emergencia deberán preparar las flotas de vehículos para la extinción de incendios.
- El sistema de transporte debe estar preparado para abastecer las instalaciones desde los lugares de reserva del país a cada planta de generación que lo requiera.
- Identificar instalaciones críticas y condiciones de riesgo de incendio y establecer planes de acción que eliminen/minimicen este riesgo (presencia de árboles cerca de estas instalaciones críticas, por ejemplo).
- Establecer sistemas de alerta y vigilancia de incendios forestales en zonas donde existan o estén en funcionamiento activos críticos, que permitan una detección temprana.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

III. MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Entre las medidas a adoptar durante la crisis se incluyen las siguiente:

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Adaptación de los programas de intercambio con Francia, Portugal, Andorra y Marruecos.
- En caso de pérdida de telemando, desplazamiento de personal a Subestaciones Eléctricas críticas y envío de consignas y la comunicación con agentes vía telefónica.
- Medidas adicionales para el control de tensión en función de los distintos escenarios de demanda.
- Devolución de descargos.
- Deslastre de carga manual.
- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- Esquema automático control de sobre frecuencia: incluye plan de desconexión automática de generación.

b) Otras medidas:

- Activación del Protocolo de Comunicaciones SES-OCC-FCSE[138] (Secretaria de Estado de Seguridad - Oficina de Coordinación de Ciberseguridad – Fuerzas y Cuerpos de Seguridad del Estado).
- Aplicación de los Planes de Seguridad del Operador[139]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el Centro Nacional Protección de Infraestructuras y Ciberseguridad CNPIC.
- Aplicación de los Planes de Protección Específicos[140]. El Interlocutor con el que se mantendrán las comunicaciones en el ámbito de este plan es el CNPIC y también habrá comunicaciones con las Fuerzas y cuerpos de Seguridad del Estado (FCSE)
- Aplicación de los Planes de Apoyo Operativos[141]. Las acciones de despliegue serán realizadas por las FCSE.

Medidas para atenuar la crisis en el marco regional

Entre las medidas que se pueden adoptar durante la crisis, cuando ésta tiene un impacto transfronterizo, se incluyen las siguiente:

- Intercambios de apoyo de potencia activa entre los Gestores de Redes de Transporte vecinos.
- Procedimientos de apoyo de los sistemas español y francés para la reposición del servicio tras incidentes generalizados.
- Procedimientos de apoyo de los sistemas español y portugués para la reposición del servicio tras incidentes generalizados.

IV. IMPACTO

Se prevé que la crisis tenga un impacto sobre consumidores, Gestores de las Redes de Distribución, Generadores, así como en el caso de una crisis regional en los TSO vecinos.

V. EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA

En este aspecto, se llevará a cabo un:

- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

7.10 Escenario de erupción volcánica.

Desencadenante/suceso inicial:

El desencadenante de esta crisis es la erupción de un volcán activo. La actividad sísmica en los alrededores puede ocurrir antes de la erupción, aunque lo más probable es que ocurra con menos de una hora de aviso.

[138] Art. 14 del Real Decreto-ley 12/2018, de 7 de septiembre.
[139] Art. 16 y Capítulo III del Real Decreto 704/2011, de 20 de mayo.
[140] Art. 16 y Capítulo IV del Real Decreto 704/2011, de 20 de mayo.
[141] Art. 16 y Capítulo V del Real Decreto 704/2011, de 20 de mayo.

El 19 de septiembre de 2021 el volcán de Cumbre Vieja (en la isla de La Palma) entró en erupción y el Gobierno de Canarias con la cooperación del Gobierno español aplicó el Plan de Emergencia Volcánica de Canarias (PEVOLCA). La erupción volcánica duró 85 días y hubo suministro eléctrico exclusivamente en la isla.

En España[142] existen varias áreas volcánicas entre las que se incluyen:

- Las Islas Canarias (en los SETNP).
- La comarca de La Garroxta (Girona).
- Cabo de Gata (Almería).
- Cofrentes (Valencia).
- Las Islas Columbretes (Castellón).
- Campos de Calatrava (Ciudad Real).

Entre ellas, solamente en La Garrotxa y en Canarias han tenido lugar erupciones durante los últimos 10.000 años, y únicamente en el archipiélago canario ha habido erupciones en épocas históricas recientes[143].

El impacto de una erupción sobre el sistema eléctrico, los hogares, las infraestructuras de transporte y cualquier otra infraestructura es potencialmente grande. También son más prolongados en el tiempo que en la mayoría de los escenarios de crisis porque el acceso a las instalaciones dañadas debe esperar hasta que la lava se enfríe.

Antes del incidente/desencadenante.

El Instituto Geográfico Nacional (IGN) detecta cuándo comienza a crecer la actividad sísmica[144] en un volcán o alrededores. Este proceso pre-eruptivo evolucionará y el IGN monitoreará cómo se desarrolla. Este seguimiento y análisis del proceso volcánico ayudará a prevenir y mitigar sus riesgos primarios y secundarios (apertura de centros eruptivos, afectación de infraestructuras, deslizamientos de tierra, mapa de peligrosidad térmica, etc.).

Otras entidades, como el Instituto Español de Oceanografía y AEMET podrán contribuir realizando análisis similares de las posibles consecuencias de la erupción.

En este sentido, el Instituto Español de Oceanografía puede evaluar las consecuencias de la llegada de lava al mar en el ecosistema marino y la navegación, así como analizar las posibles salidas de gases de origen volcánico o hidrotermal[145].

AEMET puede activar el sistema de modelización y seguimiento de la posible emisión de gases y cenizas volcánicas a la atmósfera[146].

Condición inicial del sistema antes del evento desencadenante.

[142] https://www.proteccioncivil.es/coordinacion/gestion-riesgos/geologicos/volcanes
[143] https://www.proteccioncivil.es/coordinacion/gestion-riesgos/geologicos/volcanes
[144] Art. 16.1.f) del Real Decreto 253/2024, de 12 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Transportes y Movilidad Sostenible, y se modifica el Real Decreto 1009/2023, de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.
[145] Conforme a lo establecido en el art. 3.3 del Estatuto del Instituto Español de Oceanografía.
[146] A través del servicio de relativo a la Composición química de la atmósfera: https://www.aemet.es/es/eltiempo/prediccion/calidad_del_aire

El sistema eléctrico se encuentra en estado normal. Es decir, en una situación en la que todas las variables de control que caracterizan el estado del sistema (frecuencia, tensiones en los nodos de la red y niveles de carga en los diferentes elementos de la red de transporte) se encuentran dentro de los márgenes normales de operación y los criterios de seguridad ante contingencias se están cumpliendo, según lo indicado en el procedimiento de operación *PO 1.1. Criterios de funcionamiento y seguridad para la operación del sistema eléctrico*.

Crisis.

Las siete principales amenazas de una erupción son:

- Flujos de lava.
- Caída de ceniza.
- Flujos piroclásticos, que están compuestos por gases y material sólido (cenizas y rocas de diversos tamaños) capaces de fluir a altas temperaturas y velocidades y de superar obstáculos en su camino.
- Emanaciones de gases.
- Lahares, que son flujos de sedimentos y agua que se desplazan desde las laderas de los volcanes.
- Deslizamientos de tierra, cuando la erupción se produce en tierra firme continental o cerca de regiones montañosas.
- Tsunamis, cuando la erupción se produce en el mar/océano o incluso en la costa.

Los ciudadanos deben evacuar inmediatamente aquellas regiones y zonas donde se producirán flujos piroclásticos y de lava. Estos riesgos se ven agravados por posibles deslizamientos de tierra, aumentando así la necesidad de reubicación de estos ciudadanos. Además, las erupciones volcánicas casi siempre causarán daños graves e irreparables a edificios e infraestructuras, otras redes energéticas, redes de suministro de agua y carreteras.

Las acciones correctivas (para mitigar o simplemente responder a los desafíos en el suministro de energía) son más difíciles porque los viajes físicos son más difíciles, cuando no imposibles.

Otras Consideraciones.

Los impactos que es más probable que ocurran debido a este tipo de crisis son esencialmente:

- Reducciones y cortes en el suministro eléctrico.
- Daños en distintas infraestructuras y edificios.
- Posible racionamiento del suministro eléctrico si el combustible para
- Falta de otros recursos y equipos vitales.
- Impacto negativo en el transporte local por carretera, el transporte marítimo y el transporte aéreo.

El ejemplo más reciente de este tipo de crisis es la erupción volcánica en Cumbre Vieja de 2021.

Las principales características de este escenario de crisis y las acciones a tomar ante él se muestran a continuación:

• **DESENCADENANTE DE LA CRISIS**
Detección de la Crisis/Evento desencadenante

El Instituto Geográfico Nacional (IGN).

Agentes implicados

Se han identificado los siguientes agentes implicados:

- Red Eléctrica de España, S.A.U.,
- E-distribución Redes Digitales, S.L.U. como Gestor de la Red de Distribución (DSO) de los Sistemas Eléctricos de os Territorios No Peninsulares (SETNP) de Canarias.
- Empresas de generación.
- Ministerios, gobiernos regionales y gobiernos municipales.

• PREVENCIÓN Y PREPARACIÓN

Medidas preventivas a nivel nacional

Entre las medidas que se pueden tomar antes de la crisis se incluyen:

- Planificación:
  - Anticipar el recorrido de la lava antes y durante la erupción volcánica. Una evaluación continua de la situación ayudará al TSO y al DSO a realizar cortes preventivos por tramos para evitar cortocircuitos y problemas de suministro en las líneas que aún quedan en pie.
- Valorar la devolución de descargos y la reposición de elementos.
- Implementar la cancelación de recierres de líneas/unidades.
- Preparación de la red de distribución del DSO:
  - El diseño de la red del DSO debería dar relevancia a la redundancia. Una red reticular está formada por una serie de infraestructuras desplegadas como anillos sucesivos, con múltiples líneas que interconectan diferentes anillos.
  - o El DSO puede desplegar un número significativo de recursos técnicos y humanos donde se esperan problemas en la red (si las condiciones de seguridad lo permiten).
- Revisar recomendaciones realizadas a los consumidores sobre cómo reducir el consumo de electricidad.

Medidas preventivas a nivel regional

No existen medidas preventivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

• MEDIDAS CORRECTIVAS QUE PODRÁN ADOPTARSE DURANTE LA CRISIS

Medidas para atenuar la crisis a nivel nacional

Las acciones que se pueden tomar durante la crisis incluyen las siguientes. La adopción de estas acciones dependerá de las características específicas de la crisis y de los impactos que pueda tener en los sistemas eléctricos.

a) Medidas relacionadas con la operación del sistema:

- Aplicación de restricciones técnicas en tiempo real para gestionar desvíos de frecuencia fuera de los límites establecidos.
- Gestión de la generación a través de redespachos de generación.
- Devolución de descargos.
- Deslastre de carga manual.

- Esquema de deslastre automático de cargas por subfrecuencia: incluye la desconexión de grupos de bombeo y posteriormente deslastre de cargas preseleccionadas.
- En caso de situación de subfrecuencia: deslastre automático de carga mediante mecanismos y esquemas de subfrecuencia. Incluye la desconexión de los grupos de bombeo y posterior deslastre de carga preseleccionado.
- En caso de situación de sobrefrecuencia: mecanismos y esquemas de control automático de sobrefrecuencia, incluido el plan de desconexión automática de generación.
- Asignación de personal de campo para identificar líneas afectadas y líneas abiertas.
- También podrán realizar cortes preventivos para evitar mayores daños a la red y minimizar posibles incidencias en el suministro.
- La restauración del sistema puede incluir el uso de unidades de generación móviles/portátiles. Las unidades de energía móviles pueden abastecer a los consumidores que enfrentan escasez debido a líneas dañadas en la red DSO.

b) Otras medidas:

- Reconstrucción del sistema:
  - Realizar una planificación considerando restricciones en el acceso físico a las ubicaciones debido a que la lava ha dañado la red viaria.
  - Ordenar actuaciones considerando otras necesidades como las de vivienda, medicamentos o agua.
  - Reconstruir líneas eléctricas dañadas, soportes de media y baja tensión, centros de distribución.

Medidas para atenuar la crisis en el marco regional

No existen medidas correctivas a nivel regional para este tipo de escenarios de crisis del sistema eléctrico.

- **IMPACTO**

Se prevé que la crisis tenga un impacto sobre consumidores, en el Gestor de las Redes de Distribución, Generadores, así como en la red del TSO.

- **EVALUACIÓN POSTERIOR Y ACCIONES DE MEJORA**

En este aspecto, se llevará a cabo un:

- Involucrar a las empresas en simulaciones conjuntas de Red Eléctrica y el DSO local de escenarios de crisis.
- Análisis y correlación de eventos para reconstruir la secuencia de hechos.
- Informe, lecciones aprendidas y acciones de mejora.
- Participación en grupos de trabajo internacionales para el análisis de incidentes (Ej. ENTSO-E).

8. Consulta a las partes interesadas.

Con fecha 5 de noviembre de 2020, el Ministerio para la Transición Ecológica y el Reto Demográfico, como Autoridad Competente, inició las consultas sobre el plan de preparación frente a los riesgos del sector eléctrico de conformidad con el apartado 1 del artículo 10 del Reglamento (UE) 2019/941.

En la consulta participaron DSOs, el TSO, los principales generadores y sus asociaciones empresariales.

El TSO dirigió la reunión de consulta, trascurrida la cual el ministerio recibieron contribuciones de 11 partes interesadas, que se incorporaron al PRR finalizado.

El 5 de enero de 2022, el Ministerio para la Transición Ecológica y el Reto Demográfico remitió al ECG la primera versión del PPR español de conformidad con el apartado 4 del artículo 10 del Reglamento (UE) 2019/941. Esta versión del documento también aparece en la plataforma CIRCAB.

Según establece el apartado 5 del artículo 10 del Reglamento (UE) 2019/941, durante el período de seis meses siguiente, otros Estados miembros, ya sea en la misma región que España (SWE SOR) o en otras regiones, así como el ECG, podrían contribuir a mejorar el plan PPR con sus sugerencias, recomendaciones y propuestas. El Ministerio no recibió comentarios ni recomendaciones sobre la primera versión del plan.

La Comisión Europea elaboró y envió Dictamen de fecha 14 de junio de 2022 con arreglo al Reglamento (UE) 2019/941, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE, relativo al plan de preparación frente a los riesgos presentado por la autoridad competente de España.

El Ministerio para la Transición Ecológica y el Reto Demográfico ha considerado las diferentes recomendaciones realizadas por la Comisión en esta versión final del PPR.

Además, con fecha 5 de noviembre de 2022, el Ministerio para la Transición Ecológica y el Reto Demográfico consultó nuevamente a los DSOs, el TSO, los principales generadores y sus asociaciones empresariales esta vez sobre la versión final del PPR.

En esta segunda consulta se plantearon dos cuestiones derivadas de las recomendaciones:

I. La revisión de la identificación de los escenarios realizada.

Se solicitó valorar la posibilidad de incorporar un escenario adicional a los identificados e incluidos en la primera versión del PPR enviado a la Comisión el 5 de marzo de 2022.

Se trataba del Escenario de desabastecimiento de combustibles fósiles (incluido el gas natural).

Se informó a los interesados que dados los eventos que tuvieron lugar en Ucrania, la Comisión Europea había recomendado incluir una nueva valoración en los planes de riesgos nacionales, para estudiar la posibilidad de incluir el escenario relativo a una interrupción o falta de suministro de combustible fósiles en el PPR.

La guerra en Ucrania había puesto de manifiesto la problemática de suministro de gas natural. Esto tenía impactos transversales en la sociedad, entre los que se incluía el incremento de precios de la energía y los riesgos que sufrían todos los ciudadanos, y en particular aquellos que se encontraban en situaciones de vulnerabilidad y de pobreza energética.

Fue por esto por lo que este escenario fue objeto específico de la segunda consulta a los agentes.

II. La revisión de la información de los escenarios seleccionados.

Por otra parte, se solicitó una revisión de los procedimientos y acciones establecidos en el actual capítulo 7 del PPR. Se revisó toda la información relativa a:

- Los desencadenantes de las diferentes crisis de electricidad.
- Las medidas propuestas tanto nacionales como regionales.
- Los impactos de las diferentes crisis.
- Las medias encaminadas a llevar a cabo la evaluación posterior y las acciones de mejora que podían resultar de esta evaluación.

En relación con la posible incorporación al PPR del escenario de desabastecimiento de combustibles fósiles (incluido el gas natural) también se solicitó que, si se consideraba necesaria su inclusión, se añadieran igualmente la correspondiente información relativa a los desencadenantes, medidas, impactos y evaluación.

Varios agentes e interesados han realizado propuestas en una o ambas convocatorias de la consulta del plan. El Ministerio para la Transición Ecológica y el Reto Demográfico ha analizado las diferentes recomendaciones y las ha incluido en el PPR, mejorándolo.

Entre las respuestas recibidas se encontraron las siguientes:

- Un DSO sugirió, en línea con la recomendación de la Comisión Europea, que en el PPR se especifique cuál es la región de operación a la que pertenece España. Se ha procedido a incorporar esta propuesta.
- Por otra parte, sugirió introducir un apartado explicando la coordinación prevista entre la preparación ante el riesgo del sector gasista y el eléctrico tanto en España como en la región. Se han recogido en los apartados correspondientes el marco de coordinación entre el sector eléctrico y el del gas en los capítulos 1, 5, 6 y 7.
- Otro DSO señaló que debería tenerse en cuenta la casuística específica de los territorios no peninsulares, debido a su carácter aislado, menor tamaño, menor mallado de las redes y la dificultad de solucionar rápidamente determinados problemas que se pudieran dar, aunque la probabilidad de ocurrencia pudiese ser baja. También se ha tomado en consideración esta propuesta, destacando que como resultado final se ha incorporado el escenario de erupción volcánica, que puede afectar en especial a los SETNP.

En relación con los escenarios concretos se han realizado una serie de propuestas que se detallan a continuación:

- En el escenario de pandemia se han recibido y tomado en consideración en el PPR las siguientes propuestas:
    - Un DSO propuso como medida preventiva en el escenario de pandemia que cada compañía dispusiera de planes de continuidad de negocio que abordasen las medidas a tomar en caso de posibles indisponibilidades de personas, instalaciones, sistemas y proveedores. Se ha tomado razón de esta propuesta.
    - Además, añadió que era necesario probar estos planes de continuidad de manera periódica con el fin de asegurar su viabilidad, actualización y conocimiento por parte de toda la organización.

- En el escenario de pandemia se propuso añadir como medida preventiva el incluir medidas a aplicar al personal de campo (propio y de empresas colaboradoras) como las de evitar contacto entre brigadas y rotación, establecer turnos de uso de vestuarios y zonas comunes, limitación de aforos en zonas comunes, etc.
- Contemplar también que se utilicen Centros de Control de Respaldo en caso de existir para facilitar la creación de "equipos burbuja".

- En el escenario de tormenta extrema se han tomado en consideración las siguientes propuestas, incorporándolas al PPR:

  - Se puntualizó que la dificultad de acceso también puede estar causado por la caída de arbolado sobre la vía pública (carreteras) o pistas forestales para acceso a las instalaciones. Esto mismo ocurriría en caso de lluvia torrenciales que causen daños a la red viaria, desprendimientos, etc.
  - Se recomendó incluir en la descripción que las consecuencias pueden incluir la pérdida de comunicaciones de voz y datos a través de señal móvil que afecte al personal de campo y a la comunicación de los Centros de Control con dicho personal.
  - Se propuso añadir como medida preventiva la preactivación de los recursos que se estimen necesarios para gestionar la crisis una vez ésta se materialice (personal de campo, grupos electrógenos, medios de repostaje de grupos, medios de acceso especiales como motos de nieve, helicópteros, etc.).
  - Se indicó la necesidad de tener en cuenta la posible afección al sistema de telecomunicaciones (voz y datos) motivado por la pérdida de suministro a antenas y repetidores durante un largo periodo de tiempo (previsión de instalación de grupos electrógenos y repostaje de éstos).

- En el escenario de ciberataque a los centros de control se han tomado en consideración las siguientes propuestas, incorporándolas al PPR:

  - Se propuso incluir que en los escenarios de ciberataque a los centros de control el desencadenante también puede ser detectado por la Oficina de Coordinación de Ciberseguridad (OCC) a través de la declaración de nivel de alerta máximo, así como por INCIBE-CERT. También debería reflexionarse si el SOC de otros agentes (como DSOs) pueden detectar el desencadenante, aunque podría coordinarse a través del CERT de referencia (INCIBE).
  - Se sugirió añadir como medida preventiva adicional la definición de diferentes niveles de aislamiento de las redes IT/OT de los agentes implicados en caso de amenaza de ciberataque.
  - Se recomendó incluir que en el caso de los centros redundantes se debe asegurar que disponen de capas de seguridad redundantes o asegurar que el ciberataque no pueda llegar a éstos a la vez que a los centros de control principales (equipos apagados o aislados de red externa)
  - Se ha incluido en otras medidas, con el fin de contener el ciberataque, pero permitir que se pueda seguir operando -aunque sea en precario- los operadores de servicios esenciales como los DSOs disponían de un conjunto de medidas de aislamiento que permiten ir reduciendo la superficie de exposición de la compañía con el fin de mantener los procesos críticos (operación de la red).

- En el escenario de ciberataque a activos críticos además de replicar las consideraciones anteriores (debidamente ajustadas) se recomendó incluir la necesidad de disponer de planes de contingencia asociados a aquellos activos que se identifiquen como críticos (no sólo Centros de Control) con el objetivo de minimizar el efecto de la pérdida de la instalación.
- En el escenario de sabotaje se sugirió añadir como medida preventiva el identificar maniobras singulares con gran afección a la red de modo que requieran de una doble validación, de modo que un único usuario no pueda ejecutarla de manera independiente. Esto daría cobertura en caso de sabotaje o de error humano.
- En el escenario incendios se propuso añadir como medida preventiva la identificación de instalaciones críticas y su riesgo de incendio con el objetivo de definir el correspondiente plan de actuación que eliminase o minimizase ese riesgo. También se sugirió incluir la necesidad de establecer sistemas de alerta y vigilancia de incendios forestales en zonas en las que existan o discurran activos críticos, que permitieran la detección temprana.

Por otra parte, se han realizado una serie de propuestas que superan el ámbito de este PPRy que, por lo tanto, no se han incorporado al plan. Se trata de las siguientes:

- Respecto a los escenarios propuestos por ENTSO-E, se señaló que el escenario de incidente invernal y el escenario de ola de frío estaban interrelacionados y se propuso tenerlo en cuenta en la valoración. Esta cuestión no era objeto del PPR, sino de la revisión de los escenarios de crisis regionales.
- Respecto al escenario de fallos múltiples por fenómenos meteorológicos extremos se propuso su eliminación por solaparse con los escenarios de incidente invernal y ola de calor. Nuevamente se trataba de una cuestión que no era objeto de este plan, sino de la revisión de los escenarios de crisis regionales.
- Desde el sector se señaló que, para mitigar el impacto de estos escenarios, existían procedimientos de operación en vigor, algunos de los cuales estaban desactualizados, requiriendo una revisión profunda y adaptación a los tiempos y necesidades actuales, como el Reglamento (UE) 2017/2196 de la Comisión de 24 de noviembre de 2017, por el que se establece un código de red relativo a emergencia y reposición del servicio (NC ER). La revisión de normas y procedimientos tampoco entraba en el objeto del PPR.
- Uno de los DSO considera que los escenarios más críticos serían los de los ataques físicos o ciberataques. No obstante, se les asigna una probabilidad de ocurrencia *"muy improbable"*, cuando consideran que se le debería asignar un nivel mayor (*"posible"*). Esta revisión de la valoración deberá realizarse en el momento de seleccionar los escenarios nacionales.

Finalmente, en relación con la valoración del escenario de desabastecimiento de combustibles fósiles (incluido el gas natural) se recomendó desde un DSO que se desarrollase este escenario por completo, aunque aparentemente pueda pesar menos en España que en otros países del entorno. La situación internacional y las limitaciones a determinadas importaciones eran un ejemplo de esta situación de riesgo que podían acaecer. Más allá del suministro peninsular (gas fundamentalmente), se indicó que debía tenerse en cuenta que en los sistemas eléctricos de los territorios no peninsulares los productos petrolíferos son la principal base de la generación eléctrica.

Se realizó el desarrollo de las particularidades de este escenario, pero como se ha explicado finalmente este tipo de crisis no forman parte de los escenarios nacionales de crisis de electricidad de este PPR.

9. Simulacros.

Existen varias simulaciones relacionadas con la crisis de electricidad y el funcionamiento del sistema. Los dos campos principales en los que se centran estos ejercicios son la operación del sistema y la ciberseguridad.

9.1 Simulacros relativos a la operación del sistema.

El TSO realiza una serie de simulacros relacionados con la operación del sistema. La mayoría de ellos son periódicos, pero otros son ejercicios puntuales para probar la preparación del sistema.

Simulacros periódicos de operación del sistema.

El Operador del Sistema realiza periódicamente simulacros de reposición de servicios:

- Son ejercicios en los que se considera como situación de partida una incidencia que provoca un fallo de suministro que afecta a todo el Sistema Peninsular o a parte de él, y se simula cómo se llevaría a cabo la reposición del servicio.
- El objetivo de estos ejercicios es validar los Planes de Reposición del Servicio, contribuir a la formación continua de los operadores y verificar la coordinación, organización y jerarquía entre los centros de control.
- Estos ejercicios involucran la participación de todas las empresas de generación y distribución de electricidad que tengan activos en el área cubierta por el ejercicio. Además, se dispone de la participación de los TSO vecinos (RTE y REN) si el incidente simulado afecta a la interconexión con Francia y/o Portugal.

Tanto para las tecnologías de la información como para las tecnologías de operación, se dispone de planes de recuperación y se realizan las pruebas periódicas pertinentes. Contamos con un conjunto de documentos con los posibles tipos de pruebas, el cronograma de pruebas periódicas definido y una descripción de cómo realizar y planificar las pruebas. Los principales escenarios contemplados para los simulacros son:

a) Compromiso e interrupción de los sistemas del centro de control.
b) Compromiso y fallo de los sistemas de ambos centros de control.
c) Compromiso del equipo de protección.
d) Compromiso de los sistemas de telecomunicaciones y compromiso de los enrutadores.
e) Compromiso de los equipos de telecontrol IOS y CCS.

9.2 Simulacros relativos a la de ciberseguridad.

INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad de España, lleva a cabo cada año una serie de ciber-ejercicios sectoriales y multisectoriales, denominados CyberEx[147].

Desde 2012, INCIBE-CERT ha sido uno de los coordinadores (junto con la OCC) en la ejecución de ciber-ejercicios y simulacros para el sector privado. Estos ejercicios constan de diferentes pruebas que se centran en la capacidad de respuesta de cualquier entidad ante un ciberataque. Uno de los participantes potenciales son los operadores de servicios esenciales y los operadores críticos.

Dado que la ciberseguridad es un elemento transversal en la estructura organizativa de la entidad, en los ejercicios CyberEx participan todos los perfiles que tienen un papel que desempeñar en este ámbito:

- Perfiles ejecutivos,
- Mandos intermedios/gerentes,
- Equipos técnicos para responder a ciberataques,
- Equipo de seguridad física, y
- Perfiles no técnicos.

Todos los años se realizan simulaciones de CyberEx. Los operadores estratégicos y críticos del sector eléctrico son uno de los principales participantes, centrándose en los aspectos técnicos y procedimentales de la ciberseguridad. Los ejercicios CyberEx se desarrollan en 5 fases:

- ***Fase 01 - Invitación y manifestación de interés:***

INCIBE y OCC invitan a participar en el plazo establecido a todas las entidades elegibles, que puedan manifestar su interés.

El plazo de manifestación de interés está normalmente abierto hasta mediados de noviembre del año anterior al ejercicio.

- ***Fase 02 - Firma de acuerdos:***

INCIBE y OCC seleccionan a los participantes finales, de entre todos los operadores invitados que han mostrado su interés, y una vez seleccionados proceden a firmar los acuerdos legales pertinentes con las entidades seleccionadas.

El periodo de firma del acuerdo está normalmente abierto hasta la última semana de diciembre del año anterior al ejercicio.

- ***Fase 03 - Ejecución:***

En los ejercicios participan las entidades que se han apuntado. Estos han sido elaborados previamente, teniendo en cuenta la experiencia acumulada en ediciones anteriores de los ejercicios y la información recopilada sobre nuevos desarrollos y actores en ciberseguridad.

Fechas de ejecución: desde la segunda semana de enero hasta el 31 de marzo.

[147] Capítulo 4 – Líneas de Acción y Medidas de la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, Línea de Acción 2.11

- ***Fase 04 - Evaluación y revisión:***

Una vez finalizado el simulacro, INCIBE-CERT evalúa el desempeño de los participantes en las diferentes pruebas a través de los controles predefinidos y envía la evaluación de sus resultados a las entidades. Podrán revisar la evidencia recopilada y su evaluación y brindar sus comentarios en caso de detectar algún error o inconsistencia.

La fecha prevista de la fase de evaluación y revisión se sitúa en el mes de julio del año en que se realicen los ejercicios.

- ***Fase 05 – Informe final:***

INCIBE-CERT elabora y envía a cada operador un informe final sobre su desempeño, incluyendo posibles aspectos de mejora.

La fecha estimada de emisión del informe final es en el mes septiembre del año en que se realicen los ejercicios.

Descripción de los ejercicios de la Fase 03:

Durante los ejercicios CyberEx se llevan a cabo tres pruebas diferentes:

i. Juego de roles:

Es una prueba que simula un escenario de crisis. La respuesta se orienta a la toma de decisiones por parte de los diferentes niveles ejecutivos de la entidad. A medida que avance el ejercicio, se producirán diferentes eventos/circunstancias hipotéticas y los diferentes roles de la entidad deben valorar cómo actuar y analizar si es adecuado el diseño de los procedimientos de la propia entidad.

Este ejercicio está dirigido a perfiles ejecutivos y mandos intermedios que forman parte del comité de crisis. Se realiza mediante videoconferencia y tiene una duración máxima de 3 horas.

ii. Simulación de incidentes:

El objetivo de esta prueba es formar en cómo realizar una investigación de forma ágil y solvente. Los agentes deben actuar combinando la toma de decisiones, la colaboración y la coordinación interna y externa a diferentes niveles. Para que la prueba finalice es necesario controlar completamente el incidente y sentar las bases para la recuperación ante el ataque y sus consecuencias.

Este ejercicio está enfocado a los equipos técnicos que responden a ciberataques. Se desarrolla online a lo largo de un día y tiene una duración estimada de 8 horas.

iii. Ataque dirigido:

Es una prueba en la que hay un intento de intrusión en la infraestructura tecnológica de la entidad participante. Los atacantes utilizan diferentes técnicas y herramientas, no comunicadas previamente, como las que podría utilizar un atacante real. El objetivo final consiste en conseguir que el atacante no logre penetrar la infraestructura tecnológica de la entidad participante.

Este ejercicio está dirigido a equipos de seguridad física y lógica, equipos técnicos de respuesta a ciberataques y otros empleados. Se realiza a lo largo de uno o más días, pero no requiere una intervención planificada por parte de la entidad.