Síguenos en

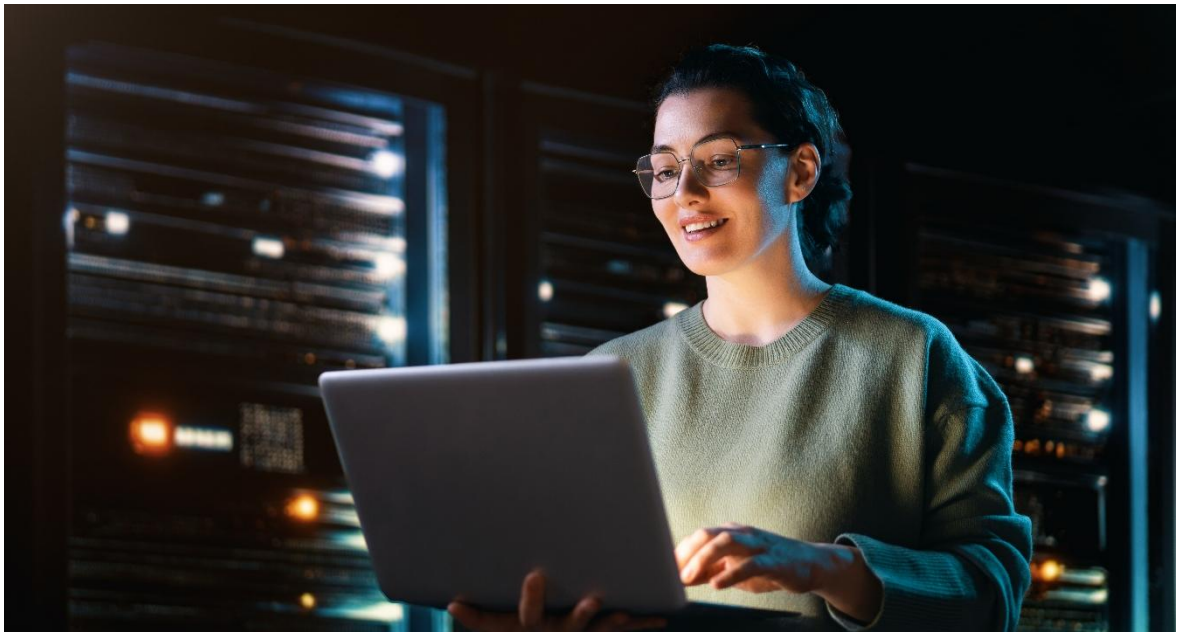
INFORME SOBRE RIESGO DIGITAL DE GRANT THORNTON

# Casi la mitad de las empresas españolas no es plenamente consciente de la gravedad de los riesgos de ciberseguridad a los que está expuesta

## España se mantiene lejos de los estándares europeos y globales en materia de riesgos digitales

## El 70% de las compañías del middle-market admite no estar satisfecha con su capacidad para detectar y gestionar ataques

## Las pequeñas y medianas empresas son las más expuestas al crecimiento de los riesgos digitales en nuestro país



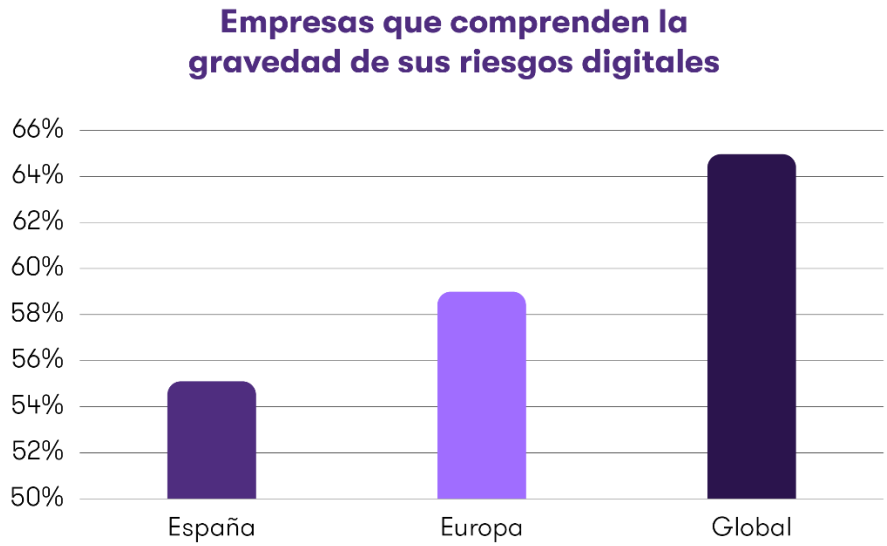


USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

**Madrid, lunes 9 de noviembre de 2026**

El incremento y la sofisticación de los ciberataques realizados contra empresas e infraestructuras clave han puesto de manifiesto la necesidad de reforzar la inversión en ciberseguridad y, especialmente, las capacidades de prevención, detección, respuesta y recuperación ante incidentes. Un aspecto en el que las propias empresas reconocen su margen de mejora. Según los datos recopilados por Grant Thornton, **casi la mitad de las empresas del middle-market nacional** (45%) reconoce no ser plenamente conscientes de la gravedad de los riesgos digitales a los que está expuesta. Asimismo, el 70% de las encuestadas admite no estar plenamente satisfecha con su capacidad para detectar y gestionar ciberataques.

Son algunas de las conclusiones del informe **"Cómo gestionar mejor el riesgo digital: hacia una nueva etapa de la ciberrevolución"**, elaborado por Grant Thornton a partir de una encuesta realizada a más de 4.000 directivos en 35 países. Un documento que refleja el margen de mejora que posee España en esta materia: el porcentaje de empresas que es consciente de sus propios riesgos digitales se sitúa en nuestro país 10 puntos porcentuales por debajo de la media global y 4 puntos por debajo del conjunto de la UE.

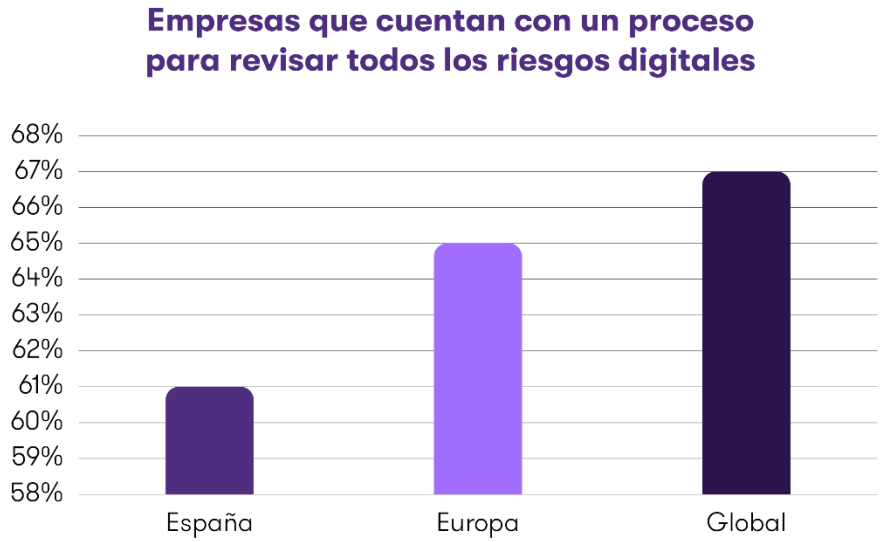





USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

“Estamos viviendo un momento determinante en España. Las amenazas digitales son cada vez más frecuentes y sofisticadas, y las empresas necesitan reforzar no solo su tecnología, sino también su modelo de gobierno, sus procesos y su capacidad de respuesta y recuperación ante incidentes”, explica la **socia de Forensic y Ciberseguridad de Grant Thornton España, Cristina Muñoz-Aycuens**. Según sus palabras, son las pequeñas y medianas empresas las que pueden estar especialmente expuestas al incremento y sofisticación de las amenazas, al disponer en muchos casos de menos recursos y capacidades especializadas en ciberseguridad.

Lo cierto es que los ciberataques contra empresas españolas han seguido aumentando tanto en número como en sofisticación. Según los datos del Instituto Nacional de Ciberseguridad (Incibe), casi la mitad de las empresas españolas ha sufrido un ciberataque en los últimos años. Y peor aún: en muchos casos las compañías ni siquiera son conscientes de que han sido víctimas de esta situación.




Esto puede ser consecuencia de que, mientras en España **el 61% de las empresas cuentan con un proceso para revisar todos los riesgos digitales**, este porcentaje crece hasta el 65% en el conjunto de Europa y al 67% en el resto del mundo.



USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

Los expertos en la materia opinan que no suele ser sencillo inculcar a las empresas la necesidad de invertir en ciberseguridad porque no se percibe un retorno rápido. Sin embargo, el coste de restaurar sistemas cuando se sufre un ciberataque es exponencialmente mayor cuando no se ha acometido una inversión en ciberseguridad.

## La Inteligencia Artificial y el papel de los empleados

El auge de la Inteligencia Artificial (IA) supone un nuevo reto en este ámbito. El socio experto en Derecho Digital y DPO de Grant Thornton Eloi Font cree que “la IA es una herramienta que puede sofisticar las técnicas que se utilizan para acometer distintos fraudes en el ámbito digital, por lo que es necesario establecer políticas que definan en la empresa qué uso se dará a la IA, e incluso quizás debemos contar con una IA propia”.

El estudio de Grant Thornton hace referencia a esta realidad. Un 39% de las empresas encuestadas reconocen que el hecho de que sus empleados no tengan claro de qué riesgos son responsables es su principal punto débil a la hora de gestionar ciberriesgos. Además, casi **el 20% de los encuestados reconoce que sus sistemas de gestión de riesgos digitales están desfasados o no están adecuados para los fines que persiguen**. De igual forma, solo el 24% de las empresas asegura estar preparada para detectar nuevos riesgos en materia de ciberseguridad. A ello se suma el riesgo derivado del uso no controlado de herramientas de IA por parte de los empleados, que puede generar nuevas vías de fuga de información, exposición de datos sensibles o incorporación de información corporativa a servicios externos.

## Una nueva estrategia regulatoria

La Unión Europea ha reforzado en los últimos años las obligaciones en materia de ciberseguridad y resiliencia digital. Entre las principales iniciativas figuran la Directiva NIS2, orientada a elevar el nivel común de ciberseguridad en sectores esenciales e importantes, el Reglamento DORA, aplicable desde enero de 2025 y dirigido a reforzar la resiliencia operativa digital del sector financiero y el Reglamento de Ciberresiliencia, aplicable desde el pasado mes de septiembre,



USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

que establece requisitos obligatorios de ciberseguridad para los productos con elementos digitales comercializados en la UE durante todo su ciclo de vida.

“Existen nuevos retos regulatorios, pero en este caso la regulación puede ser positiva para impulsar la concienciación en esta materia, especialmente, de los órganos de dirección que pasarán a tener responsabilidad en el caso de que no las cumplan. Las empresas van a tener la necesidad de invertir para cumplir con todas estas obligaciones regulatorias”, destaca Eloi Font.

¿Por dónde debe empezar su estrategia digital una compañía? El informe de Grant Thornton señala la **necesidad de realizar un primer análisis de la situación** en materia de riesgos de ciberseguridad y tener en cuenta tanto a los procesos que se acometen como el trabajo de la plantilla. Un trabajo que permitirá contar con una visión clara de la realidad de cada empresa y qué riesgos existen dentro de la compañía. Un primer paso indispensable para construir una estrategia de ciberseguridad basada no solo en la prevención, sino también en la capacidad de anticiparse, responder y recuperarse ante los incidentes.

**Sobre Grant Thornton**

En Grant Thornton España ayudamos a que tu empresa vaya más allá. Servicios profesionales de Auditoría & Assurance, Advisory, Tax, Asesoramiento Financiero, Legal, Laboral y Outsourcing. 11 oficinas y 900 profesionales en nuestro país. Pertenecemos a Grant Thornton Advisors, una plataforma multinacional y multidisciplinar que proporciona una experiencia de cliente única y transfronteriza, con soluciones y capacidades potenciadas por la última tecnología y los mejores equipos. A su vez, formamos parte de Grant Thornton International, una de las redes globales de servicios profesionales líderes, con 80.000 profesionales presente en más de 150 mercados en todo el mundo.

Para ampliar información o hablar con profesionales de Grant Thornton, no dudes en llamarnos:

**DEPARTAMENTO COMUNICACIÓN GRANT THORNTON**

**POLICARPO AROCA**
Director de Comunicación, Marketing y Desarrollo de Negocio
T 91 576 39 99
M 650 71 31 21
Policarpo.aroca@es.gt.com

**LEAD BY THOUGHT**

**GABRIELE CAGLIANI**
+34 669 496 103
gabriele@leadbythought.com

**MARÍA CUESTA**
+34 646 494 090
maria.cuesta@leadbythought.com



USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

Síguenos en

**JOSÉ MARÍA GÓMEZ**
Supervisor de Comunicación
T 932 06 39 00
M 681 15 65 13
josemaria.gomez@es.gt.com

**MARTA CARDENAL**
Técnica de Comunicación Corporativa
T 932 06 39 00
M 608 99 02 14
marta.cardenal@es.gt.com

**GUILLERMO GINÉS**
+34 637 916 561
guillermo.gines@leadbythought.com



USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-