Cámara de Comercio de España

# OBSERVATORIO DE competitividad empresarial

CIBERSEGURIDAD

Nº 19/2026

# El Observatorio de Competitividad Empresarial

El Observatorio de Competitividad Empresarial es una iniciativa de la Cámara de Comercio de España cuyo **objetivo es contribuir al conocimiento y valoración de la capacidad competitiva de nuestro tejido empresarial.**

**El Observatorio estudia periódicamente diversos factores o ámbitos clave para la competitividad empresarial,** con un análisis específico.

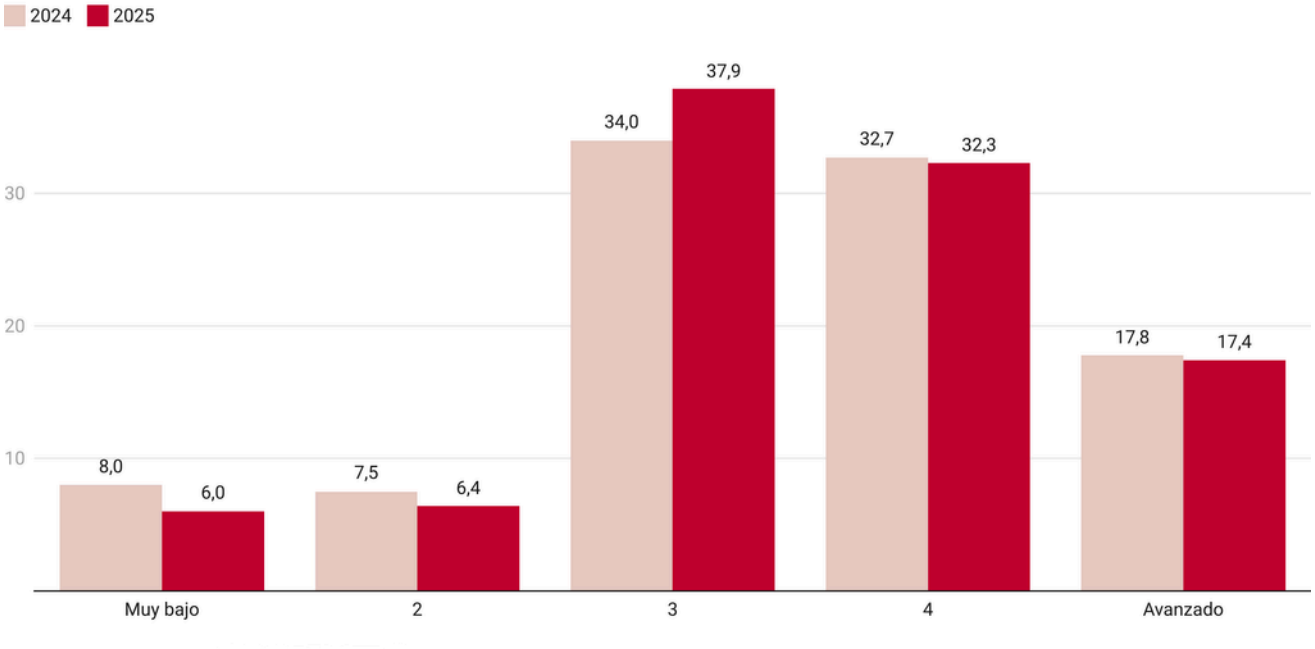
Este número del Observatorio se dedica a la **ciberseguridad.** Se trata de un monográfico en el que se analizan diferentes aspectos relativos a la ciberseguridad empresarial, tales como la gestión y planificación de la ciberseguridad, las medidas de protección adoptadas, la tipología y el impacto de los ciberataques sufridos o las barreras para mejorar las defensas ante las ciberamenazas. Para ello, la información ha sido recogida a partir de una encuesta ad hoc a las empresas españolas.

Con la publicación de este Observatorio, la **Cámara de Comercio** contribuye activamente al conocimiento e interpretación de la realidad competitiva de nuestras empresas, en su ejercicio responsable como **institución consultiva en defensa del interés general.**

# Resumen

**Las empresas españolas muestran un alto grado de digitalización, el 87,6% de las empresas percibe que su nivel de digitalización se sitúa en niveles intermedios o avanzados,** cifra superior a la del año anterior y más elevada en empresas de mayor tamaño y en el sector servicios.

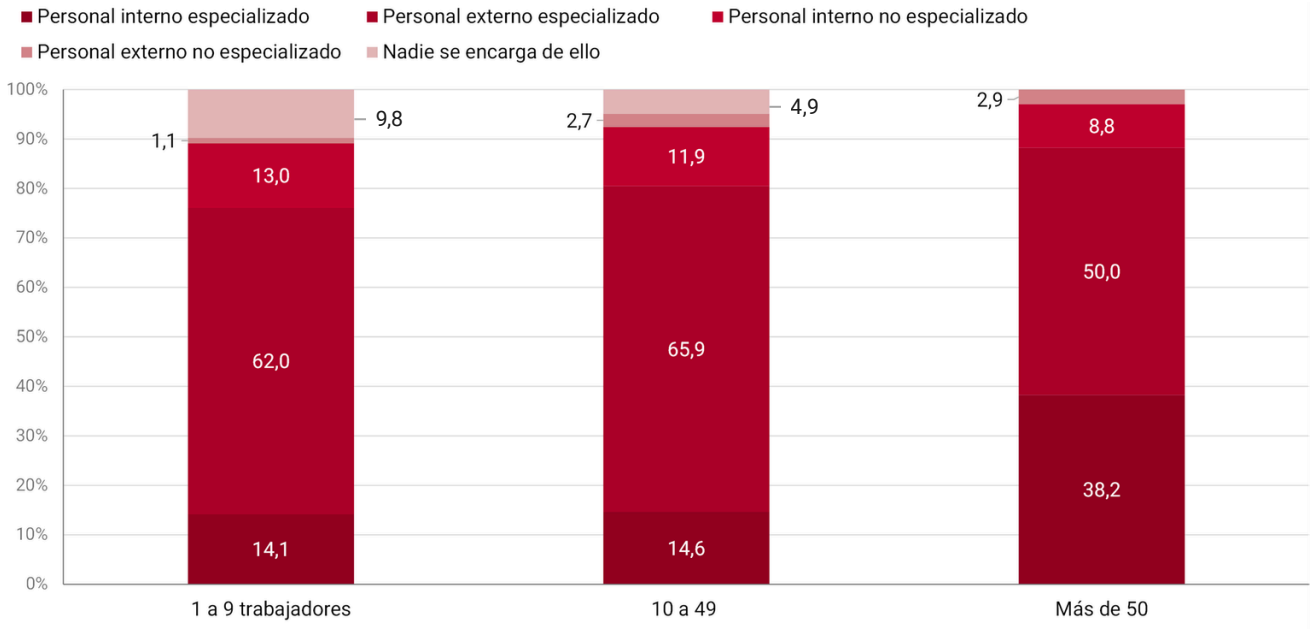
## Nivel de digitalización percibido (%)




Fuente: Cámara de España

En 2025 se observa una tendencia creciente a la externalización de la gestión de la ciberseguridad por parte de las empresas**. El 62,8% de las empresas delega la gestión en personal externo** (frente al 53% en 2024), mientras que la presencia de personal interno especializado baja del 20% al 16,4%. **Las pymes dependen casi por completo de proveedores externos, mientras que las grandes empresas aumentan la internalización** (38,2% de personal interno y 50% externo).

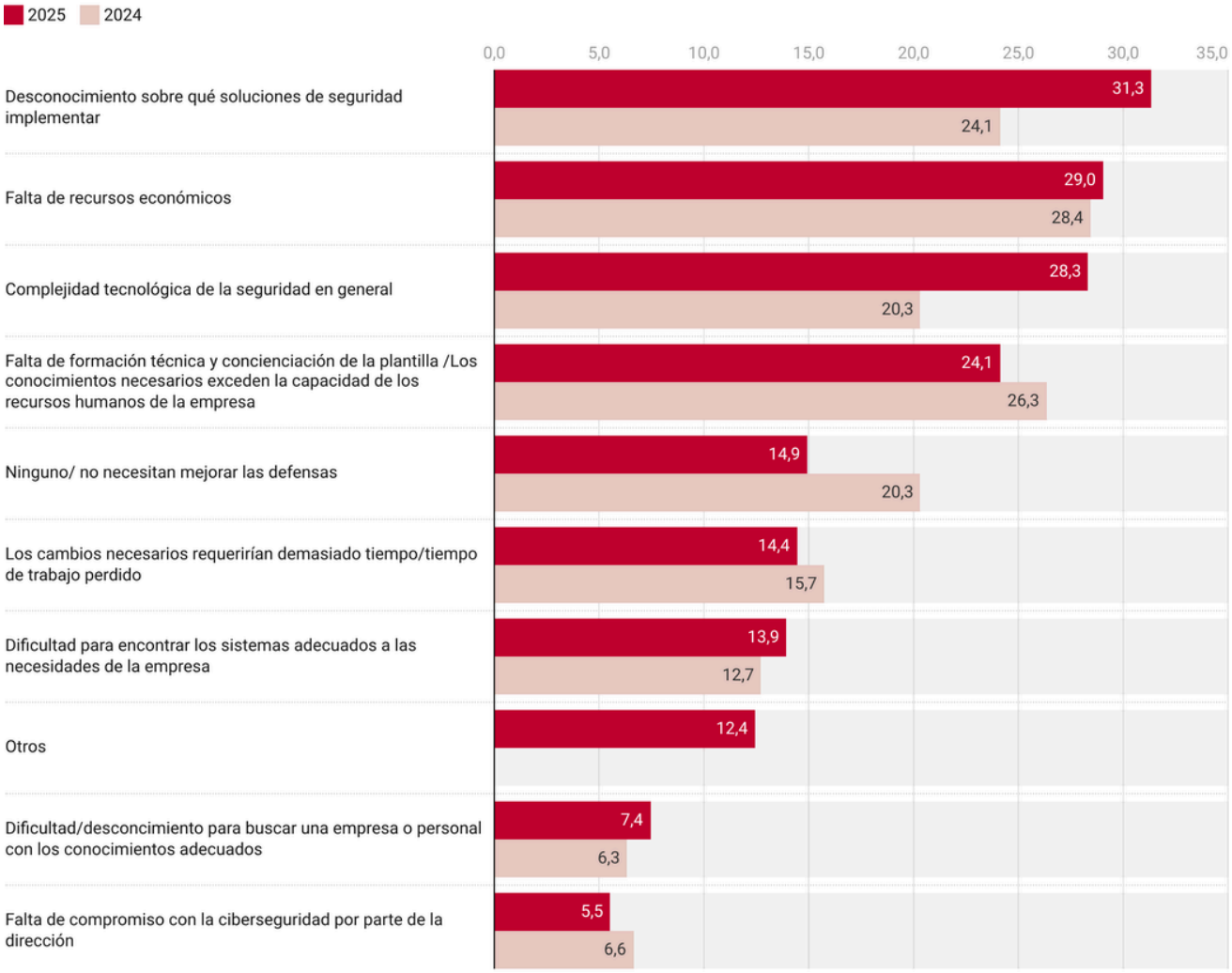
## ¿Quién gestiona la ciberseguridad de la empresa?, por tamaño (%)




Fuente: Cámara de España

**Las empresas muestran confianza en su nivel de protección frente a ciberataques y, además, muchas se perciben como poco atractivas para los ciberdelincuentes, lo que contribuye a una planificación y estrategia de ciberseguridad insuficientes.** Así, el 68,5% de las empresas se considera bien protegida, el 53,1% cree ser poco o nada atractiva para los atacantes y el solo 42,9% dispone de una estrategia formal de ciberseguridad. Las medidas básicas, como antivirus y copias de seguridad, están prácticamente universalizadas, pero persisten diferencias en la adopción de soluciones más avanzadas: cortafuegos (94% en grandes empresas frente a 66,8% en microempresas) y redes privadas virtuales (VPN) (76,5% frente a 44%). Entre los principales obstáculos para mejorar la ciberseguridad destacan el desconocimiento (31,3%), la complejidad tecnológica (28,3%) y las limitaciones presupuestarias (29%).

## Factores que impiden a las empresas mejorar sus defensas contra los ciberataques (%)




Fuente: Cámara de España

Las empresas españolas están cada vez más digitalizadas, son conscientes del riesgo de los ciberataques, pero con carencias en planificación y adopción de soluciones avanzadas. Por ello, sería importante **fomentar una cultura sólida de ciberseguridad, ofrecer formación y asesoramiento para reducir el desconocimiento y la complejidad tecnológica, e impulsar mecanismos de financiación que alivien las restricciones presupuestarias.** Además, se debe reforzar la percepción realista del riesgo, traducirla en acciones preventivas y reactivas, e incorporar contramedidas frente a amenazas emergentes como las basadas en inteligencia artificial. Por otra parte, la experiencia del teletrabajo demuestra que las adaptaciones pueden realizarse sin aumentar la exposición si se acompañan de buenas prácticas. Finalmente, respecto a las perspectivas para los próximos 12 meses, **solo un 24,3% de las empresas tiene previsto incrementar su presupuesto para la ciberseguridad.** Por ello, sería conveniente promover una **inversión sostenida y progresiva, especialmente en pymes**, para equilibrar capacidades y garantizar la resiliencia digital, factor clave para la competitividad y la confianza del tejido empresarial español en un entorno global cada vez más complejo

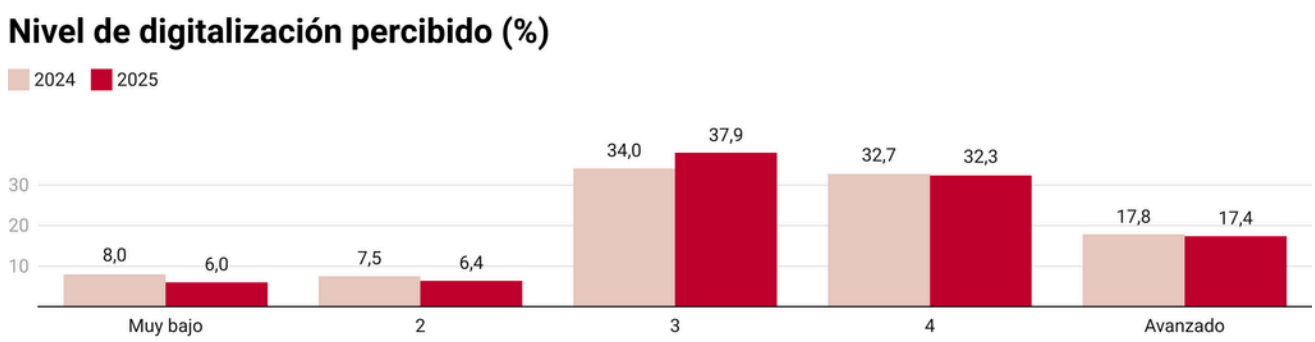
# Contextualización: grado de digitalización de las empresas, gestión de la ciberseguridad y percepción del riesgo

Como punto de partida, y con el objeto de poner en contexto el análisis de la ciberseguridad de las empresas españolas, en este apartado se realiza una aproximación al nivel de digitalización de las compañías y a la manera en que gestionan la ciberseguridad y el riesgo que perciben al respecto.

## Percepción del grado de digitalización de las empresas

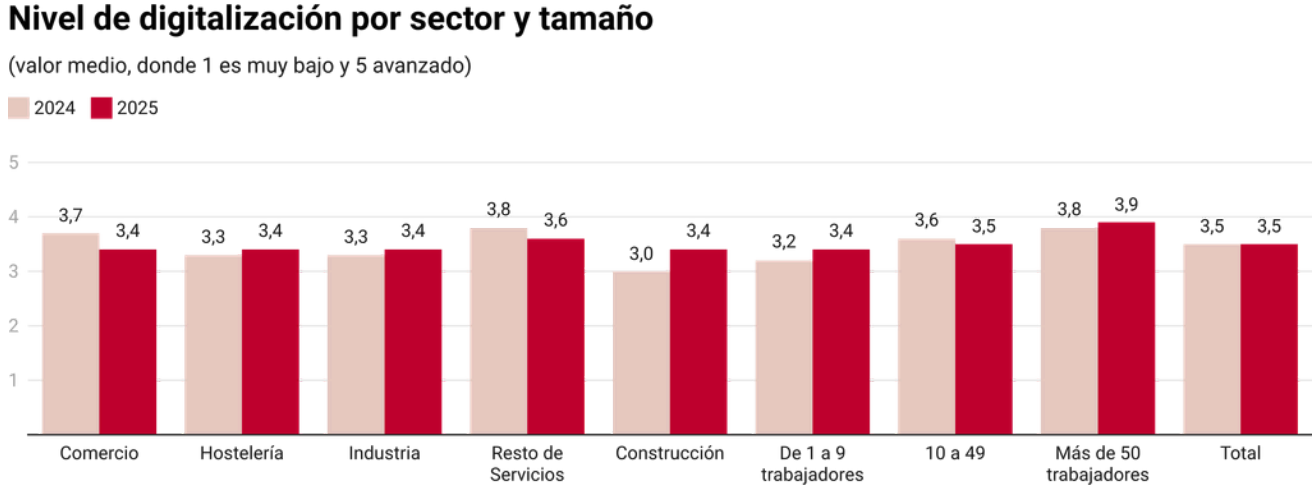
**Las empresas españolas son optimistas en cuanto a su nivel de digitalización**. El 87,6% de las empresas encuestadas manifiestan que su digitalización se sitúa en un nivel de intermedio a avanzado. Además, está percepción es superior a la que tenían las empresas el año anterior, que era del 84,5%.

Atendiendo al tamaño de las empresas, **el grado de digitalización autopercibida aumenta según se incrementa el número de trabajadores**, pasando de una media de 3,4 puntos entre las más pequeñas hasta 3,9 puntos entre las de más de 50 trabajadores. **Por sectores, son las pymes del resto de servicios las perciben un mayor nivel de digitalización.**




Fuente: Cámara de España

La evolución en la percepción del nivel de digitalización en las empresas encuestadas, por sector y tamaño, muestra que las empresas pertenecientes al sector de la **construcción junto con las de menor dimensión son las que más han avanzado en la digitalización**, o al menos las que perciben mayores niveles de digitalización respecto al año anterior. Así, las empresas de construcción pasan de percibir un nivel de digitalización de 3,0 puntos en 2024 a 3,4 puntos un año después y las empresas de 1 a 9 trabajadores de 3,2 puntos a 3,4 puntos.

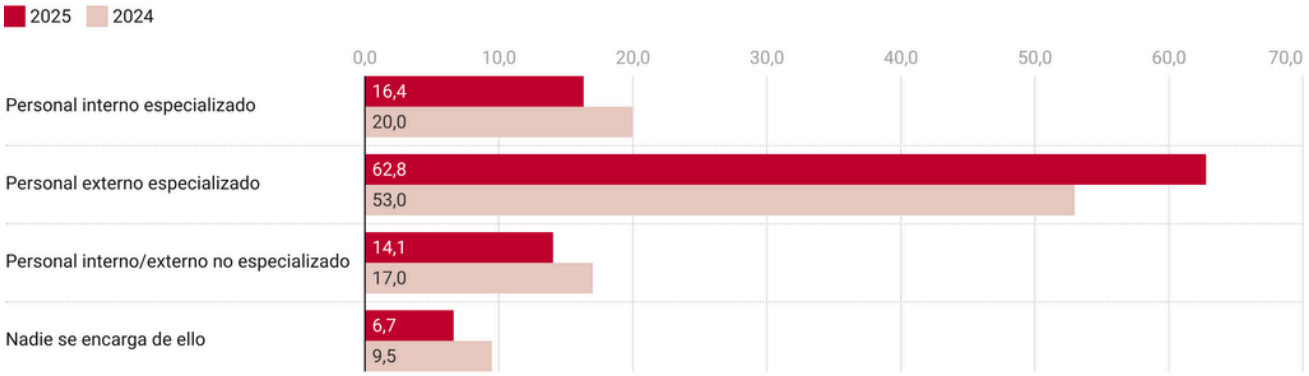



Fuente: Cámara de España

# Gestión de la ciberseguridad

En 2025, se observa una **tendencia a la externalización de la gestión de la ciberseguridad en las empresas.** Así el 62,8% de las empresas encuestadas confía la gestión de la ciberseguridad en personal externo especializado, frente al 53% en 2024. Por el contrario, el personal interno especializado disminuye del 20% al 16,4%, lo que indicaría que las pymes prefieren contratar expertos externos en lugar de formar equipos internos. También se observa una reducción de la gestión por personal no especializado (del 17% al 14,1%) y de las empresas donde nadie se encarga de ello (del 9,5% al 6,7%), lo que evidencia tanto una mayor concienciación sobre la importancia de la ciberseguridad como que las empresas estarían profesionalizando la gestión de riesgos digitales.

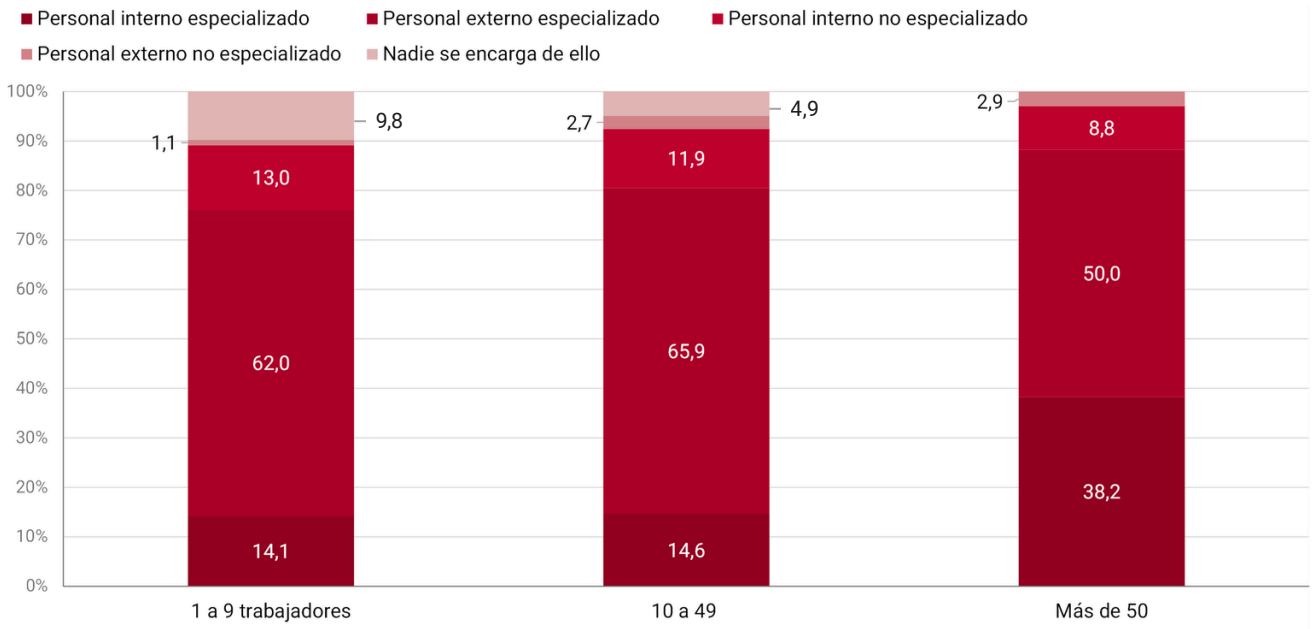
## ¿Quién gestiona la ciberseguridad? (%)




Fuente: Cámara de España

**El análisis por tamaño empresarial indica que las grandes empresas tienen más recursos y mayor capacidad para crear equipos internos, mientras que las pequeñas dependen en mayor medida de proveedores externos.** En las empresas más pequeñas (1 a 9 trabajadores), la ciberseguridad se gestiona principalmente por personal externo especializado (62%), mientras que solo un 14,1% cuenta con personal interno especializado. En las de 10 a 49 empleados, la externalización aumenta al 65,9%, confirmando su predominio. Sin embargo, en las empresas de más de 50 trabajadores, gana peso el personal interno especializado el 38,2% dispone de personal interno especializado, reduciendo la gestión externa al 50%.

## ¿Quién gestiona la ciberseguridad de la empresa?, por tamaño (%)

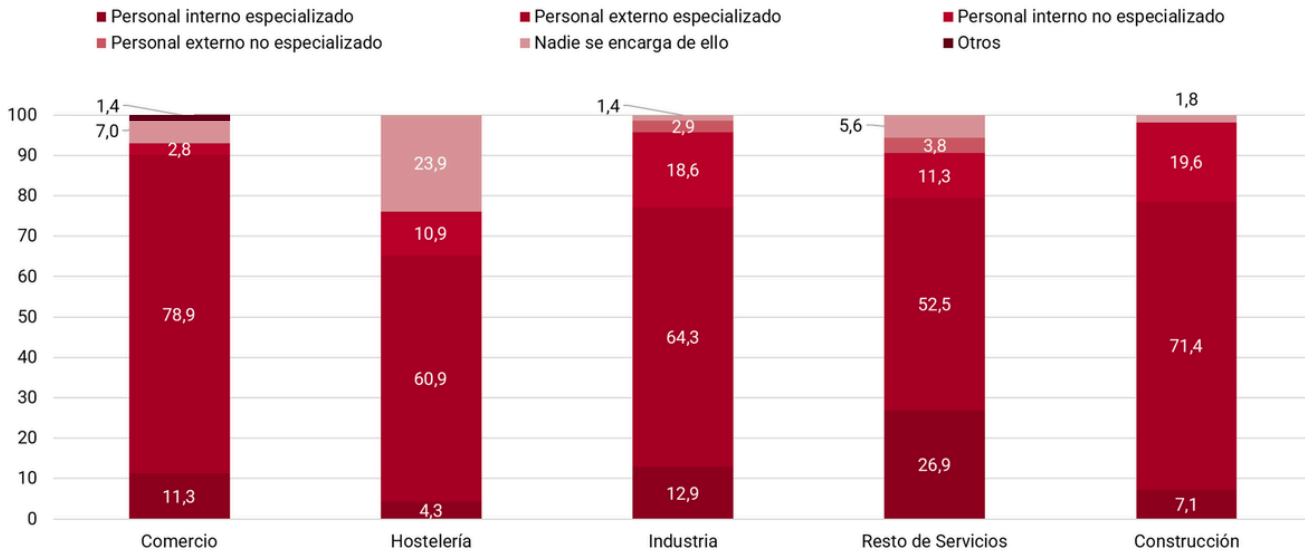



Fuente: Cámara de España

Por sector de actividad, en general, **todos dependen en gran medida de proveedores externos; destaca el sector turismo, con el mayor porcentaje de empresas que no dispone de recursos humanos para la gestión de la ciberseguridad, el 23,9% de las empresas.**

En comercio y construcción, predomina el personal externo especializado con un 78,9% y 71,4%, respectivamente; mientras que el personal interno especializado apenas alcanza el 11,3% y 7,1%. En hostelería e industria, la externalización sigue siendo mayoritaria (60,9% y 64,3%, respectivamente).

### ¿Quién gestiona la ciberseguridad de la empresa?, por sector (%)

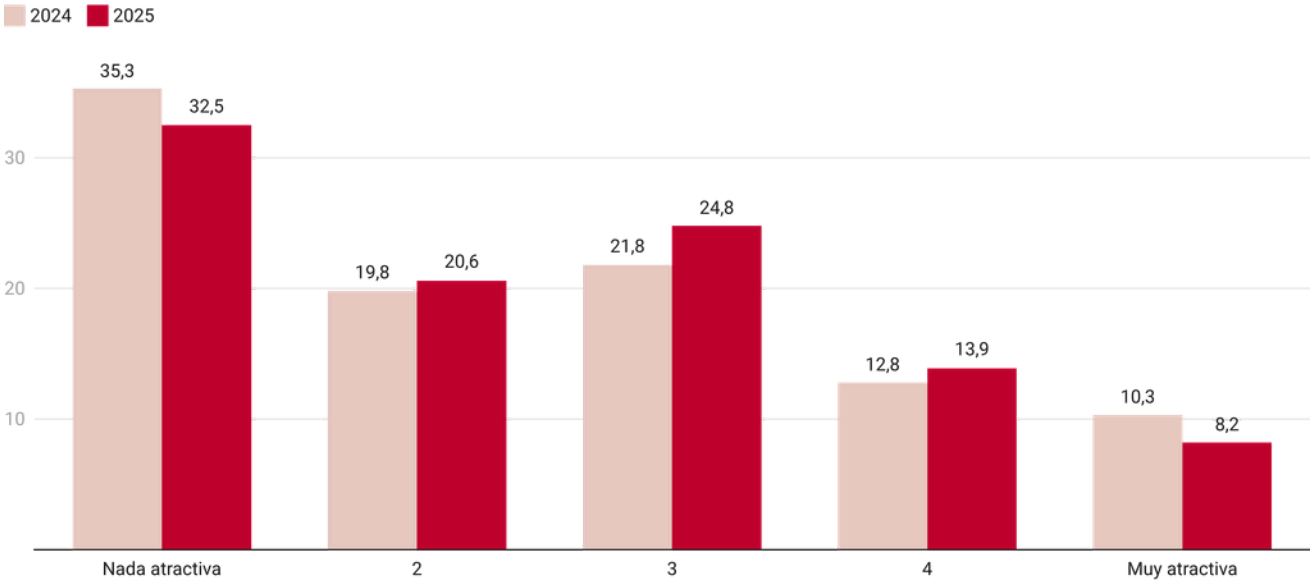



Fuente: Cámara de España

## Riesgo de sufrir un ciberataque: autopercepción de atractivo para los ciberdelincuentes

**La mayoría de las empresas se perciben como poco atractivas para los ciberdelincuentes:** en 2025, el 53,1% de las empresas encuestadas consideran que son nada o poco atractivas para los ciberdelincuentes, ligeramente inferior a la encuesta anterior (55,1%). Un 22,1% de las empresas percibe que son un atractivo alto o muy alto en 2025, similar al 23,1% de 2024.

### Atractivo de la empresa para los ciberdelincuentes (%)

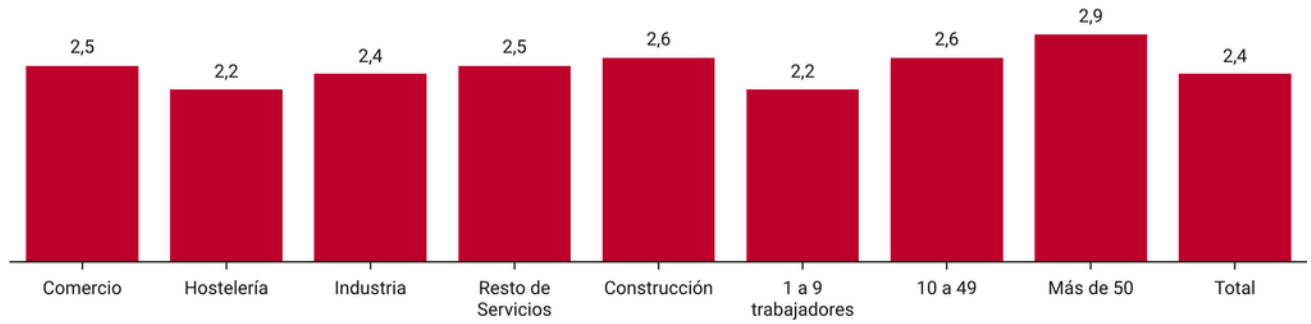



Fuente: Cámara de España

Las empresas más grandes tienen una percepción del riesgo ante los ciberdelincuentes mayor, con un valor medio de 2,9, frente a 2,2 en las microempresas (1 a 9 empleados). Por sectores, construcción (2,6), resto de servicios y comercio (2,5) presentan los mayores niveles medios de percepción de atractivo frente a ciberdelincuentes, mientras que las empresas hoteleras son las que se consideran menos propicias (2,2) para los ciberdelincuentes.

## Atractivo para los ciberdelincuentes, por sector y tamaño

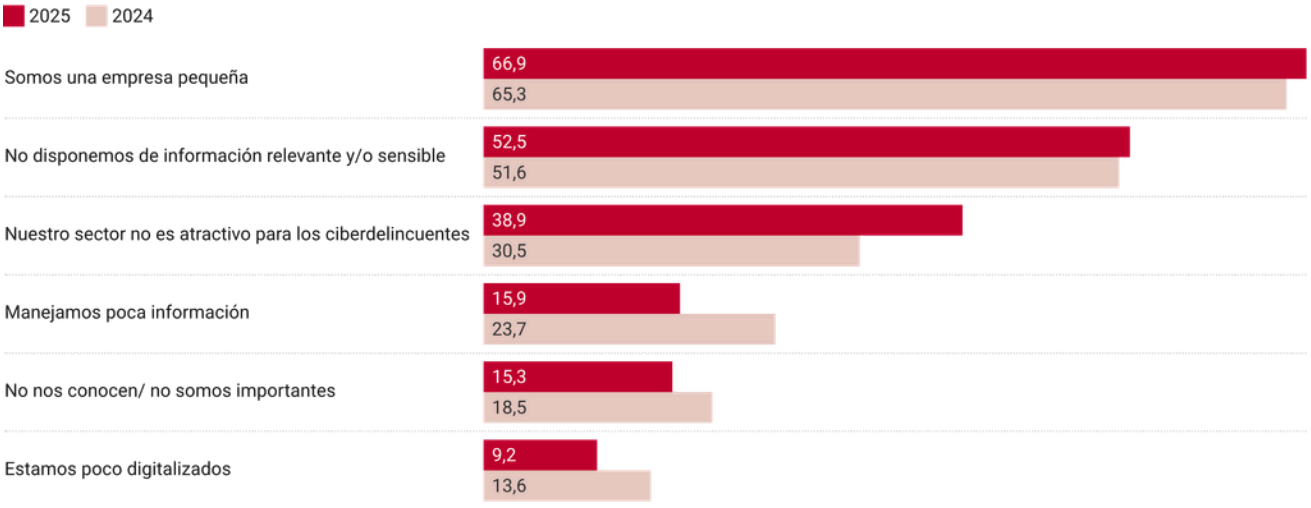
(valor medio, donde 1 es muy bajo y 5 muy elevado)




Fuente: Cámara de España

**El principal motivo por el que las empresas se consideran poco atractivas para los ciberdelincuentes sigue siendo su tamaño reducido,** con un ligero aumento en 2025 (66,9%) respecto a 2024 (65,3%). También destaca la percepción de no disponer de información relevante o sensible, que se mantiene estable (52,5% en 2025 frente a 51,6% en 2024). Sin embargo, **se observa una disminución significativa en la idea de manejar poca información,** lo que restaría interés para la ciberdelincuencia (15,9% en 2025 frente a 23,7% en 2024). Por otro lado, la baja digitalización como motivo cae entre las opciones señaladas por las empresas al 9,2%, lo que corroboraría el mayor nivel de digitalización que perciben las empresas en 2025, que se ha descrito anteriormente.

## Motivos por los que considera que la empresa es un objetivo poco atractivo para los ciberdelincuentes* (%)




** Empresas que valoran su atractivo para los ciberdelincuentes entre 1 y 3 puntos.*

Fuente: Cámara de España

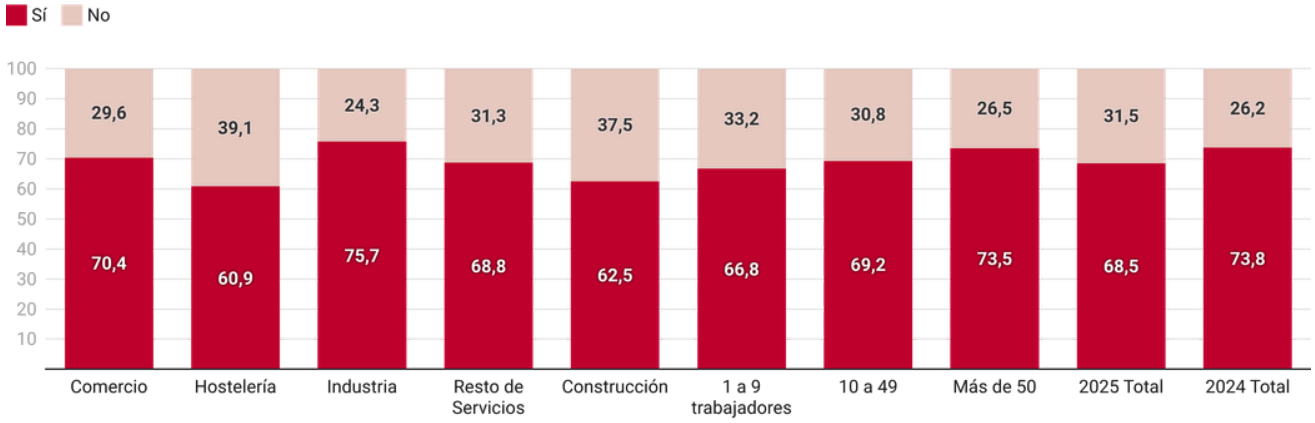
# Planificación de la ciberseguridad y medidas adoptadas

A continuación, se analiza la manera en que las empresas consultadas se protegen de las ciberamenazas. En este sentido, se profundiza en la percepción de seguridad que tienen las compañías ante los ciberataques, la existencia o no de una planificación específica en materia de ciberseguridad, así como en las características de las medidas establecidas para defenderse.

## Protección y planificación ante los ciberataques

Las empresas perciben un aumento a la vulnerabilidad frente a la ciberdelincuencia. En 2025, **el 68,5% de las empresas encuestadas consideran que están bien protegidas contra ciberataques, por debajo del 73,8% en 2024.** El **sector industrial es el más confiado (75,7%)**, mientras que construcción y turismo presentan menor percepción de protección, por debajo de la media, con 62,5% y 60,9%, respectivamente.

### Considera que actualmente su empresa está bien protegida contra los ciberataques (%)

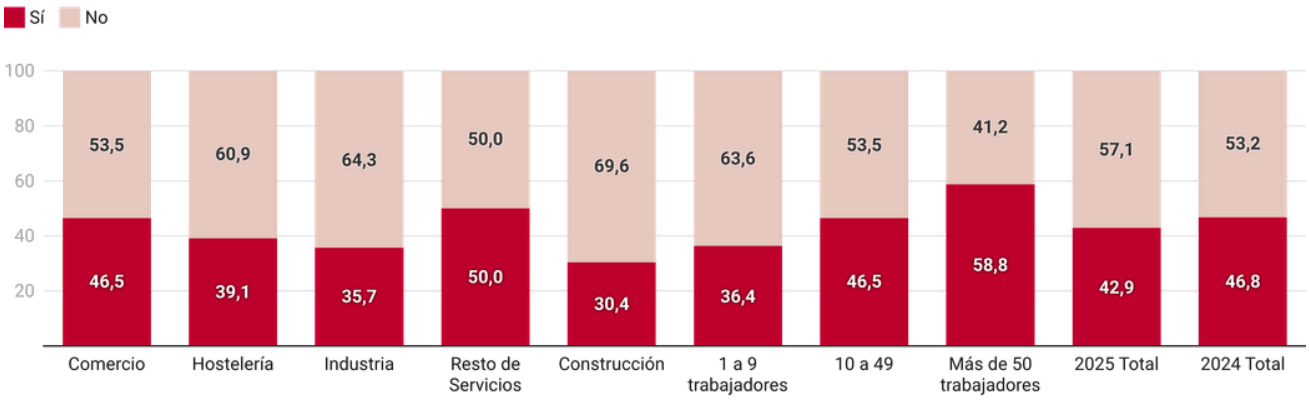



Fuente: Cámara de España

En 2025, **menos de la mitad de las empresas cuenta con una estrategia de ciberseguridad**, el 42,9%. Quizá porque como se ha señalado anteriormente, la mayoría (68,5%) considera que está bien protegida frente a ciberataques. **Por sectores, aquellos con menor implantación de estrategias (industria y construcción)** coinciden con percepciones más bajas de protección, lo que refuerza la relación entre planificación y confianza.

Por tamaño empresarial, se dibuja una **relación directa entre la existencia de una estrategia de ciberseguridad y la dimensión empresarial. Así, el 58,8% de las empresas de más de 50 trabajadores sí disponen de una política de ciberseguridad, frente al 36,4% de las empresas de 1 a 9 asalariados.**

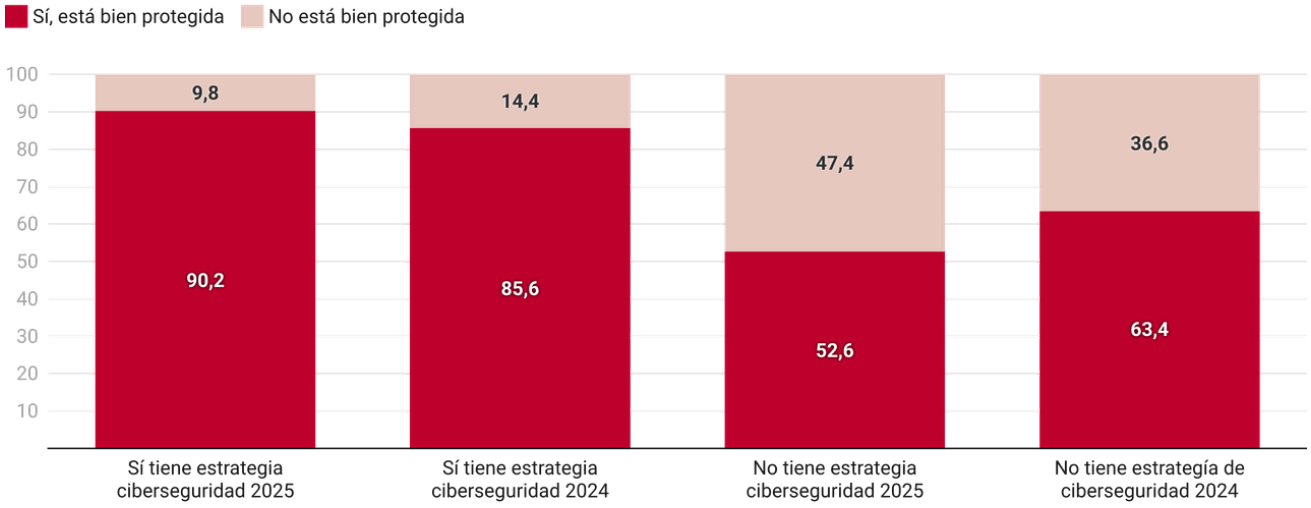
### Existencia de una estrategia/política de ciberseguridad en la empresa, por sector y tamaño (%)




Fuente: Cámara de España

El análisis de la percepción de seguridad frente a los ciberataques, según las empresas dispongan o no de una estrategia de ciberseguridad, muestra una diferencia notable: **aquellas empresas que cuentan con una estrategia definida se sienten significativamente más seguras, percepción que además se intensifica en 2025.** En concreto, el 90,2% de las empresas con una política de ciberseguridad en 2025 se considera bien protegida, frente al 52,6% de las que afirman sentirse protegidas aun sin disponer de una estrategia implementada.

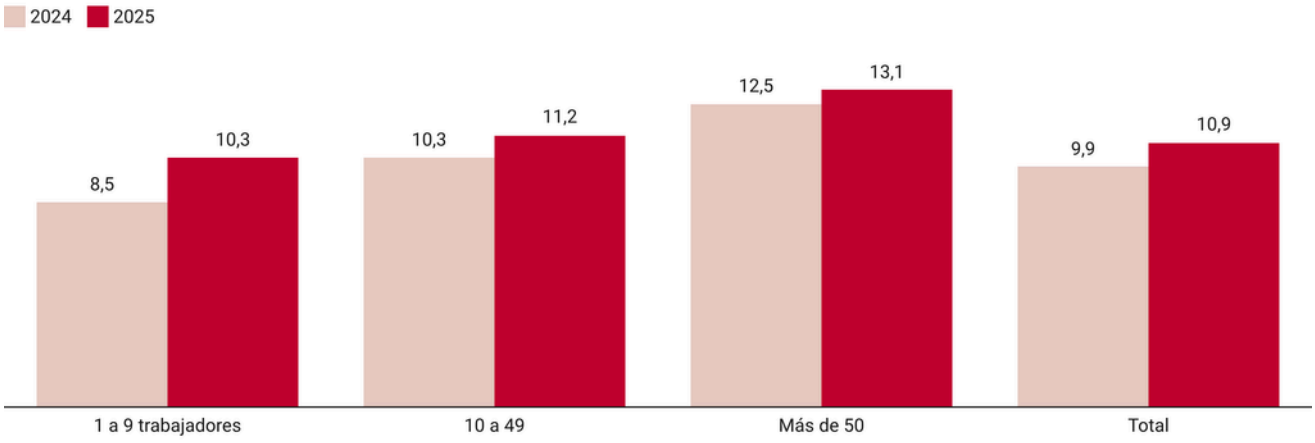
## Percepción de protección, según la existencia o no de una política/estrategia de ciberseguridad en la empresa (%)




Fuente: Cámara de España

En 2025, **el número medio de medidas de ciberseguridad implantadas aumenta pasando de 9,9 en 2024 a 10,9. En todos los tamaños de empresa, especialmente en las más pequeñas** (de 8,5 a 10,3), lo que indica un esfuerzo tangible por mejorar la protección.

## Número medio de medidas de ciberseguridad implantadas, por tamaño



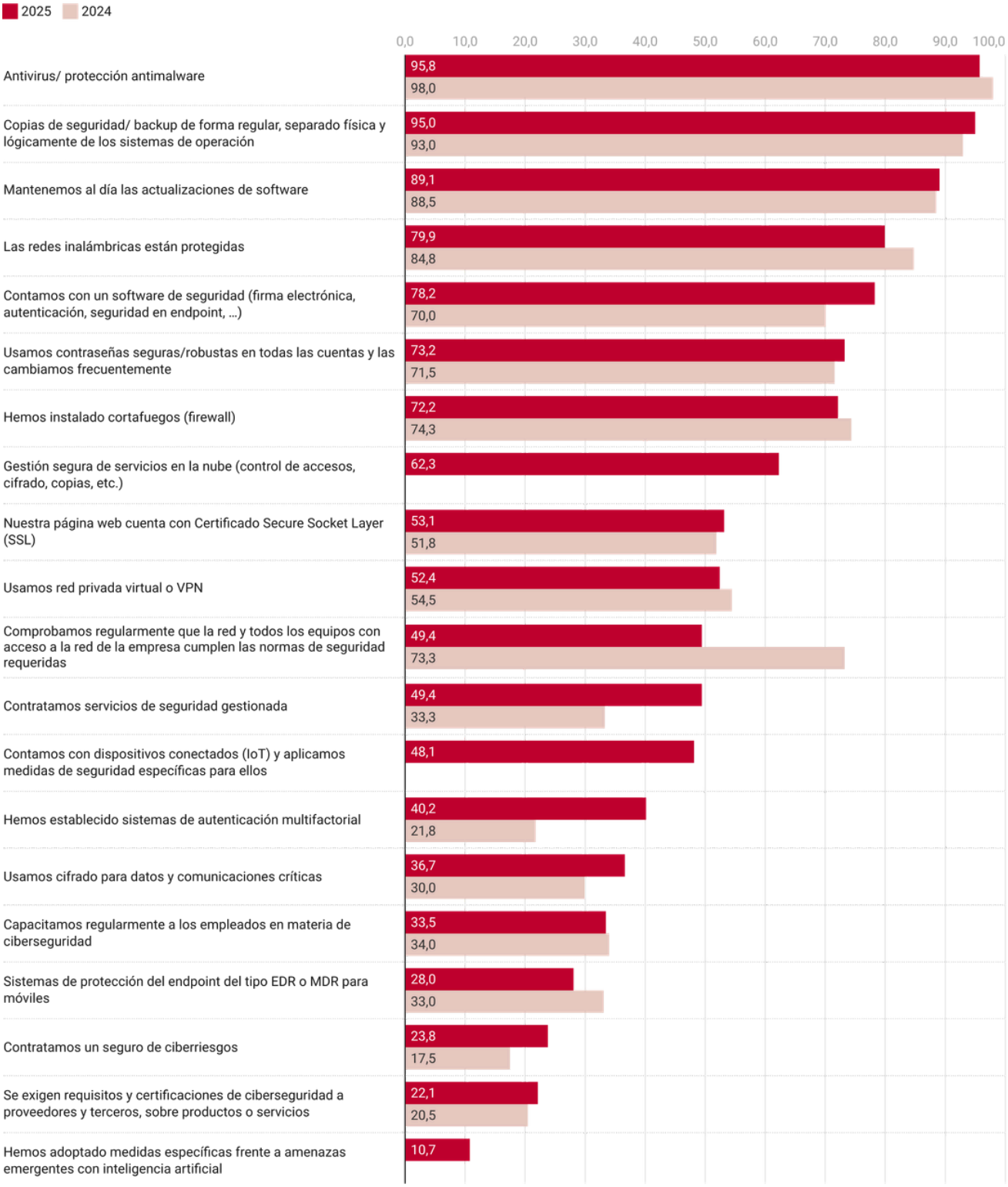

Fuente: Cámara de España

# Medidas de ciberseguridad implementadas

En 2025, **las empresas muestran una tendencia hacia la consolidación de medidas básicas de ciberseguridad: antivirus y protección antimalware (95,8%), copias de seguridad / backup de forma regular, separado física y lógicamente de los sistemas de operación (95,0%) y actualizaciones de software (89,1%) son prácticamente universales.** Sin embargo, l**as medidas más avanzadas y estratégicas siguen siendo minoritarias**: solo el 10,7% adopta soluciones frente a amenazas emergentes con IA, y apenas el 23,8% contrata seguros de ciberriesgos.

Otras medidas de ciberseguridad implementadas por, aproximadamente, tres cuartas partes de las empresas encuestadas son la protección de las redes inalámbricas (79,9%), el software de seguridad (firma electrónica, autenticación, seguridad en *endpoint*) (78,2%), uso de contraseñas seguras/robustas en todas las cuentas y cambio frecuentemente de las mismas (73,2%) e instalación de cortafuegos (firewall) (72,2%). Por otro lado, se observa un avance significativo, respecto al año anterior, en medidas como sistemas de autenticación multifactorial implementada por el 40,2% de las empresas encuestadas en 2025 frente al 21,8% de 2024 o contratación de servicios de seguridad gestionada pasando al 49,4% en 2025 desde el 33,3% en 2024.

## Medidas de ciberseguridad implementadas por las empresas (%)




Fuente: Cámara de España

Por el contrario, se reduce el porcentaje de empresas que comprueba regularmente que la red y todos los equipos con acceso a la red de la empresa cumplen con las normas del 73,3% en 2024 al 49,4% en 2025.

**Las empresas muestran diferencias en las medidas de ciberseguridad según su tamaño. En 2025, prácticamente todas las empresas españolas encuestadas han implantado medidas básicas de ciberseguridad, aunque el porcentaje aumenta con la dimensión empresarial.** Así, el antivirus está instalado en el 96,2% de las empresas de 1 a 9 trabajadores, en el 95,1% de las de 10 a 49 trabajadores y en el 97,1% de las de más de 50 trabajadores. En cuanto a las copias de seguridad, el 93,5% de las empresas de 1 a 9 trabajadores las realizan, el 95,7% en las de 10 a 49 trabajadores y el 100% en las de más de 50 trabajadores.

Sin embargo, se observan diferencias significativas en medidas más avanzadas, como la instalación de cortafuegos (firewall): el 94,1% de las empresas con más de 50 trabajadores frente al 66,8% de las microempresas (1 a 9 trabajadores). También en el uso de redes privadas virtuales (VPN): el 76,5% en empresas grandes frente al 44,0% en microempresas.

Por otro lado, las empresas aún no han adoptado masivamente medidas específicas frente a amenazas emergentes relacionadas con la Inteligencia Artificial, como formación sobre suplantaciones mediante *deepfakes*, detección de mensajes generados por IA o controles reforzados para prevenir fraudes automatizados. Según los resultados de la encuesta, solo el 17,6% de las empresas de más de 50 trabajadores han implementado medidas contra amenazas basadas en IA, porcentaje que desciende al 6,5% en las empresas de 1 a 9 trabajadores.

**Medidas de ciberseguridad implementadas por las empresas, en 2025, por tamaño (%)**


Fuente: Cámara de España

# Barreras a la mejora de la ciberseguridad

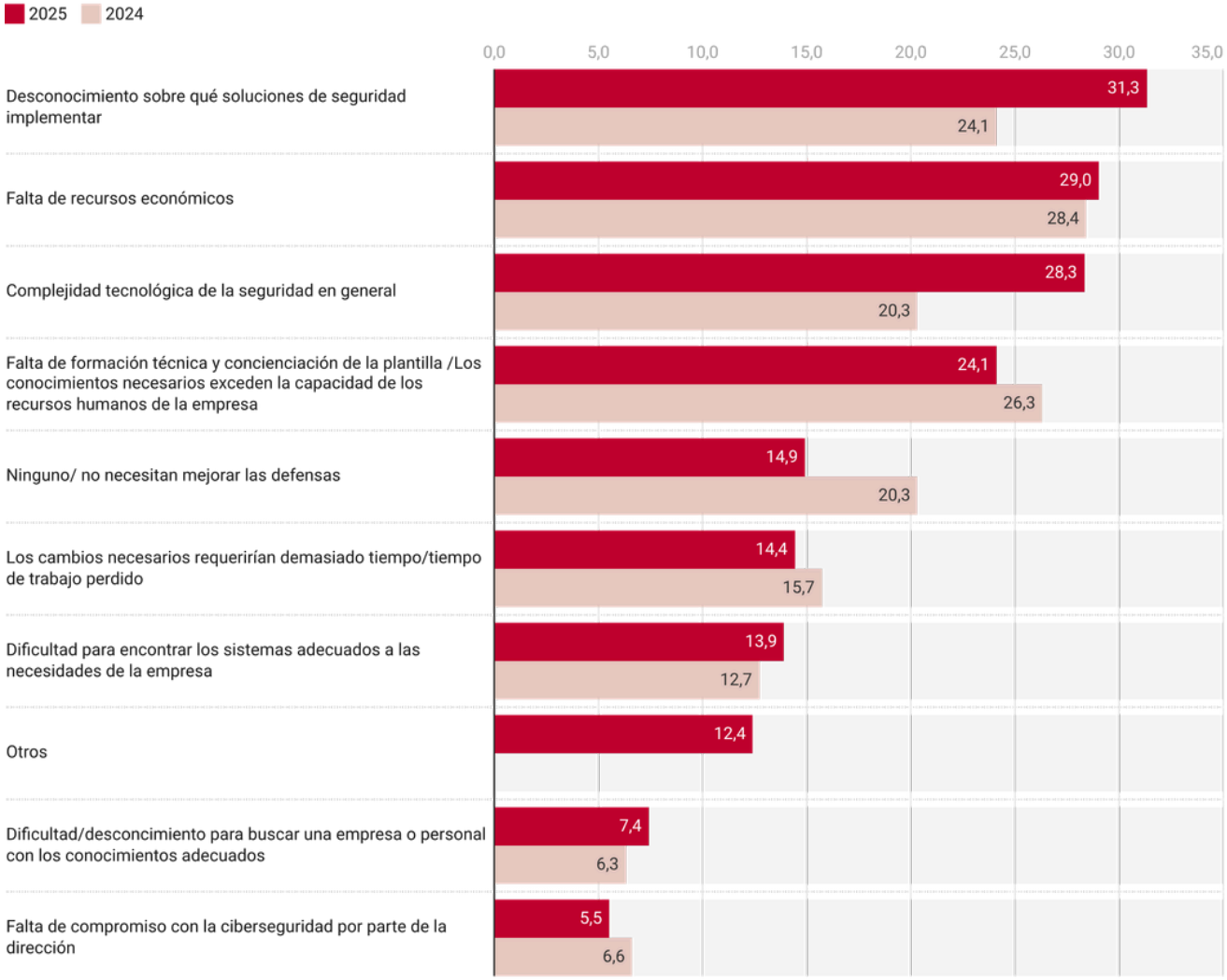
En este apartado se analizan las posibles barreras que obstaculizan o impiden la mejora de la ciberseguridad en las empresas.

## Elementos que dificultan a las empresas mejorar sus defensas ante las ciberamenazas

En 2025, **las principales barreras a las que se enfrentan las empresas para mejorar la defensa contra los ciberataques se concentran en el desconocimiento sobre qué soluciones implementar (31,3%) y la complejidad tecnológica (28,3%),** ambas con incrementos significativos respecto a 2024, lo que evidencia que el reto ya no es solo económico, sino estratégico y técnico. La limitación presupuestaria presenta un ligero repunte: el 29,0% de las empresas encuestadas lo han señalado como un obstáculo para la implementación de medidas frente a los ciberataques (28,4% en 2024).

La dificultad para encontrar sistemas adecuados a las necesidades de las empresas y el tiempo que requieren los cambios necesarios para la implementación de las medidas son factores que destacan aproximadamente el 14% de las empresas, en ambos casos. **Se reduce el porcentaje de empresas encuestadas que considera que no necesitan mejorar sus defensas contra los ciberataques, del 20,3% al 14,9%.**

**Factores que impiden a las empresas mejorar sus defensas contra los ciberataques (%)**



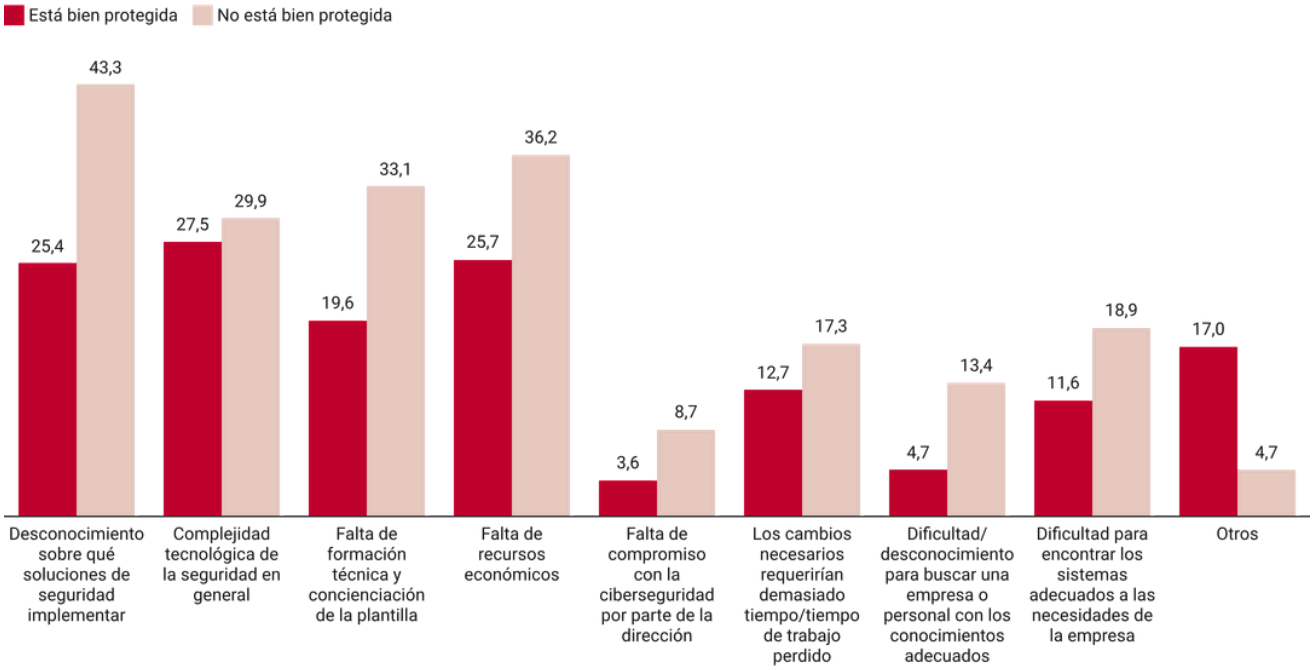

Fuente: Cámara de España

El análisis de los factores que impiden a las empresas mejorar en la defensa contra los ciberataques en función de si la empresa considera que está bien protegida o no frente a los ciberataques, revela diferencias entre ambos grupos de empresas.

Para **las empresas que perciben que no están bien protegidas, todos los obstáculos son señalados en mayor porcentaje.** El desconocimiento sobre qué soluciones implementar (43,3%) y la falta de recursos económicos (36,2%) son las barreras más críticas, muy por encima de las empresas que se perciben seguras (25,4% y 25,7%, respectivamente). También destaca la falta de formación técnica (33,1%) y la complejidad tecnológica (29,9%), lo que indica que la percepción de vulnerabilidad está fuertemente ligada a carencias de conocimiento y presupuesto.

En contraste, **las empresas que se consideran bien protegidas presentan porcentajes significativamente menores en estos factores, pero muestran cierta dificultad por la complejidad tecnológica de la seguridad en general (27,5%),** lo que sugiere que incluso las empresas más preparadas se enfrentan a retos de adaptación tecnológica. Este escenario evidencia que mejorar la protección no depende solo de inversión, sino de orientación estratégica, formación especializada y soluciones escalables que reduzcan la complejidad.

**Factores que impiden a las empresas mejorar sus defensas contra los ciberataques, según se sienten bien protegidas o no (%)**



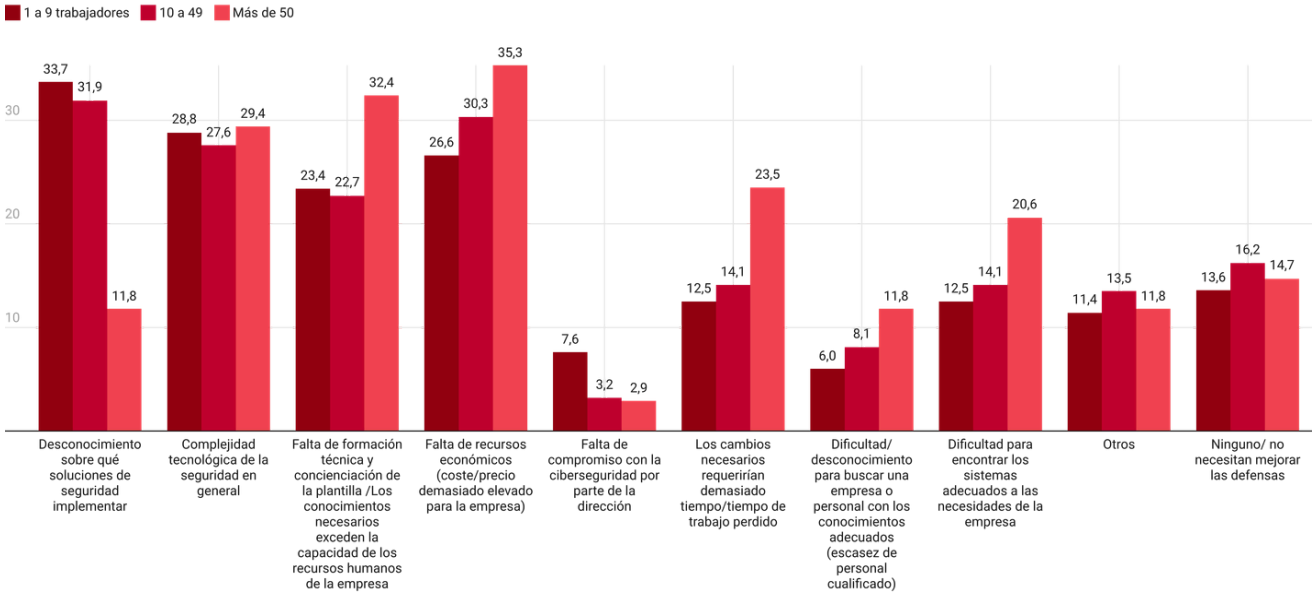

Fuente: Cámara de España

**El análisis por tamaño de empresa muestra diferencias en las barreras a las que hacen frente las empresas para mejorar la ciberseguridad.**

Uno de los factores que obstaculiza, en mayor medida, a la implementación de medidas frente a los ciberataques por parte de las empresas es la falta de recursos económicos, como ponen de manifiesto el 35,3% de las empresas de más de 50 trabajadores para los que, junto con la falta de formación técnica (32,4%), es el factor que más limita la ciberseguridad entre las empresas de mayor dimensión.

Las empresas de 1 a 9 trabajadores y de 10 a 49 trabajadores, también señalan la falta de recursos económicos como uno de los factores limitantes de su defensa frente a los ciberataques, con un 26,6% y un 30,3%, respectivamente. Sin embargo **la falta de recursos económicos para estas empresas no es el mayor obstáculo para la protección ante la ciberdelincuencia, sino que la falta de conocimiento sobre las soluciones de seguridad que deberían implementar les supone la mayor limitación** (para el 33,7% de las empresas de 1 a 9 trabajadores y 31,9% de 10 a 50, frente al 11,8% de las empresas de más de 50 trabajadores).

## Factores que impiden a las empresas mejorar sus defensas contra los ciberataques, según tamaño (%)

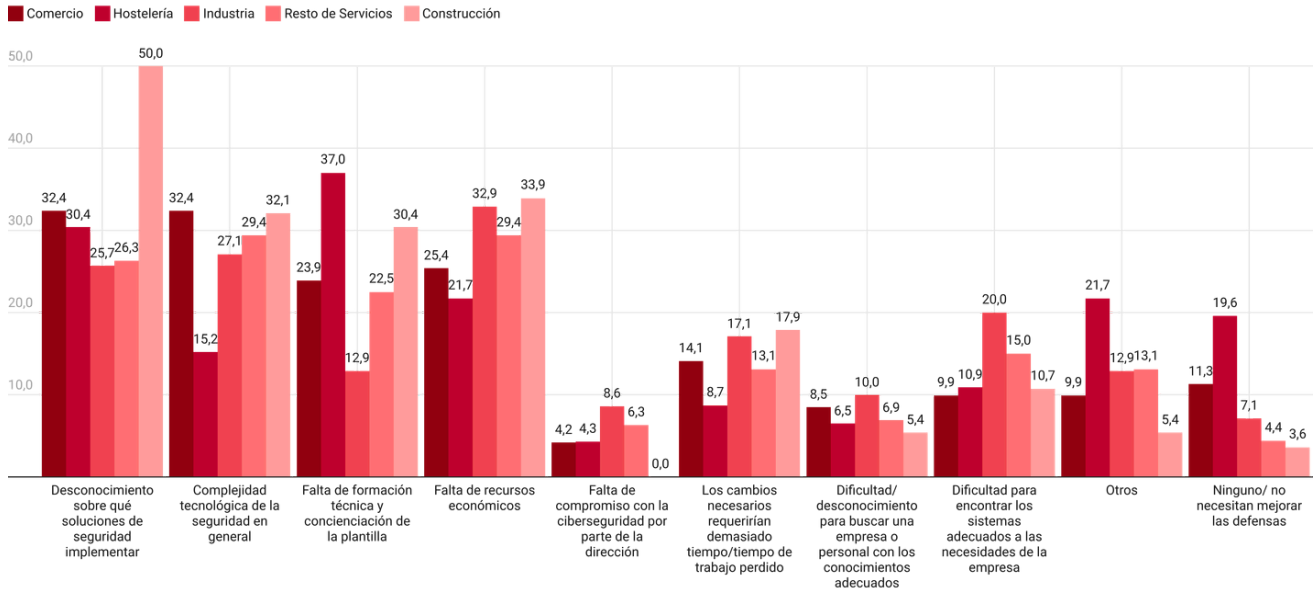



Fuente: Cámara de España

**Los factores que dificultan la mejora de las defensas contra ciberataques varían según el sector, pero destacan tres obstáculos principales:** el desconocimiento sobre qué soluciones implementar, la falta de recursos económicos y la falta de formación técnica.

En construcción, el desconocimiento sobre qué soluciones implementar alcanza el 50%, muy por encima de otros sectores como comercio (32,4%) o industria (35,6%). En cuanto a la falta de formación técnica, las empresas pertenecientes a la hostelería lideran con un 37%, seguida por construcción (30,4%) y comercio (23,9%). La falta de recursos económicos también es significativa, con porcentajes superiores al 30% en construcción (33,9%) e industria (32,9%). Otros factores, como la complejidad tecnológica, afectan especialmente a comercio (32,4%) y construcción (32,1%). Estos datos reflejan que la mejora en ciberseguridad no depende únicamente de inversión, sino también de capacitación y asesoramiento especializado.

## Factores que impiden a las empresas mejorar sus defensas contra los ciberataques, según sector (%)




Fuente: Cámara de España

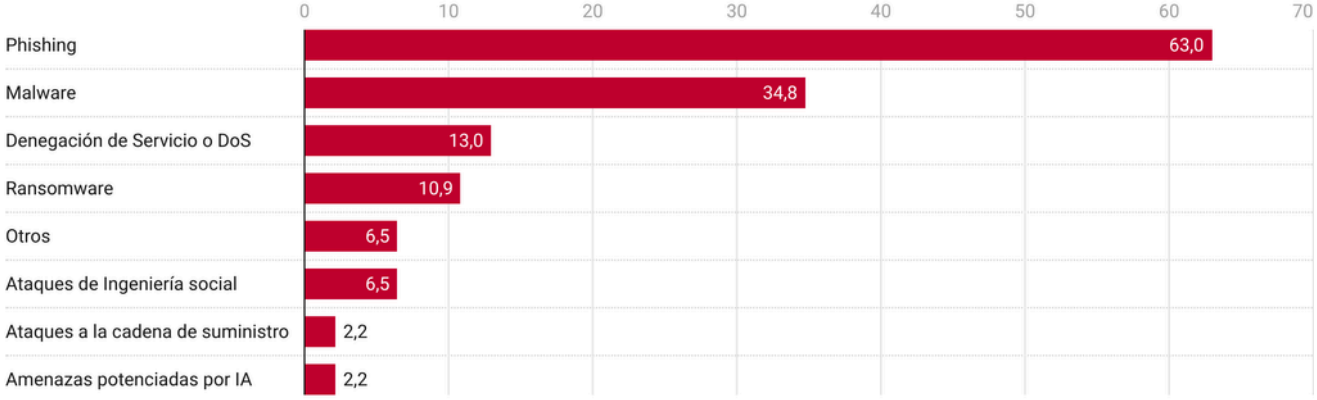
# Incidentes de seguridad experimentados

A continuación, se profundiza en la incidencia de los ciberataques sobre las empresas, la tipología de los incidentes de seguridad que ocurren con mayor frecuencia, los efectos directos y consecuencias de los mismos, así como en la percepción de vulnerabilidad que las empresas afectadas tienen ante la posibilidad de sufrir un nuevo ataque. Finalmente, se indaga especialmente sobre el efecto potencial del teletrabajo sobre la ciberseguridad.

## Tipología de los ciberataques sufridos

**Algo más de una de cada diez de las empresas consultadas (11,4%) ha sufrido algún ciberataque en los últimos 24 meses,** siendo los más habituales el phishing (correos electrónicos con enlaces o archivos adjuntos que conducen a sitios maliciosos) (63,0%), el *malware* (infecta el ordenador y lo deja inservible) 34,8% y la Denegación de Servicio o DoS (interrumpe el funcionamiento de una máquina o servicio conectado a la red), 13,0%.

### Tipo más frecuente de ciberataque sufrido en los últimos 24 meses* (%)



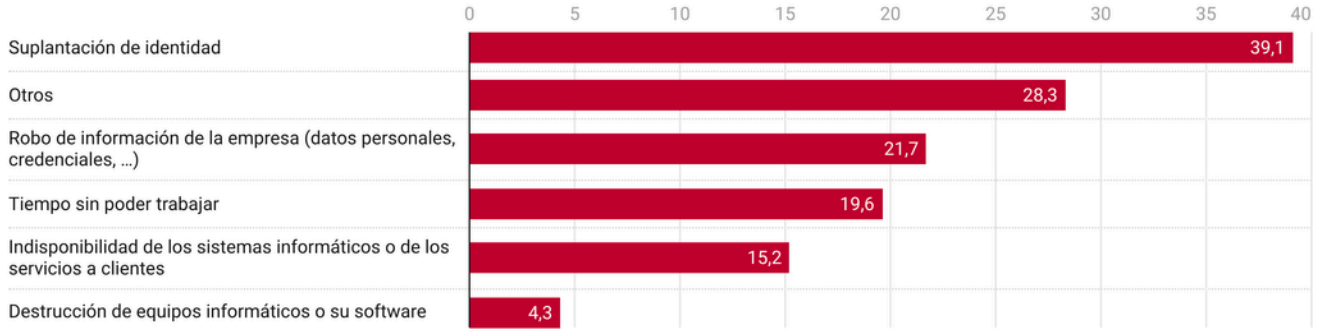

** Empresas que han sufrido un ciberataque en los últimos 24 meses.*

Fuente: Cámara de España

## Efectos directos y consecuencias

**El efecto directo más frecuente para las empresas que han sufrido un ciberataque es la suplantación de identidad (39,1%).** Le sigue la categoría Otros (28,6%), que refleja una diversidad de impactos no estandarizados, posiblemente relacionados con interrupciones menores o daños indirectos. Entre los efectos operativos más relevantes destacan el robo de información (21,7%), el tiempo sin poder trabajar (19,6%), la indisponibilidad de sistemas (15,2%) y, por último, la destrucción de equipos (4,3%).

### Principales efectos directos del ciberataque* (%)




** Empresas que han sufrido un ciberataque en los últimos 24 meses.*

Fuente: Cámara de España

Muchos ciberataques parecen no generar consecuencias visibles para las empresas, así lo indican un 45,7% de las empresas encuestadas. El incremento de costes y la pérdida de reputacional es señalado por el 39,1% y 13,0% respectivamente.

### Principales consecuencias del ciberataque*(%)

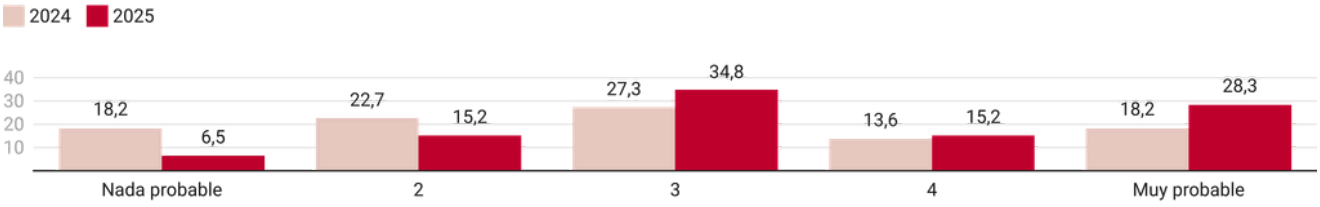

** Empresas que han sufrido un ciberataque en los últimos 24 meses.*

Fuente: Cámara de España

## Posibilidad de sufrir un nuevo ciberataque

Consultadas las empresas que han sufrido un ciberataque en los últimos 24 meses por la probabilidad de que en el año siguiente sean víctimas de un nuevo ciberataque, **se observa un incremento en la percepción de riesgo. Así, en 2025, el 43,5% de las empresas considera probable o muy probable sufrir un nuevo ciberataque frente al 31,8% del año anterior.** El porcentaje de empresas que se sitúan en una posición intermedia también es mayor, el 34,8% frente al 27,3%.

### Probabilidad de que la empresa sea víctima de un nuevo ciberataque en los próximos 12 meses*(%)



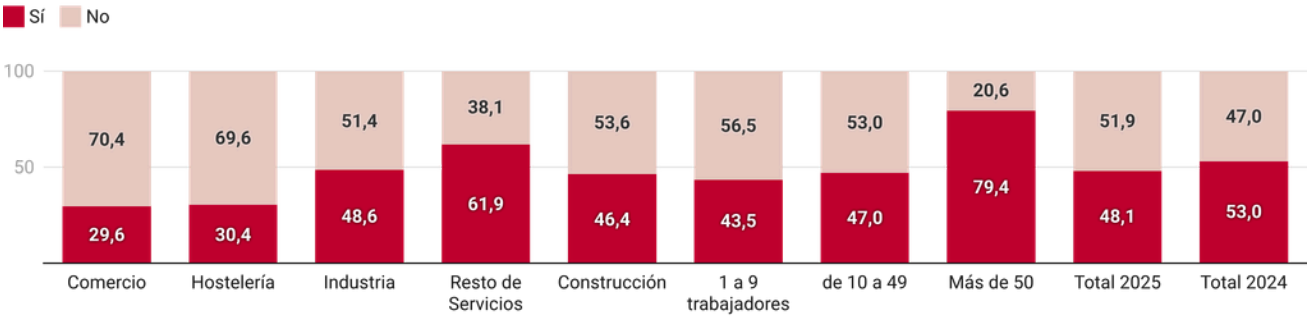

** Empresas que han sufrido un ciberataque en los últimos 24 meses.*

Fuente: Cámara de España

## Teletrabajo y vulnerabilidad ante los ciberataques

**Casi la mitad de las empresas encuestadas permite el teletrabajo, en concreto el 48,1%, porcentaje inferior a 2024, en el que el 53,0% de las empresas permitía el teletrabajo.** La posibilidad de teletrabajar varía significativamente según el sector y el tamaño de la empresa. En sectores como comercio (29,6%) y hostelería (30,4%), la opción de teletrabajo es limitada debido a la naturaleza presencial de estas actividades. En cambio, el resto de los servicios destaca con un 61,9%, siendo el sector más favorable para el trabajo remoto. Respecto al tamaño de la empresa, las grandes compañías (más de 50 trabajadores) presentan una alta posibilidad de teletrabajo (79,4%), mientras que las microempresas (1 a 9 trabajadores) apenas alcanzan el 43,5%.

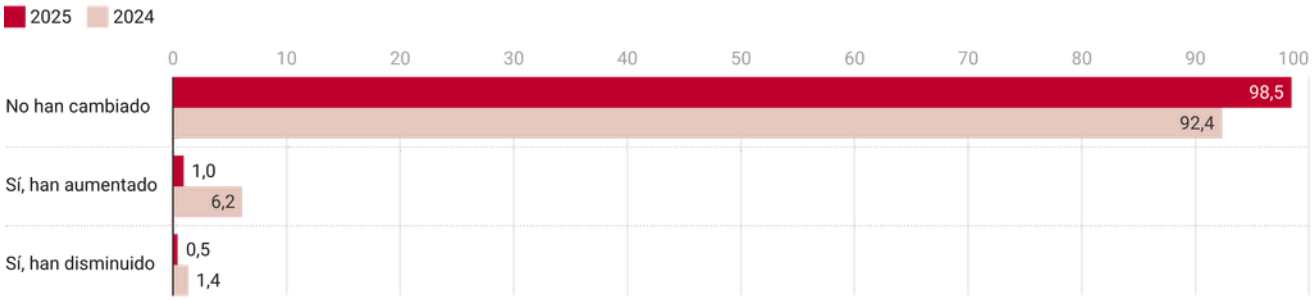
### Posibilidad de teletrabajar en las empresa (%)




Fuente: Cámara de España

Si bien esta práctica, a priori, podría implicar riesgos adicionales en la ciberseguridad, la gran mayoría de ellas declara que su implementación no ha supuesto un incremento en su vulnerabilidad ante los ciberataques. Así lo **manifiesta 98,5% de las empresas que considera que el número de ciberataques no se ha modificado con el establecimiento del teletrabajo** y solo un 1,0%.

**Cambio en el número de ciberataques desde la implantación del teletrabajo*(%)**




** Empresas que han implantado el teletrabajo*

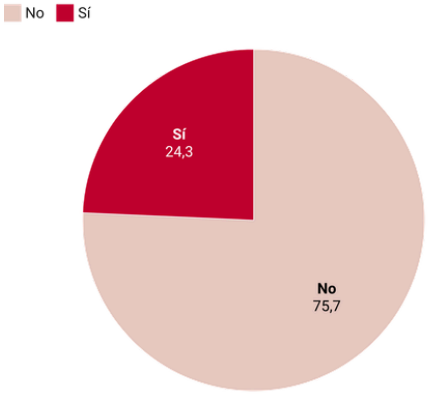
Fuente: Cámara de España

# El futuro: inversión prevista en ciberseguridad

Finalmente, en este apartado se analiza las perspectivas de las empresas consultadas de reforzar sus defensas ante los ciberataques en un futuro próximo.

## Previsión de incremento de la inversión en seguridad

**Previsión de incrementar el presupuesto para ciberseguridad en los próximos 12 meses (%)**




** Empresas que han implantado el teletrabajo*

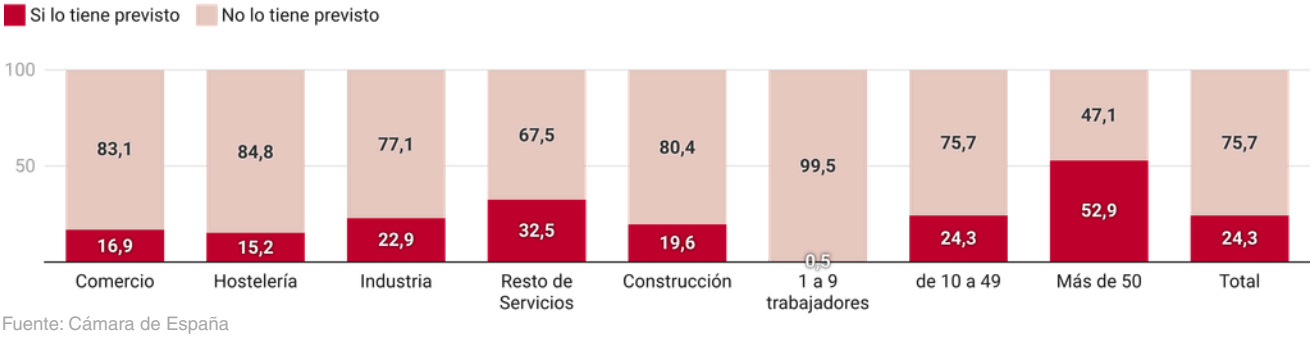
Fuente: Cámara de España

En 2025, **una de cada cuatro empresas españolas tiene previsto incrementar el presupuesto de ciberseguridad en los próximos 12 meses.** Esta proporción se mantiene constante respecto a 2024.

Las empresas del sector 'resto de servicios' son las que presentan la mayor previsión de inversión en ciberseguridad para el próximo año. Un 32,5% planea incrementar su presupuesto, lo que supone casi el doble que en sectores como hostelería o comercio.

Por tamaño, la previsión de inversión en ciberseguridad se incrementa según aumenta la dimensión empresarial. Así, más de la mitad de las empresas de más de 50 trabajadores (52,9%) tiene previsto aumentar su inversión en ciberseguridad frente al 24,3% de las empresas de 10 a 49 trabajadores o sólo el 0,5% de las empresas de 1 a 9 trabajadores.

**Previsión de incrementar el presupuesto en ciberseguridad en los próximos 12 meses, por sector y tamaño (%)**




Fuente: Cámara de España

En 2025, **el porcentaje de empresas que incrementarán más del 20% el presupuesto destinado a ciberseguridad sube a 37,3%, frente al 33,3% en 2024.** Por otro lado, los incrementos hasta el 10% disminuyen (30,5% en 2025 frente a 36,5% en 2024), mientras que los aumentos entre el 10% y el 20% se mantienen relativamente estables (32,2% en 2025 y 30,2% en 2024). Esto indicaría que las empresas en 2025 prevén dedicar un mayor parte del presupuesto a inversiones en ciberseguridad.

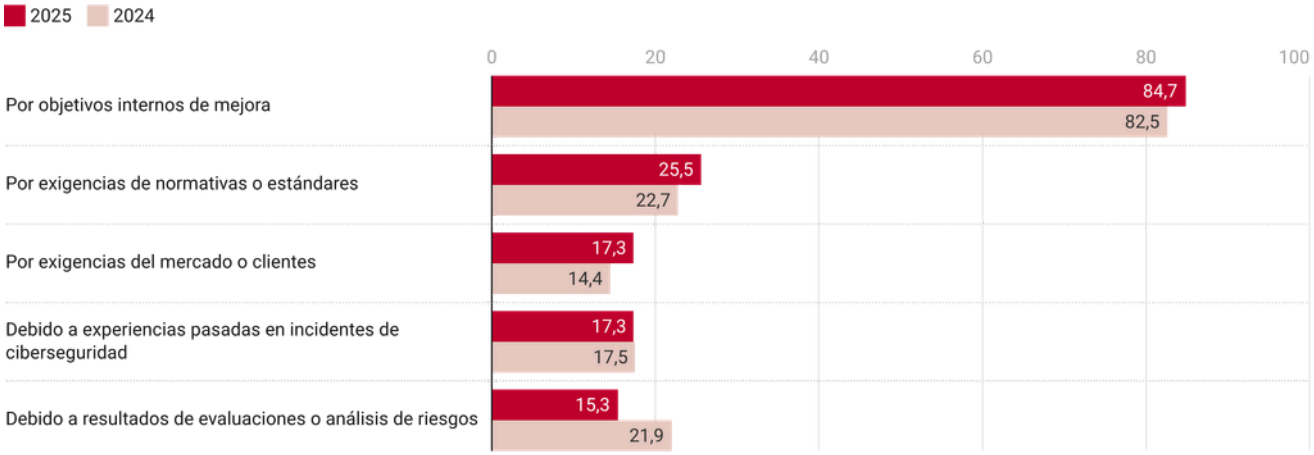
## Incremento aproximado del presupuesto en ciberseguridad* (%)


**Empresas que sí tienen previsto aumentar el presupuesto en ciberseguridad.*

Fuente: Cámara de España

A continuación se analizan los principales motivos de las empresas para incrementar el presupuesto dedicado a la ciberseguridad. **El motivo más relevante en 2025 y 2024 son los objetivos internos de mejora**, con porcentajes muy altos (84,7% en 2025 y 82,5% en 2024), lo que indica que las empresas priorizan la optimización interna. En segundo lugar, destacan las exigencias derivadas de normativas o estándares, que aumentan ligeramente en 2025 (25,5% frente a 22,7% en 2024). Por otro lado, los motivos relacionados con evaluaciones de riesgos disminuyen notablemente (de 21,9% en 2024 a 15,3% en 2025), mientras que las experiencias pasadas en incidentes y las exigencias del mercado se mantienen relativamente estables. Esto podría indicar una tendencia hacia la mejora proactiva en la ciberseguridad más que la reacción ante incidentes.

## Motivos para incrementar el presupuesto dedicado a la ciberseguridad*(%)




**Empresas que sí tienen previsto aumentar el presupuesto en ciberseguridad*

Fuente: Cámara de España

# Metodología

Los datos de este estudio se han obtenido a partir de una encuesta ad hoc realizada por la Cámara de Comercio de España en septiembre y octubre de 2025.

La muestra se compone de 400 empresas de al menos un asalariado en todo el territorio nacional y de todos los sectores de actividad, distribuidas de acuerdo con 2 criterios de desagregación: sector (Industria, Construcción, Comercio, Hostelería y Resto de Servicios) y tamaño (1 a 9 trabajadores, 10 a 49 trabajadores, más de 50 trabajadores).

El margen de error máximo para un nivel de confianza del 95% es de ±4,9%. Los resultados por tamaño y sector son orientativos, dado que la muestra no proporciona resultados estadísticamente significativos en estos casos.

*Elaborado por el Servicio de Estudios de la Cámara de Comercio de España.*


Cámara
de Comercio de España