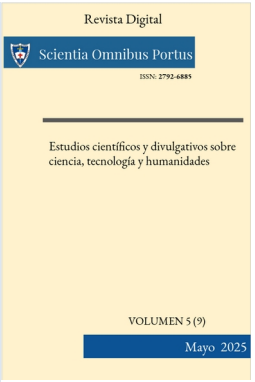
SciOP. 2024, 5(9)
Scientia Omnibus Portus
ISSN: 2792-6885
https://iescelia.org/ojs



Artículo

El Sistema de Seguridad Nacional como eje vertebrador de la protección de infraestructuras críticas. 28A25: la dimensión de disponibilidad

Francisco José de Haro Olmo
I.E.S. Celia Viñas
fjharo@iescelia.org

Resumen: El pasado 28 de abril de 2025, España se vio inmersa en un evento sin precedentes que puso de manifiesto la compleja interconexión de sus servicios esenciales: un apagón de alcance nacional. Este suceso trascendió la mera interrupción del suministro eléctrico, revelando la vulnerabilidad sistémica de un entramado de infraestructuras críticas cuya operatividad es fundamental para el sostenimiento de la sociedad moderna. El presente trabajo analiza los requisitos de protección implementadas en el marco de la Ley de Seguridad Nacional y su interacción con el Esquema Nacional de Seguridad, resaltando la importancia de la dimensión de disponibilidad de los servicios ofrecidos por las infraestructuras críticas.

Palabras clave: Seguridad, infraestructuras críticas, apagón, crisis energética, resiliencia, disponibilidad.

Introducción

El pasado 28 de abril de 2025, España se vio inmersa en un evento sin precedentes que puso de manifiesto la compleja y, en ocasiones, frágil interconexión de sus servicios esenciales: un apagón de alcance nacional. Este suceso, cuyas causas aún se investigan en profundidad, trascendió la mera interrupción del suministro eléctrico, revelando la vulnerabilidad sistémica de un entramado de infraestructuras críticas cuya operatividad es fundamental para el sostenimiento de la sociedad moderna. Sectores tan vitales como la energía, las telecomunicaciones, la banca y la sanidad se vieron directa o indirectamente afectados, evidenciando un fallo en cascada como consecuencia de la falta de suministro eléctrico que tuvo consecuencias de amplio espectro.

En este contexto de creciente complejidad y sofisticación de las amenazas, tanto de origen natural como humano, la **Ley de Seguridad Nacional** (LSN) [1] emerge como el marco jurídico fundamental para garantizar la protección del Estado y sus ciudadanos. Dicha ley articula el **Sistema de Seguridad Nacional** (SSN), cuyo núcleo operativo se

encuentra en el Departamento de Seguridad Nacional (DSN), y establece la hoja de ruta para la identificación y protección de aquellos activos estratégicos recogidos en el **Catálogo de Infraestructuras Críticas**. La disponibilidad ininterrumpida de estos activos, así como su capacidad de resiliencia ante perturbaciones, constituyen pilares esenciales para la estabilidad y el bienestar de la nación.

El presente trabajo de investigación se erige sobre la premisa de que el apagón del 28 de abril de 2025, actuando como un factor estresor de magnitud considerable, ofrece una oportunidad crítica para analizar la efectividad de las medidas de protección implementadas en el marco de la LSN y su interacción con el **Esquema Nacional de Seguridad** (ENS) [2]. El ENS, como política de seguridad de la información, juega un papel crucial en la protección de los sistemas de información de las infraestructuras críticas, contribuyendo directamente a su disponibilidad y resiliencia. La evaluación del tiempo de recuperación de los servicios esenciales tras el citado evento se convierte, asimismo, en un indicador clave de la robustez del sistema de protección en su conjunto.

A través de un análisis exhaustivo de las interdependencias sectoriales y la respuesta institucional ante la crisis, esta contribución pretende dilucidar las fortalezas y debilidades del marco actual de protección de infraestructuras críticas en España. Se explorará la alineación efectiva entre la LSN, el Catálogo de Infraestructuras Críticas y el ENS, identificando posibles áreas de mejora para fortalecer la resiliencia del país ante futuras amenazas y garantizar la continuidad de los servicios esenciales para la ciudadanía.

Protección de derechos y libertades de los ciudadanos

La intrínseca relación entre la **Constitución Española** (CE) [3] y la **Ley 36/2015, de Seguridad Nacional** [1] radica en que la segunda emana directamente del espíritu y los preceptos fundamentales establecidos en la primera. La Constitución, como norma suprema del ordenamiento jurídico español, sienta las bases del sistema de seguridad del Estado, encomendando a los poderes públicos la garantía de la paz, la seguridad y la libertad de todos los ciudadanos (Título I, Capítulo I). La LSN, por su parte, desarrolla y articula los mecanismos y la estructura organizativa necesarios para hacer efectivo este mandato constitucional en el complejo y dinámico escenario de las amenazas y riesgos contemporáneos.

En primer lugar, la Constitución Española establece en su **artículo 149.1.29ª** la competencia exclusiva del Estado en materia de "seguridad pública", un concepto amplio que la LSN concreta y expande hacia la noción de "Seguridad Nacional". Esta última, definida en el **artículo 2 de la LSN**, abarca las acciones dirigidas a **proteger a España de aquellos actos y omisiones que puedan menoscabar su libertad, soberanía, integridad territorial, intereses vitales y estratégicos, así como la seguridad y bienestar de sus ciudadanos**. Por consiguiente, la LSN se erige como el instrumento legal que vehícula la competencia constitucional del Estado en este ámbito crucial.

En segundo lugar, la LSN se fundamenta en los principios rectores de actuación de los poderes públicos consagrados en la Constitución, tales como la legalidad, la eficacia, la eficiencia, la coordinación y la lealtad institucional (artículo 3 de la LSN). Asimismo, la ley se alinea con los derechos y libertades fundamentales reconocidos en el Título I de la CE. Un ejemplo paradigmático lo encontramos en el **artículo 24 de la LSN**, que regula las limitaciones o prohibiciones de actividades que puedan afectar a la seguridad nacional, estableciendo que estas deberán ser proporcionadas y respetar en todo caso los derechos fundamentales y libertades públicas.

Además, la Constitución Española, en su **artículo 97**, atribuye al Gobierno la dirección de la política interior y exterior, de la Administración civil y militar y la defensa del Estado. La LSN, en coherencia con este precepto, designa al Presidente del Gobierno como la autoridad superior del Sistema de Seguridad Nacional (artículo 17) y le encomienda la dirección y coordinación de las acciones necesarias para garantizar la seguridad de España. El **Consejo de Seguridad Nacional** (CSN), creado por la LSN (artículo 19), se configura como el órgano colegiado de apoyo al Presidente del Gobierno en esta tarea, reflejando la estructura de gobernanza establecida por la Carta Magna.

Por último, la LSN, al definir el ámbito de la Seguridad Nacional y los actores que intervienen en ella (Administraciones Públicas, sector privado y ciudadanía), busca garantizar una respuesta integral y coordinada ante las diversas amenazas y riesgos identificados. Este enfoque holístico se alinea con la concepción de la seguridad como un bien público que requiere la participación y la colaboración de todos los estamentos de la sociedad, tal como se

desprende del espíritu de la Constitución Española en su búsqueda del bienestar general y la protección de los derechos de todos los españoles.

Catálogo de Infraestructuras Críticas.

En el complejo panorama de la seguridad del siglo XXI, caracterizado por la proliferación de amenazas híbridas, la interconexión global y la creciente dependencia de la tecnología, la protección de las infraestructuras críticas emerge como un pilar fundamental para la estabilidad y el bienestar de las naciones. Estas infraestructuras, cuyo funcionamiento ininterrumpido resulta esencial para el mantenimiento de las funciones vitales de la sociedad, abarcan sectores tan diversos como la energía, el transporte, las telecomunicaciones, alimentación, suministro de agua, la sanidad y el sistema financiero, entre otros (figura 1). La materialización de una amenaza sobre alguna de estas infraestructuras puede desencadenar efectos en cascada de consecuencias devastadoras, afectando no solo a la economía y la seguridad pública, sino también a la propia cohesión social.

En este contexto, el **Catálogo Nacional de Infraestructuras Críticas** (CNIC), establecido en el marco de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [4], y desarrollado posteriormente por el Real Decreto 704/2011, de 20 de mayo, [5] se erige como un instrumento central para la identificación y gestión de aquellos activos estratégicos cuya disrupción o destrucción tendría un impacto significativo en la seguridad nacional. El presente artículo tiene como objetivo analizar en profundidad la relación simbiótica existente entre el CNIC, el **Sistema de Seguridad Nacional (SSN)**, articulado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y el **Esquema Nacional de Seguridad (ENS)**, regulado por el Real Decreto 311/2022, de 18 de enero, por el que se aprueba el Esquema Nacional de Seguridad. Se argumentará que el CNIC no opera de forma aislada, sino que constituye un elemento vertebrador que informa y se nutre de ambos sistemas, contribuyendo de manera esencial a la robustez y resiliencia de la nación frente a un espectro cada vez más amplio y sofisticado de amenazas.

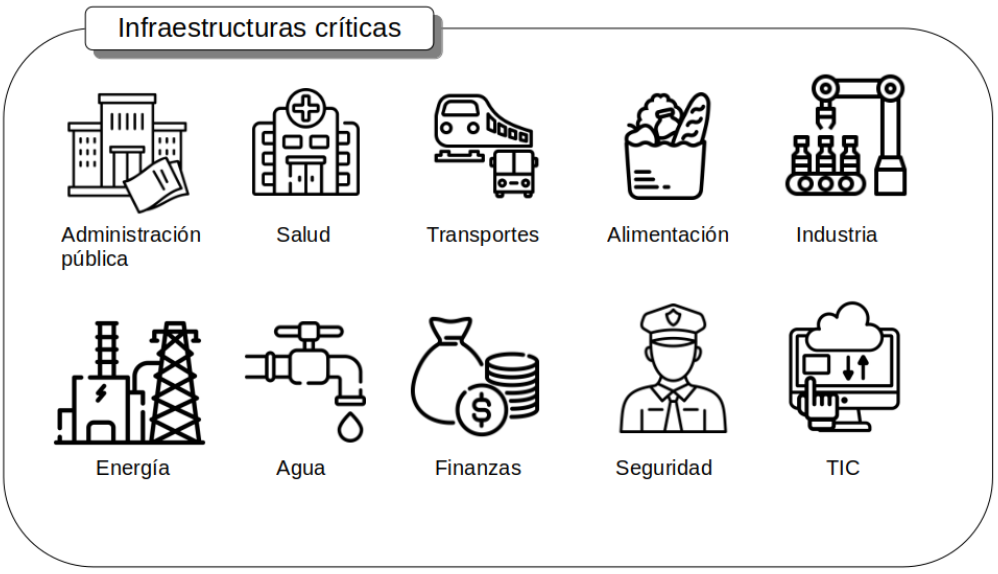


Figura 1. Infaestructuras críticas

Entre las obligaciones de los operadores de las infraestructuras críticas, se encuentran las siguientes:

- Designación de un Responsable de Seguridad y Enlace (RSE): figura clave encargada de la coordinación en materia de seguridad.
- Elaboración de un Plan de Seguridad del Operador (PSO): documento estratégico que establece la política de seguridad del operador.
- Elaboración de Planes de Protección Específicos (PPE): planes tácticos detallados para cada infraestructura crítica, que definen las medidas de seguridad física y lógica.
- Notificación de incidentes de seguridad: obligación de informar sobre cualquier evento que pueda afectar la seguridad de la infraestructura.
- Cooperación con las autoridades competentes: colaboración con el CNPIC y otros organismos relevantes en materia de seguridad.
- Realización de auditorías de seguridad: evaluación periódica de la eficacia de las medidas de seguridad implementadas.

La Ley 8/2011, promueve un enfoque integral de la protección, que abarca tanto la seguridad física (control de accesos, vigilancia, protección perimetral, etc.) como la seguridad lógica o ciberseguridad (protección de sistemas de información, redes de comunicaciones, datos, etc.). Se fomenta la adopción de medidas preventivas, reactivas y de recuperación, así como la gestión de riesgos y la continuidad del negocio. Así mismo, la Ley promueve la colaboración entre el sector público y el sector privado, así como la cooperación a nivel nacional e internacional en materia de protección de infraestructuras críticas.

Sistema de Seguridad Nacional (SSN)

El Sistema de Seguridad Nacional (SSN) se configura como el conjunto de órganos, autoridades, recursos y capacidades integrados para garantizar la seguridad de España y proteger sus intereses vitales. La Ley de Seguridad Nacional establece que l**a protección de las infraestructuras críticas es un componente esencial de la seguridad nacional** (artículo 4.2.d), reconociendo explícitamente la **necesidad de asegurar su funcionamiento ininterrumpido**.

El **CNIC** desempeña un papel fundamental dentro del SSN al proporcionar la base para la planificación y la ejecución de las políticas de seguridad en este ámbito. La identificación de las infraestructuras críticas permite al Consejo de Seguridad Nacional, como órgano coordinador del SSN, **evaluar los riesgos y amenazas** que las acechan, así como **definir las líneas estratégicas de actuación**. Asimismo, el CNIC facilita la coordinación entre los diferentes ministerios y organismos con competencias en la protección de infraestructuras críticas, promoviendo una respuesta integral y coherente ante posibles incidentes.

La LSN también establece la figura de los operadores críticos, entidades responsables de la gestión y operación de las infraestructuras incluidas en el CNIC, y les impone una serie de obligaciones en materia de seguridad, incluyendo la elaboración de planes de seguridad del operador (PSO) y la designación de un delegado de seguridad. El CNIC, por tanto, no solo identifica los activos a proteger, sino que también delimita las responsabilidades de los actores clave en su salvaguarda dentro del marco del SSN.

La resiliencia, entendida como la capacidad de un sistema para resistir, absorber, adaptarse y recuperarse de las perturbaciones, **es un objetivo fundamental de la seguridad nacional**. El CNIC, al identificar los activos estratégicos y establecer las bases para su protección a través de su vinculación con el SSN y el ENS, juega un papel crucial en el fortalecimiento de la resiliencia del país. **La identificación de las interdependencias entre las diferentes infraestructuras críticas**, un aspecto cada vez más relevante en la gestión de riesgos, se facilita a través del CNIC. Comprender cómo el fallo en una infraestructura puede propagarse a otras es esencial para desarrollar estrategias de mitigación efectivas y planes de contingencia robustos, asegurando así la continuidad de los servicios. El CNIC, al proporcionar una visión holística de los activos estratégicos, permite analizar estas interdependencias y fortalecer la resiliencia del sistema en su conjunto.

El **artículo 5 de la LSN** enumera los principios rectores de la actuación de los poderes públicos en materia de seguridad nacional, entre los que destacan:

- **El principio de anticipación:** que implica la detección temprana de riesgos y amenazas para adoptar medidas preventivas.
- **El principio de prevención:** el cual exige la adopción de medidas para evitar o minimizar los riesgos y amenazas identificados.
- **El principio de resiliencia:** que hace referencia a la capacidad del sistema para resistir y recuperarse ante las crisis.
- **El principio de responsabilidad:** que impone a las autoridades y organismos competentes la obligación de actuar con diligencia en la gestión de la seguridad nacional.

Además, la LSN, en su **Título II**, establece la estructura del Sistema de Seguridad Nacional (SSN) y las responsabilidades de los diferentes órganos y autoridades. El **Consejo de Seguridad Nacional (CSN)**, como órgano colegiado presidido por el Presidente del Gobierno, tiene entre sus funciones analizar y evaluar los riesgos y amenazas para la seguridad nacional y proponer las directrices para su gestión. El artículo 29 de la LSN se refiere específicamente a la contribución de los operadores críticos a la seguridad nacional, imponiéndoles la obligación de adoptar las medidas de seguridad necesarias para garantizar la protección de sus infraestructuras y servicios.

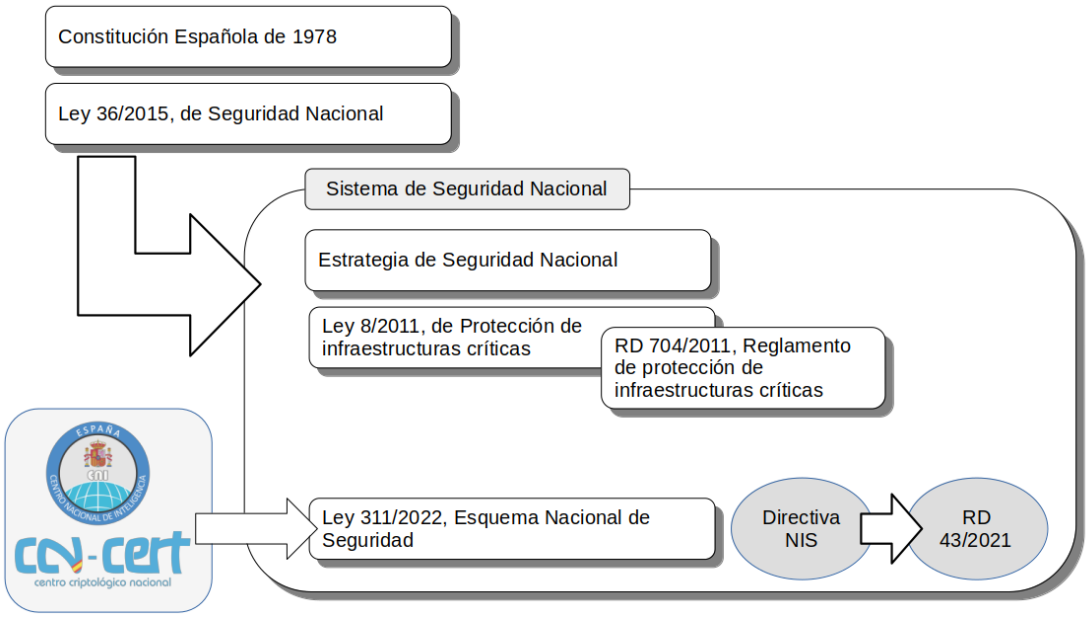


Figura 2. Legislación relacionada con el Sistema de Seguridad Nacional

Estrategia de Seguridad Nacional

Es relevante el hecho de la importancia que se le atribuye al ciberespacio y la infraestructura digital dentro de la Estrategia de Seguridad Nacional 2019 [7], relacionando amenazas, tanto actuales como emergentes. La Estrategia de Seguridad Nacional 2019 se asienta sobre los principios rectores de la Estrategia de Seguridad Nacional 2017, aplicados al ámbito de la ciberseguridad. Estos principios buscan garantizar una acción integral y eficaz en un entorno dinámico y complejo:

- **Unidad de acción:** implica la necesidad de una coordinación y colaboración estrecha entre todos los actores involucrados (administraciones públicas, sector privado, ciudadanía) para asegurar una respuesta cohesionada y eficiente ante los desafíos de ciberseguridad. Se busca evitar la duplicidad de esfuerzos y optimización de los recursos.

- **Anticipación:** resalta la importancia de la proactividad en la identificación de amenazas y riesgos emergentes en el ciberespacio. La capacidad de anticipar escenarios futuros y preparar respuestas adecuadas es crucial para minimizar el impacto de posibles incidentes.
- **Eficiencia:** se refiere a la optimización de los recursos disponibles (humanos, técnicos, económicos) para lograr los máximos resultados en la protección del ciberespacio. Esto implica la gestión inteligente de las capacidades y la priorización de las acciones más efectivas.
- **Resiliencia:** consiste en la capacidad de los sistemas, infraestructuras y la sociedad en general para resistir, adaptarse y recuperarse rápidamente de ciberataques o **incidentes significativos**. Es fundamental asegurar la continuidad de los servicios esenciales y la vuelta a la normalidad en el menor tiempo posible. Principio altamente relacionado con la dimensión de la disponibilidad.

Se establecen cinco objetivos específicos, alineados con los principios rectores y concebidos para fortalecer la ciberseguridad en España:

1. **Reforzar la prevención, detección, protección, respuesta y recuperación de los ciberataques y otras amenazas del ciberespacio.** Este es el objetivo central y más amplio, abarcando todo el ciclo de vida de la gestión de incidentes de ciberseguridad. Se busca mejorar las capacidades en cada una de estas fases para minimizar el impacto de las amenazas.
2. **Impulsar una cultura de ciberseguridad que involucre a todos los actores.** Similar al principio de "cultura de Seguridad Nacional", este objetivo busca concienciar y capacitar a la sociedad, las empresas y las administraciones públicas sobre la importancia de la ciberseguridad, promoviendo hábitos seguros y una participación activa.
3. **Fomentar la investigación, el desarrollo y la innovación (I+D+i) en ciberseguridad y las capacidades industriales y tecnológicas propias.** Reconociendo la naturaleza cambiante de las amenazas, este objetivo busca promover la generación de conocimiento y soluciones tecnológicas nacionales en ciberseguridad, reduciendo la dependencia exterior y creando un ecosistema innovador.
4. **Fortalecer la capacidad de disuasión y respuesta frente a ciberataques de alta intensidad y procedencia estatal.** Este objetivo aborda las amenazas más sofisticadas y de mayor impacto, buscando desarrollar capacidades específicas para detectar, atribuir y responder eficazmente a ataques complejos que puedan afectar a la seguridad nacional.
5. **Promover la cooperación y colaboración internacional en ciberseguridad.** Dada la naturaleza global del ciberespacio, este objetivo subraya la necesidad de establecer y mantener alianzas con otros países y organizaciones internacionales para compartir información, coordinar respuestas y desarrollar marcos normativos comunes que contribuyan a un ciberespacio más seguro y estable a nivel global.

En la Estrategia de Seguridad Nacional 2021 [8], incluye como novedades las siguientes:

- ✔ **Refuerzo de la gestión de crisis:** desarrollo de un modelo de gestión de crisis con mayor capacidad de anticipación y basado en el análisis de datos.
- ✔ **Plan Integral de Seguridad para Ceuta y Melilla:** una de las novedades específicas, motivada por las crisis migratorias y la necesidad de una estrategia de seguridad integral para estas ciudades.
- ✔ **Creación de una reserva estratégica basada en capacidades nacionales de producción industrial:** una lección derivada de la pandemia para garantizar el suministro de bienes esenciales.
- ✔ **Mayor integración de las capacidades tecnológicas:** se enfatiza el uso de inteligencia artificial y la mecanización de procesos para la prevención y alerta temprana.
- ✔ **Agencia Espacial Española:** aunque no detallada directamente en la ESN 2021, la Estrategia sienta las bases para el desarrollo de capacidades en el ámbito espacial.

Otro aspecto importante y que también supone una novedad y sobre todo por su relación con el trabajo actual, es el enfoque anticipatorio y de resiliencia, donde se resalta la necesidad de prevenir y adaptarse a los riesgos, construyendo una sociedad resiliente.

Gestión de crisis

La **Situación de Interés para la Seguridad Nacional (SINS)**, tal como se define en el **Título III de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional** [1], constituye un mecanismo legal de carácter excepcional que puede ser declarado por el **Presidente del Gobierno** mediante Real Decreto. Su activación se fundamenta en la concurrencia de circunstancias extraordinarias que, por la gravedad de sus efectos, su dimensión territorial o funcional, su urgencia y su carácter transversal, exigen una coordinación reforzada de las autoridades competentes en el ejercicio de sus atribuciones ordinarias. En esencia, la SINS se declara cuando una crisis o amenaza específica, por su naturaleza e impacto potencial, desborda las capacidades de gestión ordinarias de las administraciones sectoriales y requiere una **dirección centralizada y una colaboración intensificada** entre los diferentes poderes públicos y organismos del Estado para su resolución eficaz.

Los elementos clave que definen la Situación de Interés para la Seguridad Nacional son:

- **Gravedad de los efectos:** donde la crisis o amenaza debe tener un impacto significativo en la seguridad, los derechos y libertades de los ciudadanos, el funcionamiento de las instituciones, los servicios esenciales o los intereses vitales de España.
- **Dimensión:** que puede ser territorialmente extensa o funcionalmente transversal, impactando a múltiples sectores o ámbitos de la vida nacional.
- **Urgencia:** referida a la necesidad de una respuesta rápida y coordinada es primordial para mitigar los efectos de la crisis o amenaza.
- **Transversalidad:** elemento clave en la gestión de la situación que requiere la implicación y la coordinación de diversas autoridades y administraciones públicas en el ejercicio de sus competencias.

Es crucial destacar que la declaración de este tipo de situación se realiza sin que ello implique la suspensión de los derechos fundamentales y libertades públicas de los ciudadanos.

Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS) **establece la política de seguridad de la información** aplicable a las administraciones públicas y a las entidades privadas que presten servicios públicos o gestionen información clasificada. Dada la creciente digitalización y la interconexión de las infraestructuras críticas, la ciberseguridad se ha convertido en un elemento crucial de su protección. **El ENS, a través de sus principios básicos, requisitos de seguridad y directrices, proporciona un marco normativo y técnico para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los sistemas de información de las infraestructuras críticas**. La aplicación del ENS por parte de los operadores críticos contribuye directamente a la resiliencia de estas infraestructuras frente a ciberataques e incidentes de diversa índole.

La relación entre el CNIC y el ENS se manifiesta en la necesidad de que los operadores críticos implementen las medidas de seguridad establecidas en el ENS para proteger sus sistemas de información y comunicaciones. La inclusión de una infraestructura en el CNIC implica, por lo tanto, la obligación de cumplir con los requisitos del ENS en lo referente a la **seguridad de sus activos digitales**. Esta convergencia normativa asegura que la protección de las infraestructuras críticas abarque tanto la seguridad física como la digital, reconociendo la creciente superposición entre ambos dominios.

La dependencia de los sistemas de información y las redes de comunicaciones es inherente al funcionamiento de las infraestructuras críticas. Desde los sistemas de control industrial en las plantas de energía hasta las plataformas de gestión de datos en el sector financiero y sanitario, la ciberseguridad se ha convertido en un factor crítico para garantizar la disponibilidad, la integridad y la confidencialidad de estos activos. El ENS se erige como la política de seguridad de la información que debe aplicarse a las Administraciones Públicas y a las entidades privadas que presten servicios públicos o gestionen información clasificada. Dada la naturaleza esencial de los servicios proporcionados por las infraestructuras críticas, y la creciente sofisticación de las ciberamenazas, la adopción y la implementación efectiva del ENS por parte de los operadores críticos resulta fundamental para fortalecer su ciberresiliencia.

La relación entre el SSN y el ENS se manifiesta en la integración de la ciberseguridad como un componente transversal de la seguridad nacional. El Consejo de Seguridad Nacional, en sus estrategias y planes, incorpora la necesidad de proteger el ciberespacio y garantizar la seguridad de los sistemas de información críticos. El ENS, con sus principios básicos, requisitos de seguridad y directrices, proporciona el marco normativo y técnico para alcanzar este objetivo en el ámbito de las infraestructuras críticas. La obligación para los operadores críticos de cumplir con el ENS, especialmente en lo referente a la gestión de riesgos, la implementación de medidas de seguridad y la notificación de incidentes, contribuye directamente a la resiliencia del SSN frente a las ciberamenazas.

La colaboración entre el Centro Criptológico Nacional (CCN), como autoridad nacional en materia de ciberseguridad, y el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), como centro de coordinación para la protección de las infraestructuras críticas, ejemplifica la sinergia entre el ENS y el SSN en este ámbito crucial. Esta colaboración se materializa en la elaboración de guías y recomendaciones específicas para la ciberseguridad de las Infraestructuras críticas, la realización de ejercicios conjuntos y el intercambio de información sobre amenazas y vulnerabilidades.

Dimensión de disponibilidad en el contexto de la seguridad

Las dimensiones fundamentales de la seguridad informática, a menudo referidas como la **Tríada CID**, comprenden tres pilares esenciales para la protección de la información y los sistemas que la procesan:

1. **Confidencialidad:** esta dimensión se refiere a la necesidad de asegurar que la información sensible sea accesible únicamente a las entidades (personas, procesos o sistemas) autorizadas. Implica la implementación de mecanismos de control de acceso, cifrado de datos, autenticación robusta y anonimización para prevenir la divulgación no autorizada de información. El objetivo es preservar la privacidad y evitar que datos críticos caigan en manos equivocadas.
2. **Integridad:** garantiza que la información se mantenga precisa, completa y sin alteraciones no autorizadas. Implica la implementación de mecanismos para detectar y prevenir modificaciones, eliminaciones o adiciones no autorizadas a los datos, ya sean accidentales o maliciosas. El uso de sumas de verificación, firmas digitales, control de versiones y auditorías son ejemplos de medidas para mantener la integridad de la información y asegurar su fiabilidad.
3. **Disponibilidad:** se centra en asegurar que los usuarios autorizados tengan acceso a la información y a los recursos del sistema cuando los necesiten. Implica la implementación de medidas para prevenir interrupciones del servicio, garantizar la continuidad operativa y facilitar la recuperación ante fallos o desastres. La redundancia de sistemas, los planes de contingencia, las copias de seguridad y los sistemas de detección y prevención de ataques de denegación de servicio (DDoS) son cruciales para mantener la disponibilidad.

Si bien la Tríada CID constituye el núcleo fundamental, algunas extensiones y modelos consideran dimensiones adicionales como la autenticidad (garantizar la identidad de las entidades), la trazabilidad (mantener un registro de las acciones realizadas), y el no repudio (asegurar que una entidad no pueda negar una acción realizada). No obstante, la Confidencialidad, la Integridad y la Disponibilidad siguen siendo los pilares conceptuales sobre los que se construye la disciplina de la seguridad informática. Las dimensiones fundamentales de la seguridad informática

que hemos delineado – Confidencialidad, Integridad y Disponibilidad – son absolutamente extensibles y de crucial aplicación en el contexto de la seguridad de las infraestructuras críticas. Sin embargo, su aplicación y las prioridades relativas pueden presentar matices específicos debido a la naturaleza operativa y las consecuencias potenciales de una disrupción en estos sistemas esenciales.

A continuación se analiza la extensión de cada dimensión al ámbito de las infraestructuras críticas:

1. **Confidencialidad en Infraestructuras Críticas:** la protección de la información sensible es igualmente vital en este contexto. Esto incluye la salvaguarda de planos de las instalaciones, protocolos operativos, información sobre vulnerabilidades, datos de control de procesos industriales, información sobre la red de distribución (eléctrica, gas, agua, etc.) y datos personales de usuarios de servicios esenciales. La divulgación no autorizada de esta información podría ser explotada por actores maliciosos para planificar ataques físicos o cibernéticos, o para comprometer la integridad y la disponibilidad de la infraestructura.
2. **Integridad en Infraestructuras Críticas:** la integridad adquiere una relevancia aún mayor si cabe. La manipulación no autorizada de los sistemas de control industrial, de los datos de telemetría o de la configuración de los equipos podría tener consecuencias catastróficas, provocando fallos operativos, daños físicos a gran escala, interrupciones masivas del suministro o incluso poner en riesgo la seguridad de las personas y el medio ambiente. Garantizar la integridad implica implementar mecanismos robustos para la detección de intrusiones, la validación de comandos, el control de cambios y la auditoría de las operaciones.

3. **Disponibilidad en Infraestructuras Críticas:** se convierte en un imperativo crítico. La interrupción del funcionamiento de una infraestructura crítica, ya sea por un ciberataque, un fallo técnico o un evento físico, puede tener consecuencias devastadoras a nivel social, económico y de seguridad nacional. Por lo tanto, asegurar la continuidad operativa y la rápida recuperación ante incidentes es primordial. Esto exige la implementación de arquitecturas redundantes, planes de contingencia y recuperación ante desastres específicos para cada tipo de amenaza, y la capacidad de mantener las funciones esenciales incluso bajo condiciones adversas.

Debemos introducir un nuevo concepto, el **factor estresor** y que es aquel elemento que **desafía o excede la capacidad de un individuo o sistema para mantener su estado de equilibrio interno** [10]. La intensidad y la duración de la exposición al factor estresor son determinantes importantes de la magnitud y la naturaleza de la respuesta de estrés. Un factor estresor breve y de baja intensidad puede generar una respuesta adaptativa, mientras que un factor estresor intenso o prolongado puede ser perjudicial y conducir a la sobrecarga y al agotamiento del sistema. Los efectos de múltiples factores estresores pueden ser aditivos o incluso sinérgicos, lo que significa que la exposición simultánea a varios estresantes, aunque cada uno individualmente pueda parecer menor, puede generar una respuesta de estrés significativa.

En el contexto de nuestro trabajo, podemos identificar factores estresores específicos que afectan a los sistemas y a las organizaciones en el ciberespacio:

- ✗ **Ataques cibernéticos**: intentos maliciosos de acceder, dañar o interrumpir sistemas de información.
- ✗ **Fallos de hardware o software**: errores inesperados que comprometen la funcionalidad de los sistemas.
- ✗ **Errores humanos**: acciones no intencionadas por parte de usuarios o administradores que causan problemas de seguridad o disponibilidad.
- ✗ **Sobrecarga de la red o de los sistemas**: demandas excesivas de recursos que degradan el rendimiento.
- ✗ **Vulnerabilidades de seguridad**: debilidades en el diseño o la implementación de sistemas que pueden ser explotadas.
- ✗ **Cambios tecnológicos disruptivos**: la necesidad constante de adaptación a nuevas tecnologías y amenazas.

La comprensión de los factores estresores es fundamental para el diseño de sistemas resilientes y para la implementación de estrategias de gestión del estrés tanto a nivel individual como organizacional. Al identificar los

posibles factores estresores, podemos desarrollar mecanismos para prevenirlos, mitigar su impacto o facilitar la recuperación ante su ocurrencia.

Un fallo en el suministro eléctrico puede tener consecuencias directas y significativas en la disponibilidad y el funcionamiento de los sistemas de información, comunicaciones y otras infraestructuras. Servidores, equipos de red, sistemas de seguridad y otros componentes críticos dependen de una alimentación eléctrica estable. La capacidad de una organización para mantener la operatividad de sus servicios ante un fallo eléctrico (a través de sistemas de alimentación ininterrumpida, generadores de respaldo, o arquitecturas resilientes que puedan conmutar a fuentes de energía alternativas) es un aspecto importante de la resiliencia operativa, que está estrechamente relacionada con la ciberresiliencia. Un fallo eléctrico que cause la caída de sistemas de seguridad o la pérdida de datos críticos podría exacerbar las consecuencias de un ciberataque posterior o dificultar la recuperación tras un incidente cibernético previo.

La infraestructura eléctrica es considerada una infraestructura crítica, y su disponibilidad es fundamental para el funcionamiento de otros sectores. La ciberresiliencia de una organización depende, en cierta medida, de la resiliencia de las infraestructuras de las que depende, incluyendo el suministro eléctrico. Por lo tanto, las estrategias de ciberresiliencia deben considerar las posibles interrupciones en servicios esenciales como la electricidad y planificar la continuidad operativa en tales escenarios. **Aunque un fallo eléctrico en su origen no sea un incidente cibernético, su potencial como causa o consecuencia de un incidente cibernético, así como su impacto en la infraestructura digital, lo convierte en un factor relevante a considerar dentro de una estrategia integral de ciberresiliencia**. La capacidad de mantener la continuidad operativa de los sistemas de información ante interrupciones del suministro eléctrico, ya sea por causas físicas o cibernéticas, es un componente importante de la resiliencia general de una organización en el ciberespacio.

En el ámbito de la ingeniería de sistemas complejos y la seguridad de infraestructuras críticas, el concepto de "cero energético" [11] se define inequívocamente como el colapso sistémico y generalizado de la red eléctrica a escala nacional o de una extensa región geográfica. Este fenómeno trasciende la mera ocurrencia de cortes de suministro localizados o sectoriales, caracterizándose por la interrupción total y simultánea del flujo de energía eléctrica, dejando sin servicio a millones de usuarios y paralizando la operatividad de funciones esenciales. La magnitud y el alcance de un evento de "cero energético" implican una disfunción profunda de la infraestructura eléctrica, diferenciándose cualitativamente de las fluctuaciones o interrupciones parciales que pueden afectar a áreas geográficas delimitadas.

La relación entre el **sector energético** y el **ENS** es de una interdependencia crítica y bidireccional, fundamental para garantizar la seguridad nacional, la continuidad del suministro y la protección de la información sensible en un sector estratégico de vital importancia. Esta relación se fundamenta en la creciente digitalización del sector energético y en la consideración de sus infraestructuras como infraestructuras críticas.

En primer lugar, el sector energético se ve directamente afectado por el **ENS** en su calidad de proveedor de servicios esenciales y gestor de infraestructuras críticas. La normativa del ENS, es de obligado cumplimiento para las entidades públicas y privadas que presten servicios públicos o gestionen información clasificada. Dado que la producción, el transporte, la distribución y la comercialización de energía son servicios esenciales para el funcionamiento del país, las empresas y organismos que operan en este sector están sujetos a las exigencias del ENS. Esta sujeción implica la necesidad de implementar las **medidas de seguridad** establecidas en el ENS para garantizar la **disponibilidad**, la **integridad**, la **confidencialidad**, la **autenticidad** y la **trazabilidad** de sus sistemas de información. Esto abarca desde los sistemas de control industrial que gestionan las plantas de generación y las redes de distribución, hasta los sistemas de gestión empresarial, los sistemas de comunicación y la información de los clientes. Un fallo de seguridad en cualquiera de estos sistemas podría tener consecuencias graves, que van desde la interrupción del suministro energético hasta el acceso no autorizado a información sensible sobre la infraestructura o los procesos operativos. En este sentido, el ENS proporciona un marco de referencia robusto y armonizado para la **gestión de la seguridad de la información** en el sector energético. Su estructura, basada en principios, requisitos y medidas de seguridad organizativas y técnicas, permite a las entidades del sector establecer un sistema de gestión de la seguridad de la información eficaz y adaptado a sus riesgos específicos. La categorización de los sistemas de

información según su impacto potencial (bajo, medio o alto) permite priorizar las medidas de seguridad a implementar, asegurando una asignación eficiente de recursos.

Por otro lado, el **sector energético** también influye en la concepción y la aplicación del **ENS**. El factor crítico de sus infraestructuras y la potencialidad de un ciberataque con consecuencias a gran escala han llevado a considerar al sector energético como un ámbito de especial atención en las políticas de seguridad de la información a nivel nacional. Las particularidades de los sistemas de control industrial y la Tecnología Operacional (OT), que a menudo difieren significativamente de los sistemas de Tecnologías de la Información (TI) tradicionales en términos de protocolos, ciclo de vida y requisitos de disponibilidad, han requerido una adaptación y una especialización de las medidas de seguridad del ENS. Organismos como el **Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)** y el **Centro Criptológico Nacional (CCN)** colaboran estrechamente con las empresas del sector energético para desarrollar guías, recomendaciones y buenas prácticas específicas para la aplicación del ENS en sus entornos operativos. Se promueve la concienciación sobre los riesgos cibernéticos específicos del sector energético (como ataques a sistemas SCADA - Supervisory Control And Data Acquisition - , manipulación de datos de contadores inteligentes o intrusiones en redes de distribución) y se fomenta la adopción de medidas de seguridad proactivas y la colaboración en la respuesta a incidentes.

De aquí obtenemos las características de la relación existente entre el sector energético y el ENS:

- **Obligatoriedad.** Ya que las entidades del sector energético que prestan servicios esenciales están obligadas a cumplir con el ENS para proteger sus sistemas de información.
- **Criticidad.** Esta característica en el sector energético lo convierte en un ámbito de especial atención dentro de las políticas de seguridad de la información del ENS.
- **Adaptación.** Especial mención a las particularidades de los sistemas de control industrial del sector energético requieren una adaptación y especialización de las medidas de seguridad del ENS.
- **Colaboración.** Se hace más que necesaria una estrecha colaboración entre las entidades del sector energético, el CNPIC y el CCN para facilitar la aplicación del ENS y mejorar la ciberseguridad del sector.
- **Resiliencia.** Para una correcta implementación del ENS en el sector energético que contribuye significativamente a la resiliencia de las infraestructuras críticas y, por ende, a la seguridad nacional.

La relación entre la **disponibilidad** y la norma **ISO 22301: Sistemas de Gestión de la Continuidad del Negocio** [9] es fundamental e intrínseca. La ISO 22301 se centra precisamente en asegurar que una organización pueda mantener sus operaciones en niveles predefinidos tras la ocurrencia de incidentes disruptivos, y la disponibilidad de los servicios críticos es un componente esencial de este objetivo.

El objetivo primordial de la norma ISO 22301 es establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Continuidad del Negocio (SGCN). Este sistema busca proteger a la organización contra interrupciones, reducir la probabilidad de su ocurrencia, preparar la respuesta ante ellas y asegurar la recuperación de las operaciones críticas en el menor tiempo posible. La disponibilidad de estas operaciones críticas es, por lo tanto, un resultado directo que se persigue a través de la implementación de la norma.

La continuidad del negocio, en esencia, se trata de garantizar que los productos, servicios y operaciones esenciales de una organización estén **disponibles** para sus clientes, partes interesadas y para la propia organización, incluso en situaciones adversas. Un SGCN eficaz, conforme a la ISO 22301, debe identificar los procesos críticos y establecer los controles y planes necesarios para asegurar su disponibilidad durante y después de una interrupción.

Diversos requisitos de la norma ISO 22301 están directamente orientados a garantizar o restablecer la **disponibilidad**:

- Análisis de Impacto en el Negocio (BIA - Business Impact Analysis): esta tarea identifica los procesos críticos de la organización y evalúa el impacto que su interrupción tendría en términos financieros, operacionales, legales, reputacionales, etc. Un resultado clave del BIA es la definición de los objetivos de tiempo de recuperación (RTO - Recovery Time Objective) y los objetivos de punto de recuperación (RPO - Recovery

Point Objective) para cada proceso crítico. El RTO es el tiempo máximo tolerable para restaurar la disponibilidad de un proceso tras una interrupción.

- Estrategias de Continuidad del Negocio: la norma exige el desarrollo de estrategias para asegurar la continuidad de los procesos críticos, las cuales a menudo implican la implementación de soluciones para mantener la disponibilidad de los recursos necesarios (infraestructura tecnológica, personal, instalaciones, información, etc.).
- Planes de Continuidad del Negocio (BCP - Business Continuity Plans): son planes que detallan los procedimientos y las acciones específicas que se deben llevar a cabo para restaurar y mantener la disponibilidad de los procesos críticos tras una interrupción. Incluyen pasos para la activación del plan, la comunicación, la recuperación de sistemas y datos, y la reanudación de las operaciones.
- Pruebas y Ejercicios: la norma ISO 22301 requiere que se realicen pruebas y ejercicios periódicos de los planes de continuidad para verificar su eficacia y asegurar que la organización es capaz de restaurar la disponibilidad de sus servicios dentro de los RTO definidos.
- Mantenimiento y Mejora Continua: el SGCN debe ser revisado y actualizado de forma continua para asegurar su relevancia y eficacia en el tiempo, lo que incluye la adaptación de las medidas de disponibilidad a los cambios en la organización y en su entorno.

Aunque la ISO 22301 se centra en la continuidad del negocio, la disponibilidad es también un principio fundamental de la seguridad de la información, tal como se menciona en otras normas como la ISO 27001 y el Esquema Nacional de Seguridad (ENS). La ISO 22301 aborda la **disponibilidad** desde una perspectiva de resiliencia organizacional ante incidentes, lo que complementa las medidas de seguridad de la información que buscan prevenir la pérdida de disponibilidad por causas como fallos técnicos, errores humanos o ciberataques.

Es por tanto, la disponibilidad un pilar central de la continuidad del negocio, y la norma ISO 22301 proporciona un marco estructurado para que las organizaciones gestionen los riesgos y establezcan las capacidades necesarias para mantener la disponibilidad de sus operaciones críticas frente a una amplia gama de posibles interrupciones. La implementación de un SGCN conforme a esta norma contribuye significativamente a fortalecer la resiliencia de una organización y a asegurar la disponibilidad de los servicios de los que depende.

Conclusiones

El evento sin precedentes del apagón nacional del 28 de abril de 2025 ha servido como un catalizador ineludible para la reevaluación profunda de la resiliencia y disponibilidad de las infraestructuras críticas en España. Este suceso, lejos de ser un incidente aislado de interrupción del suministro eléctrico, ha evidenciado la intrínseca vulnerabilidad sistémica que subyace en la compleja interconexión de los servicios esenciales que sustentan la sociedad moderna. La capacidad de estos servicios para mantener su operatividad no es solo una cuestión de eficiencia, sino una dimensión fundamental de la Seguridad Nacional. En este contexto, la disponibilidad del sector eléctrico emerge como un pilar ineludible de la seguridad y el bienestar. El análisis de los requisitos de protección en el marco de la Ley de Seguridad Nacional y su interacción con el Esquema Nacional de Seguridad revela que, a pesar de los esfuerzos normativos y técnicos, persisten desafíos significativos para garantizar una disponibilidad continua y robusta. La interdependencia entre el suministro eléctrico y el funcionamiento de otros sectores críticos, como las comunicaciones, el transporte, la sanidad o los sistemas financieros, magnifica el impacto de cualquier interrupción en la cadena de valor de la energía. Un fallo en la red eléctrica no solo detiene el flujo de suministro eléctrico, sino que puede desencadenar una cascada de disrupciones con consecuencias socioeconómicas y humanitarias severas. La Estrategia Nacional de Ciberseguridad 2019, si bien establece principios rectores y objetivos claros para fortalecer la ciberseguridad, subraya la necesidad de una adaptación continua y una dotación de recursos adecuada. Es imperativo que estas directrices se traduzcan en medidas concretas que refuercen la dimensión preventiva y de respuesta del Sistema Nacional de Protección de Infraestructuras Críticas, con un foco particular en el sector eléctrico. La implementación y validación constante de planes de continuidad del negocio, la mejora de las capacidades de disuasión y respuesta ante ciberataques de alta intensidad –especialmente aquellos dirigidos a la infraestructura energética–, y el fomento de una sólida cultura de ciberseguridad en todos los niveles, son pasos

esenciales. En definitiva, la experiencia del apagón de 2025 refuerza la premisa de que la disponibilidad eléctrica no es un lujo, sino una condición *sine qua non* para la estabilidad y el desarrollo. Tanto la consideración de las alertas tempranas, indicadores de compromiso, como de la inversión en resiliencia del sector eléctrico, mediante la adopción de tecnologías avanzadas, la promoción de microrredes, el desarrollo de capacidades de operación en modo isla, y una gestión proactiva de riesgos cibernéticos, debe ser una prioridad estratégica. Solo así se podrá mitigar la vulnerabilidad inherente y asegurar que España esté preparada para afrontar los desafíos futuros en un entorno de amenazas cada vez más sofisticado y globalizado, garantizando la operatividad esencial de sus infraestructuras críticas.

Referencias bibliográficas

[1] *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.* Recuperado 12 de mayo de 2025, de https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389

[2] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado, 4 de mayo de 2022. Núm 106. https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

[3] *Constitución Española.* Boletín Oficial del Estado, 29 de diciembre de 1978. núm 311. https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[4] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.* (s. f.). Recuperado 12 de mayo de 2025, de https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

[5] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* Boletín Oficial del Estado, 21 de mayo de 2011. Núm 121. https://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf

[6] Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. Boletín Oficial del Estado, 31 de diciemjbre de 2021. Núm 314. https://www.boe.es/boe/dias/2021/12/31/pdfs/BOE-A-2021-21884.pdf

[7] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. Boletín Oficial del Estado, 30 de abril de 2019. Núm 103.

[8] Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. Boletín Oficial del Estado. Núm. 314.

[9] *UNE-EN ISO 22301:2020 Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio.* https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0063818

[10] Selye, H. (1956). *The Stress of Life*. McGraw-Hill.

[11] Parhizi, S., Lotfi, H., Khodaei, A., & Bahramipanah, S. (2015). State of the Art in Microgrid Activity. *IEEE Transactions on Smart Grid*, *6*(2), 893-905.

Biografía del autor.

Francisco José de Haro Olmo (Almería, 1974), es Doctor en Informática por la Universidad Almería y Máster en Criminología por la UNED. Funcionario de Carrera del Estado perteneciente al cuerpo de Profesores de Enseñanza Secundaria, especialidad de Sistemas y Aplicaciones Informáticas, con destino en I.E.S. Celia Viñas. Imparte docencia en formación profesional desde 2001, Colabora con la Universidad de Almería a través de la docencia en el Grado de Ingeniería Informática y en el Máster en Tecnologías y Aplicaciones en Ingeniería Informática. Entre 2016 y 2020 formó parte de la Red Andaluza de Formación del Profesorado como Asesor Provincial de Formación Profesional, implicándose en proyectos internacionales relacionados con la formación profesional y la transformación digital. Desde 2022 es miembro del Consejo Provincial del Instituto de Estudios Almerienses, área de Ciencias Sociales.