RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/35171 **23/02/2026** **101294**

AUTOR/A: FIGAREDO ÁLVAREZ-SALA, José María (GVOX); RODRÍGUEZ ALMEIDA, Andrés Alberto (GVOX); RUEDA PERELLÓ, Patricia (GVOX)

RESPUESTA:

En relación con las preguntas formuladas, se informa de que, a través de la Secretaría de Estado de Seguridad, del Ministerio del Interior, se dispone de datos relativos al sector industrial español que hacen referencia a operadores de servicios esenciales, considerados como tales conforme a lo establecido en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de la información, y del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el anterior.

En este sentido, los ciberataques de carácter relevante que la Secretaría de Estado de Seguridad ha gestionado en el marco de sus competencias y cuya categorización, según su peligrosidad o impacto, ha sido de Críticos, Muy Altos o Altos, ascienden a un total de 40 incidentes durante 2025, distribuidos en los siguientes sectores industriales:

- Transporte (14)
- Industria nuclear (4)
- Industria química (5)
- Energía (7)
- Espacio (2)
- Tecnologías de la información y la comunicación -TIC- (8)

Al respecto de los datos, se señala que, en el caso del sector Transportes, la cifra es significativamente más elevada debido a la campaña del actor NoName057 contra España en el contexto del conflicto entre Rusia y Ucrania. Durante esta campaña, el grupo incluyó a nuestro país entre sus objetivos como respuesta al apoyo brindado por España a Ucrania, lo que incrementó notablemente el volumen de acciones dirigidas a este sector.

Asimismo, el Instituto Nacional de Estadística (INE) dispone de información sobre el porcentaje de empresas que, tras experimentar un incidente de seguridad TIC, tuvieran como consecuencia una falta de disponibilidad de los servicios TIC debido a un ataque desde el exterior. Esta información está recogida en la Encuesta de uso de TIC y Comercio Electrónico (ETICCE) del año 2023. El cuestionario de esta estadística se modifica anualmente según el Reglamento (UE) 2019/1700 del Parlamento Europeo y del Consejo de 10 de octubre de 2019 por el que se establece un marco común para las estadísticas europeas relativas a las personas y los hogares, basadas en datos individuales recogidos a partir de muestras, y los reglamentos delegados posteriores que lo completan.

Esta variable se incluye de nuevo en el cuestionario del año de referencia 2025, que está actualmente en fase de recogida.

Se adjunta tabla en anexo que incluye los porcentajes para el total de la industria para empresas de 10 empleados o más, desglosado por tamaño de la empresa. Se incluye además el detalle de actividad según agrupaciones dentro del sector industrial, que se describen en la tabla.

Por otro lado, se señala que ninguno de estos ataques en los diferentes sectores fue tan relevante como para implicar la paralización total de líneas de producción o servicios, y solo en tres casos —dos incidentes de indisponibilidad por DDoS (ataque de denegación de servicio distribuido) y uno de compromiso de la información debido a una modificación no autorizada— se observó una paralización parcial, con un impacto mínimo reportado.

Respecto a la segunda cuestión, se informa de que el Ministerio de Industria y Turismo, en el ámbito de sus competencias, viene desarrollando actuaciones para reforzar las capacidades de digitalización y ciberseguridad de las pequeñas y medianas empresas (pymes) con el fin de incrementar su resiliencia frente a estas amenazas.

El Programa Activa Ciberseguridad, en coordinación con el Instituto Nacional de Ciberseguridad (INCIBE), proporciona a las pymes un asesoramiento individualizado, permitiendo evaluar el nivel de madurez en ciberseguridad de cada empresa y elaborar un Plan de Ciberseguridad adaptado a sus necesidades. Desde su creación, más de 1.000 pymes han sido beneficiarias:

https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/ACTIVA-Ciberseguridad.aspx

De manera complementaria, el Ministerio de Industria y Turismo impulsa otras iniciativas clave que contribuyen indirectamente a mejorar la ciberseguridad industrial mediante la digitalización segura y la adopción de tecnologías avanzadas.

El Programa de Apoyo a las Agrupaciones Empresariales Innovadoras (AEI) constituye una herramienta esencial para promover proyectos colaborativos de innovación que integran tecnologías digitales en entornos industriales. Los resultados del programa muestran mejoras significativas en la digitalización de las pymes participantes, incremento de su know-how y diversificación de líneas productivas, factores clave para reducir vulnerabilidades tecnológicas:

https://www.mintur.gob.es/portalayudas/agrupacionesempresariales/Paginas/Index.aspx

Asimismo, el Programa de Apoyo a los Digital Innovation Hubs (PADIH) facilita la transformación digital de las pymes mediante la red española de 25 EDIH (European Digital Innovation Hubs), que actúan como centros de referencia en tecnologías avanzadas. Estos hubs permiten a las empresas probar soluciones digitales —incluidas tecnologías de ciberseguridad industrial— antes de invertir, acceder a formación especializada y conectar con redes europeas de innovación:

https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/DIH.aspx

El Ministerio de Industria y Turismo pone también a disposición de las pymes, a través de la Plataforma Pyme, una herramienta de autodiagnóstico de ciberseguridad que permite evaluar de forma rápida, sencilla y gratuita el nivel de madurez de la empresa en esta materia. Esta herramienta facilita a las pymes identificar vulnerabilidades, conocer su grado de preparación ante incidentes y obtener recomendaciones personalizadas de mejora, convirtiéndose en un recurso útil para apoyar la toma de decisiones y orientar inversiones en seguridad digital:

https://plataformapyme.es/es-es/herramientas-digitales/Paginas/ciberseguridad.aspx

En suma, desde el Ministerio de Industria y Turismo se está desplegando una política integral de apoyo a la digitalización y a la ciberseguridad de las pymes industriales basada en asesoramiento especializado, apoyo a la innovación colaborativa y fortalecimiento de la capacidad tecnológica.

Asimismo, se informa de que desde el Instituto Nacional de Ciberseguridad (INCIBE) se desarrollan actividades e iniciativas para concienciar y reforzar los conocimientos y capacidades de las pymes, tales como asistencia para gestión y resolución de incidentes; servicios de monitorización, vigilancia digital, detección y notificación preventiva, y de identificación, análisis, gestión y mitigación de

vulnerabilidades; diseño, planificación y ejecución de ejercicios prácticos; desarrollo y apoyo de proyectos en colaboración público-privada para sensibilizar, concienciar y divulgar la importancia de la ciberseguridad; e iniciativas destinadas a la mejora de la cultura de ciberseguridad mediante acciones formativas.

Finalmente, se informa de que, actualmente, se encuentra pendiente la aprobación del Anteproyecto de Ley de Coordinación y Gobernanza de Ciberseguridad, texto derivado de la transposición de la Directiva europea NIS2, cuyo objetivo es reforzar las políticas específicas relativas a las entidades esenciales e importantes de diversos sectores, entre los que se incluye el sector industrial. En particular, dicha normativa afectará también a las pequeñas y medianas empresas, especialmente a aquellas que cuenten con más de 50 empleados o superen los 10 millones de euros de facturación anual, o aquellas que sin cumplir ese requisito sean proveedor único o crítico.

Madrid, 09 de abril de 2026

ANEXO 184/35171

	Total	De 10 a 49	De 50 a 249	De 250 y más
% de empresas que, tras experimentar un incidente de seguridad TIC, tuvieran como consecuencia una falta de disponibilidad de los servicios TIC debido a un ataque desde el exterior				
1. Total Industria (CNAE 10-39)	14,10	12,39	16,68	19,67
1.1. Alimentación bebidas tabaco textil prendas vestir cuero y calzado madera y corcho papel artes gráficas y reproducción de soportes grabados (CNAE 10-18)	10,64	8,58	16,63	14,20
1.2 Coquerias y refino de petróleo produc. farmacéuticos caucho y plásticos Productos minerales no metálicos (CNAE 19-23)	12,36	12,72	10,75	13,82
1.3 Metalurgia fabricación de productos metálicos (CNAE 24-25)	12,71	11,99	13,69	15,50
1.4. Productos informáticos, electrónico y ópticos material y equipo eléctrico maquinaria y equipo mecánico vehículos a motor material de transporte muebles industria manufacturera reparación maquinaria y equipo (CNAE 26-33)	19,81	20,70	14,98	29,54
1.5. Energía y agua (CNAE 35-39)	28,34	18,19	39,72	37,38