T5 FALLO DE INFRAESTRUCTURAS CRÍTICAS

DESCRIPCIÓN

Las infraestructuras críticas son todos aquellos sistemas, físicos o virtuales, que facilitan funciones y servicios esenciales y estratégicos para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. Cualquier alteración o interrupción en los servicios proporcionados por estas infraestructuras de sectores estratégicos, debido a causas naturales o deliberadas, podría provocar la paralización o menoscabo de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad.

¿Qué está pasando en España?

La oleada de ataques yihadistas marcados por el fatídico 11-S de 2001 en Estados Unidos o el 11-M de 2004 en España provocó, en Europa, una fuerte preocupación por la seguridad de las infraestructuras críticas y la prestación de los servicios esenciales. Ello se tradujo en el ámbito europeo en la aprobación del programa para la protección de las infraestructuras críticas europeas en 2006, seguido de la Directiva 2008/114/CE, que se transpuso al ordenamiento jurídico español dos años más tarde como Ley 8/2011 -popularmente conocida como Ley PIC- y en la que se establecieron medidas para la protección de infraestructuras críticas.

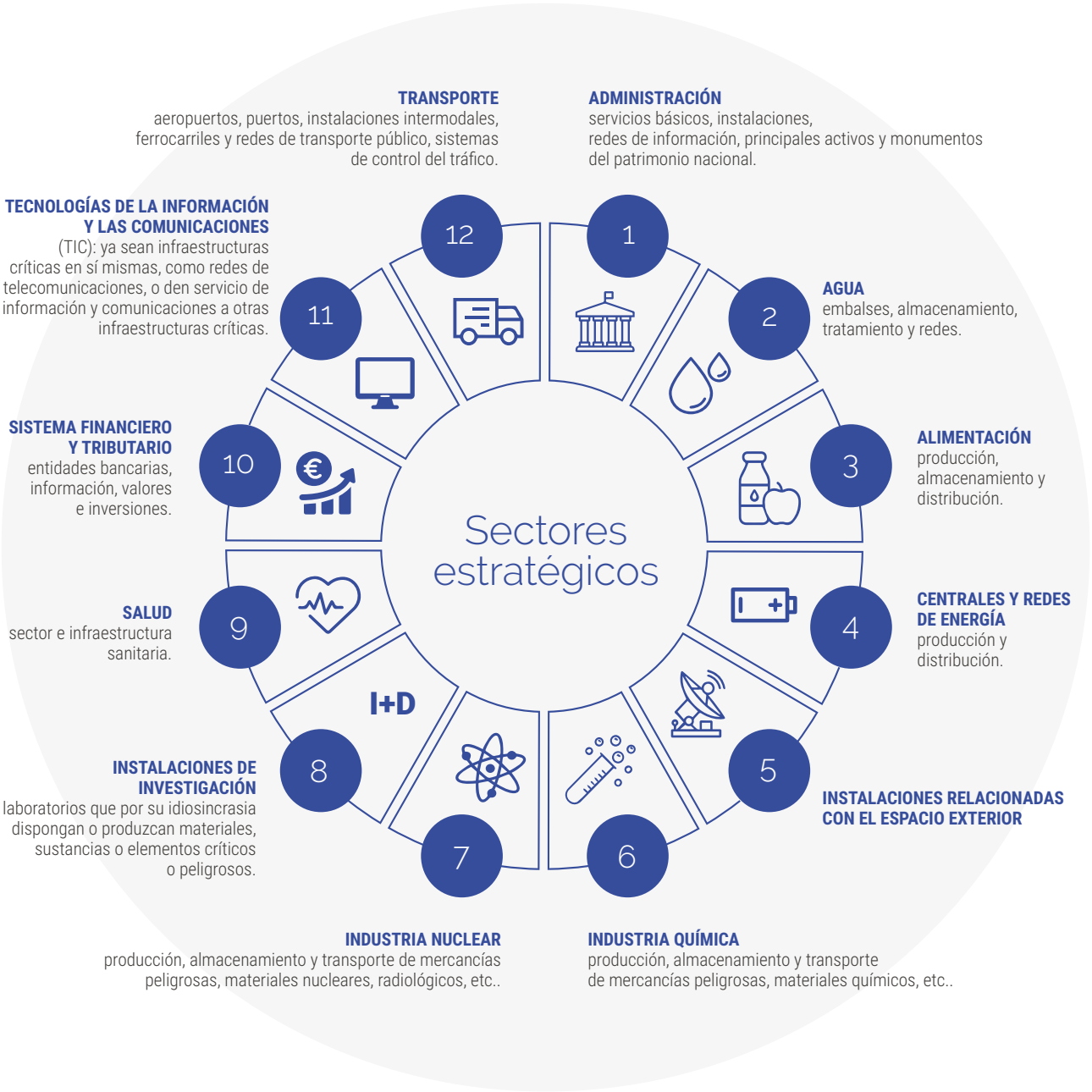
LAS POLÍTICAS DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS.

España ha formado en la última década, un sistema PIC robusto en el que el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) es el principal órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad. Dependiente de la Secretaria de Estado de Seguridad en el seno del Ministerio del Interior, **el CNPIC ha impulsado desde su nacimiento en 2007 18 Planes Estratégicos Sectoriales** para los **12 sectores en los que recaen las infraestructuras críticas españolas** (Figura 1).

A pesar de que las infraestructuras críticas son similares en todos los países, su práctica puede variar en función de las necesidades, recursos y nivel de desarrollo de cada país. La información sobre la totalidad de las infraestructuras críticas está clasificada como secreta en la mayorías de países debido a la alta sensibilidad de la cuestión para la seguridad nacional. España dispone en este sentido de un Catalogo Nacional de Infraestructuras Críticas (clasificado) en el que **el Ministerio del Interior ha**

reconocido más de 3.500 infraestructuras críticas, de un Plan Nacional de Protección de las mismas y **más de 500 planes de protección específicos**. Y es que dado que la mayoría de las áreas estratégicas y servicios esenciales identificados son proporcionados por operadores privados, la responsabilidad de protección de las infraestructuras críticas no recae únicamente en la Administración Pública, sino en un **sólido sistema de colaboración público-privada en el que los operadores de las infraestructuras identificadas (más de 180 en 2020) juegan un papel fundamental.** Entre sus obligaciones destacan el desarrollo de análisis de riesgos y amenazas, planes de respuesta, reuniones periódicas para la gestión de temas relacionados con la seguridad y la notificación de incidentes de importancia a los Organismos Competentes.

SECTORES ESTRATÉGICOS DE INFRAESTRUCTURA CRÍTICA EN ESPAÑA
(FIGURA 1)



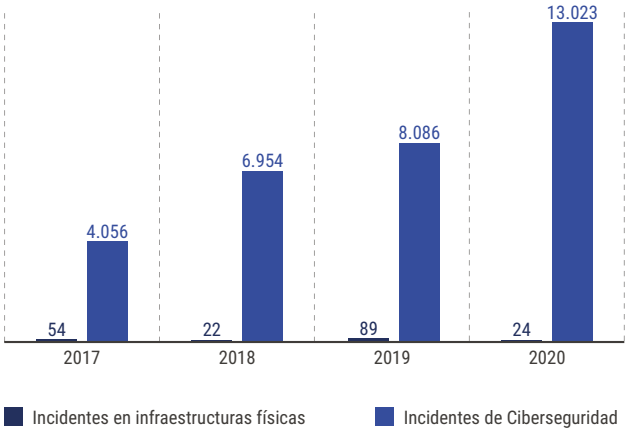
Fuente: Estrategia Nacional de Seguridad (2020)

LA AFECTACIÓN DE LA PANDEMIA.

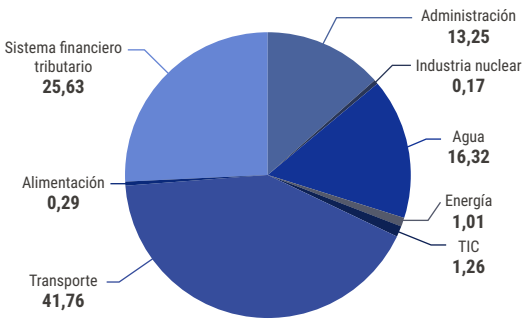
La pandemia de COVID-19 ha vuelto a poner de manifiesto la importancia de garantizar la continuidad de los servicios esenciales. En 2020 se reportaron al CNPIC un total de **24 incidentes relacionados con la seguridad física** en sectores estratégicos, frente a los 89 registrados en 2019 (Figura 2). En este mismo periodo y en el ámbito digital se registraron un total de **13.023 incidentes de ciberseguridad** de distinta peligrosidad e impacto en operadores críticos, un 61% más que en 2019 (Figura 2). Los sectores estratégicos más afectados por ciberataques fueron el sector Financiero y Tributario, en 5 de cada 10 casos, Transporte en 2/10 y Energía en 1/10 (Figura 3).

Pese a que estos incidentes no llegaron a comprometer los servicios esenciales soportados por dichas infraestructuras (aunque su efecto sobre los servicios corporativos de los operadores críticos fue en algunos casos elevado), los datos muestran la creciente

INCIDENTES REGISTRADOS EN SECTORES ESTRATÉGICOS EN LOS ÚLTIMOS AÑOS
(FIGURA 2)



DISTRIBUCIÓN DE LOS CIBERINCIDENTES EN BASE AL SECTOR ESTRATÉGICO AFECTADO
(FIGURA 3)



Fuente: Informe Anual de Seguridad Nacional (2020)

amenaza que suponen los ciberataques, tanto en número como en sofisticación (consultar el riesgo T1 `Incremento de la cantidad y la sofisticación de los ciberataques'). La colaboración entre operadores críticos, el Instituto Nacional de Ciberseguridad (INCIBE) y el CNPIC para mantener el servicio al conjunto de la ciudadanía fue una herramienta eficaz y decisiva en este sentido para superar esta crisis.

Además, si bien el impacto de la COVID-19 en cuanto a los ciber incidentes registrados en las infraestructuras críticas fue muy bajo en todos los sectores –**solo un 3% de los ciber incidentes (370) tuvo relación con la pandemia**–, el sector Sanitario fue una excepción. En particular, el número de incidentes aumentó en este sector más de un 300%, pasando de los 13 incidentes en 2019 a 55 incidentes en 2020, asociados a la disponibilidad de los sistemas y redes que lo soportan *(ransomware)* o al robo de información disponible, sobre todo ligada a centros de investigación de la COVID-19.

EL IMPACTO DE LA FUTURA REGULACIÓN EUROPEA.

La Unión Europea tiene en fase de elaboración diversas normas que impactarán en los próximos años sobre la protección de los servicios esenciales y las infraestructuras críticas. A raíz de la revisión de la Estrategia de Seguridad [Interior] de la Unión para el período 2020-2025, **la Comisión ha impulsado dos propuestas de directiva elaboradas en paralelo, la Directiva NIS2 y la Directiva sobre Resiliencia de Entidades Críticas, con el objetivo de reforzar la capacidad de los Estados miembros para proteger y recuperar sus infraestructuras y servicios críticos nacionales**. Las nuevas normas dedican mayor atención a la ciberseguridad y reivindican la necesidad de aproximar las dimensiones física y ciber de la seguridad. Además y como novedad, la nueva Directiva de Resiliencia amplía su ámbito de regulación a nuevos sectores distintos de los de transporte y energía, haciéndolos coincidentes a los sectores de servicios esenciales establecidos en la propuesta de Directiva NIS2 (administración pública, banca, finanzas, espacio, salud, aguas e infraestructuras digitales) y dedica especial atención a los que actúan en tres o más países de la UE (entidades de críticas de relevancia europea). Las entidades críticas deberán desarrollar análisis de riesgos, planes de respuesta y notificar los incidentes de importancia, unas obligaciones con las que ya están familiarizados los responsables de infraestructuras críticas de países como España, pero que conllevará un necesario periodo de adaptación.

EL RIESGO PARA LAS **EMPRESAS**

El transporte, el suministro de agua, la sanidad, la alimentación, las entidades de servicios financieros o el sector TIC son seis de los doce sectores estratégicos en España. Su carácter esencial o crítico hace que cualquier disrupción pueda provocar disfunciones graves en materia de seguridad en nuestro país y por ello, deben ser especialmente protegidos de posibles incidentes de seguridad física y por supuesto, desde el ámbito de la ciberseguridad. Es este último el que más preocupa, pues los ciberataques a los sectores estratégicos se han duplicado en los últimos dos años, y se espera que la tendencia siga al alza tanto en número como en nivel de sofisticación.

En un entorno dominado por la hiperconectividad, la automatización y la digitalización, los servicios esenciales se han vuelto menos herméticos en los últimos años. Si bien su integración con la red tiene numerosas ventajas, también los expone a las mismas vulnerabilidades que cualquier otro sistema, resultando imprescindible el refuerzo en términos de resiliencia de estas infraestructuras críticas.

IMPACTOS EN LA EMPRESA