Observatorio de Competitividad Empresarial

CIBERSEGURIDAD

Nº 11 / 2024

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 de España** 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.**

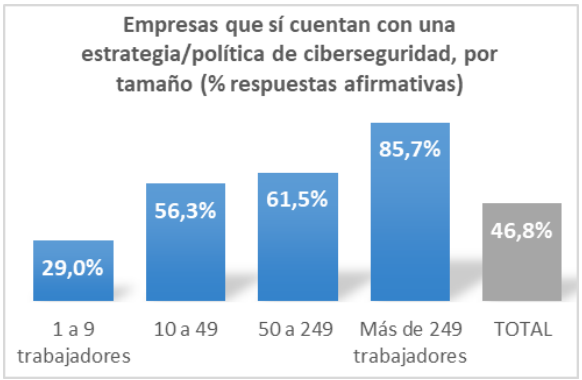
Resumen

Tan solo **el 24,3% de las empresas consultadas planea reforzar su ciberseguridad en los próximos 12 meses**, con un incremento medio de la inversión del 23,5%.

Y ello se debe a que **la mayoría de las compañías se sienten seguras**, ya sea por considerar que se encuentran bien protegidas (73,8%), porque se perciben como poco o nada atractivas para los ciberdelincuentes (55,3%), o bien porque tan solo un 11,0% de ellas han sufrido algún ciberataque en los últimos 24 meses.

Fuente: Cámara de Comercio de España.

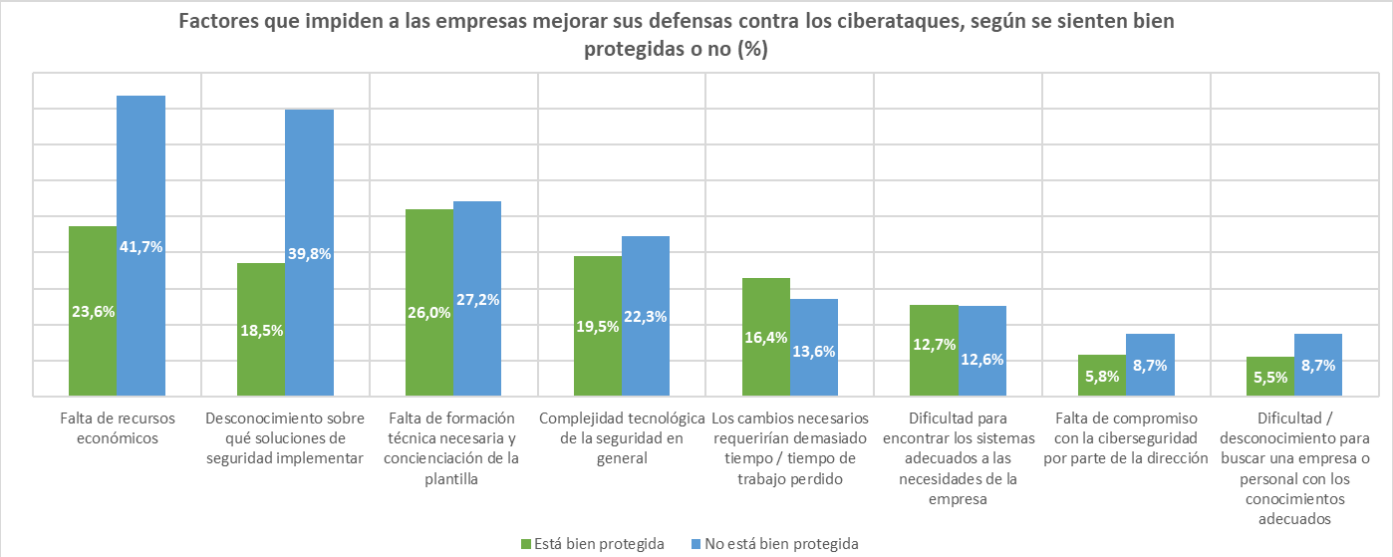
En lo que respecta a la gestión y planificación de la ciberseguridad, **el 73,0% de las empresas cuenta con personal especializado (53,0% externo y 20,0% interno), algo menos de la mitad (46,8%) dispone de una política/estrategia específica de ciberseguridad y tan solo el 34,0% desarrolla actividades de capacitación en la materia**.



Fuente: Cámara de Comercio de España.

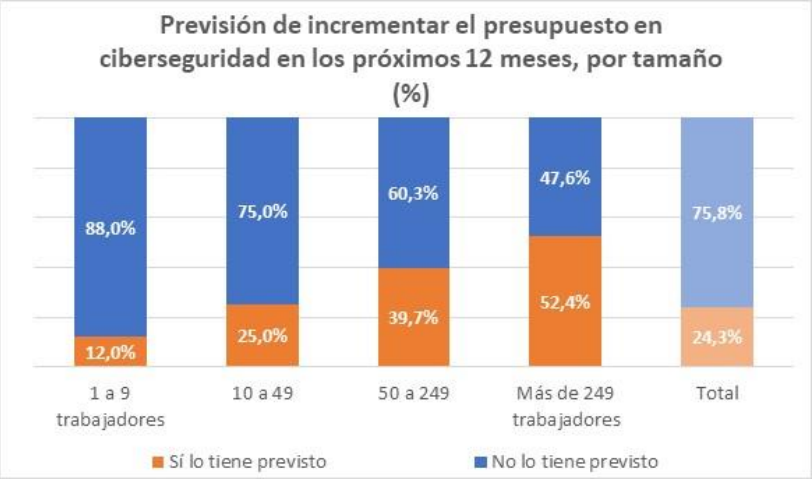
Entre las medidas de protección implementadas, la gran mayoría de las compañías ya dispone de antivirus / protección antimalware (98,0%), copias de seguridad / backup de forma regular, separado física y lógicamente de los sistemas de operación (93,0%), actualizaciones de software al día (88,5%), y redes inalámbricas protegidas (84,8%). También, algo menos de las tres cuartas partes tiene cortafuegos (74,3%), verifican regularmente que sus redes y equipos con acceso cumplan con las normas de seguridad (73,3%), usan contraseñas seguras y las cambian con frecuencia (71,5%) y cuentan con un software de seguridad (70,0%).

La falta de recursos económicos y el desconocimiento sobre qué soluciones de seguridad deben implementar surgen como dos impedimentos claros para mejorar las defensas ante las ciberamenazas, con especial incidencia entre aquellas empresas que declaran no estar bien protegidas.



Fuente: Cámara de Comercio de España.

La preocupación, la sensación de vulnerabilidad y la autopercepción de atracción para los ciberdelincuentes se incrementa conforme aumenta el tamaño de la empresa. Y en relación con ello, también adquieren mayor relevancia la especialización en la gestión de la ciberseguridad, la existencia de una planificación específica, el número y utilización de medidas de protección, y la dispocición a incrementar la inversión en ciberseguridad en los próximos 12 meses.



Fuente: Cámara de Comercio de España.

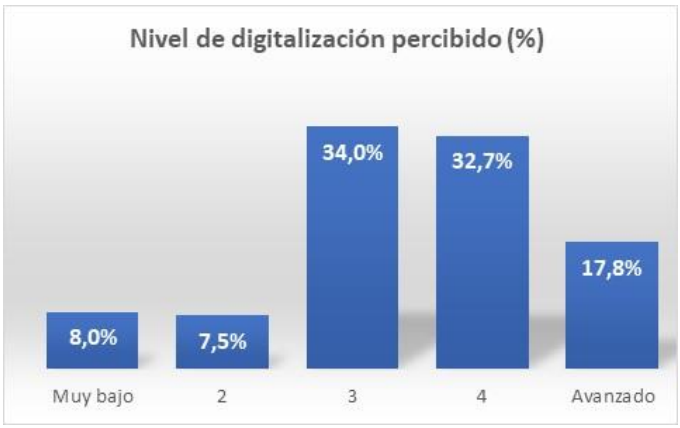
Contextualización: grado de digitalización de las empresas, gestión de la ciberseguridad y percepción del riesgo

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.

▶ Autopercepción del grado de digitalización de las empresas

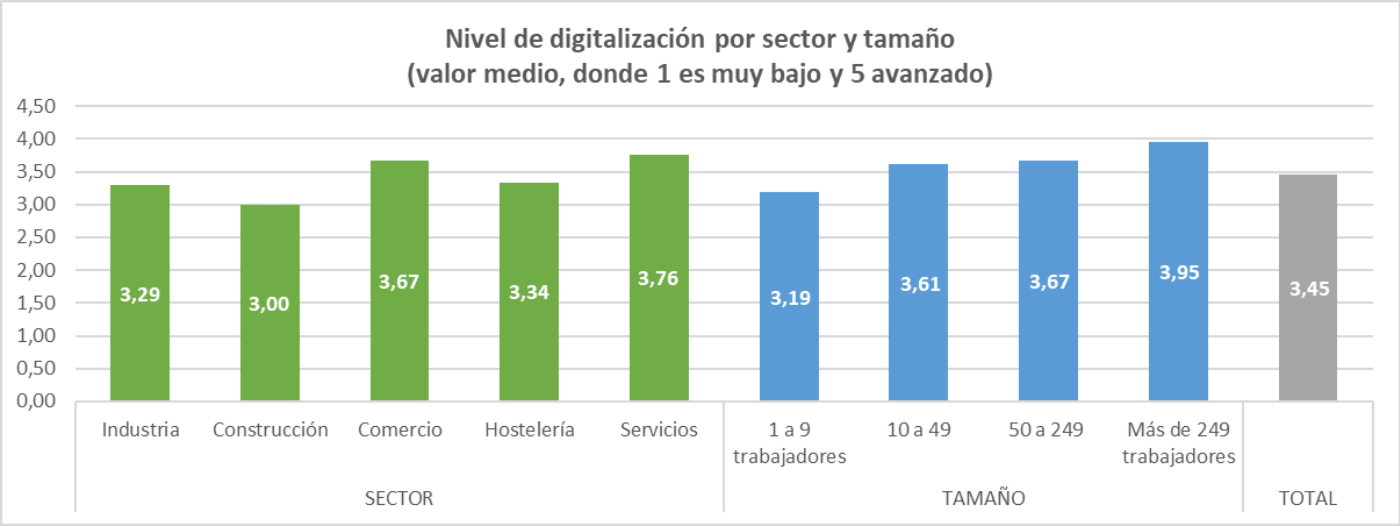
Las empresas españolas perciben su nivel de digitalización entre intermedio y avanzado (84,5%). En concreto, tan solo el 15,5% de las compañías valora su grado de digitalización como bajo o muy bajo, un 34,0% declara un nivel intermedio, en tanto que en un 50,5% de los casos el nivel de digitalización autopercibido es elevado (valoración atribuida entre 4 y 5).

Atendiendo al tamaño de las empresas, **el grado de digitalización aumenta según se incrementa el número de trabajadores,** pasando de una media de 3,19 puntos entre las más pequeñas hasta 3,95 puntos entre las de más de 249 trabajadores**.**



Fuente: Cámara de Comercio de España.

Por sectores, servicios (3,76) y hostelería (3,67) declaran, en promedio, un nivel de digitalización mayor. Por el contrario, en la construcción, el nivel de digitalización autopercido es menor en en el resto de sectores (3,00).



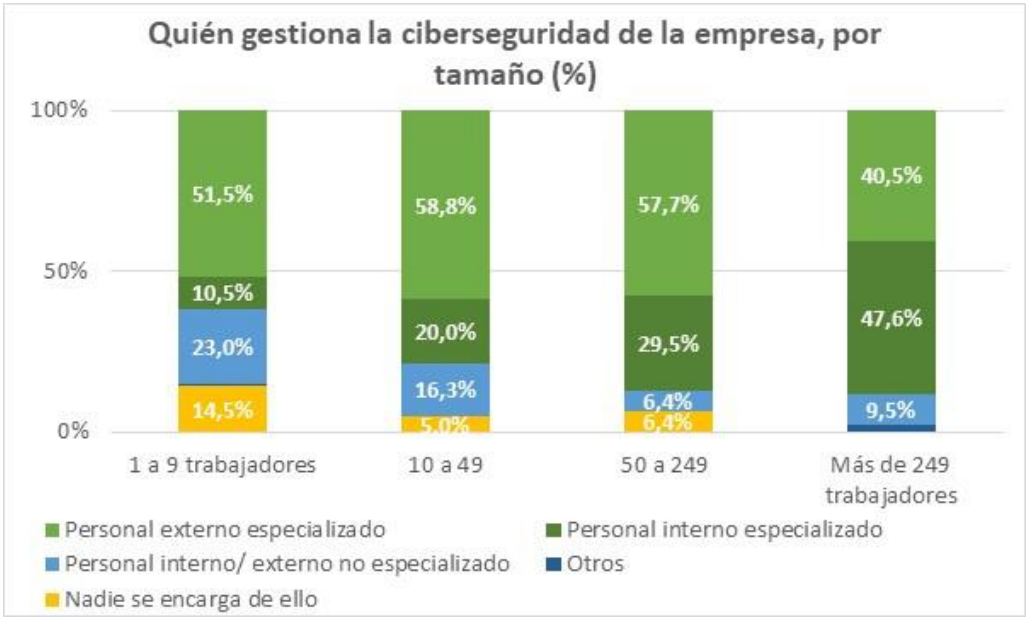
Fuente: Cámara de Comercio de España.

▶ Gestión de la ciberseguridad

Fuente: Cámara de Comercio de España.

El 73,0% de las empresas cuenta con personal especializado para la gestión de la ciberseguridad: en el 53,0% de los casos se trata de un proveedor externo y en el 20,0% de personal interno. El resto de las empresas se reparte entre un 17,0% en las que la gestión está en manos de personal no especializado, y un 9,5% donde nadie se encarga de la ciberseguridad.

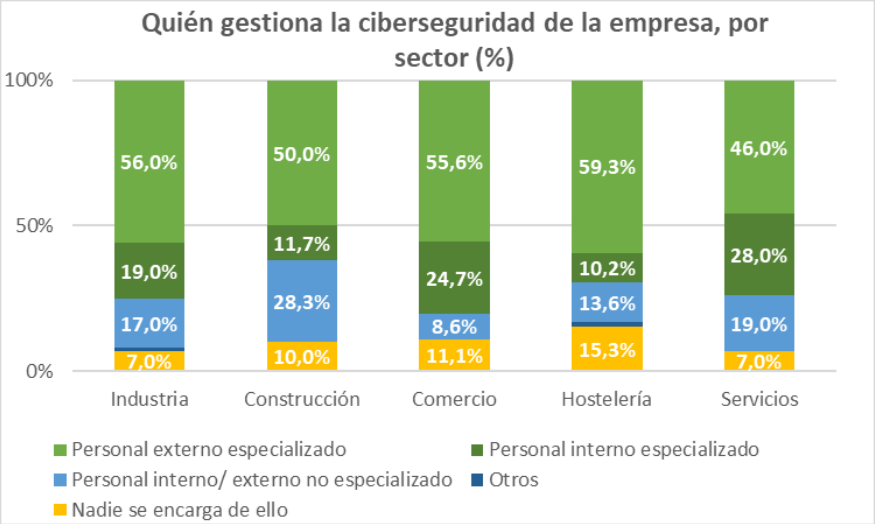
La especialización en la gestión de la ciberseguridad cobra mayor peso según aumenta el tamaño de las empresas. Así, entre las compañías de 1 a 9 trabajadores se observa una mayor ausencia de gestión (14,5%) y falta de especialización (23,0%), en tanto que entre las de 250 o más trabajadores prevalecen aquellas con gestión especializada de la ciberseguridad, en particular la internalizada (47,6%).



Fuente: Cámara de Comercio de España.

Por sector de actividad, **destaca la hostelería**, donde el peso de la ausencia de gestión de la ciberseguridad es mayor que en los demás sectores: en **un 15,3% de sus empresas nadie se encarga de ello**.

El sector de la construcción presenta una elevada proporción de empresas con una gestión no especializada (28,3%). En el extremo opuesto, la mayoría de las compañías de servicios (74,0%) han optado por una gestión especializada de la ciberseguridad.

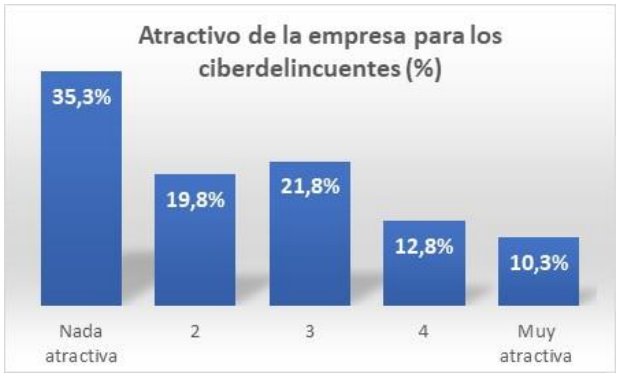


Fuente: Cámara de Comercio de España.

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

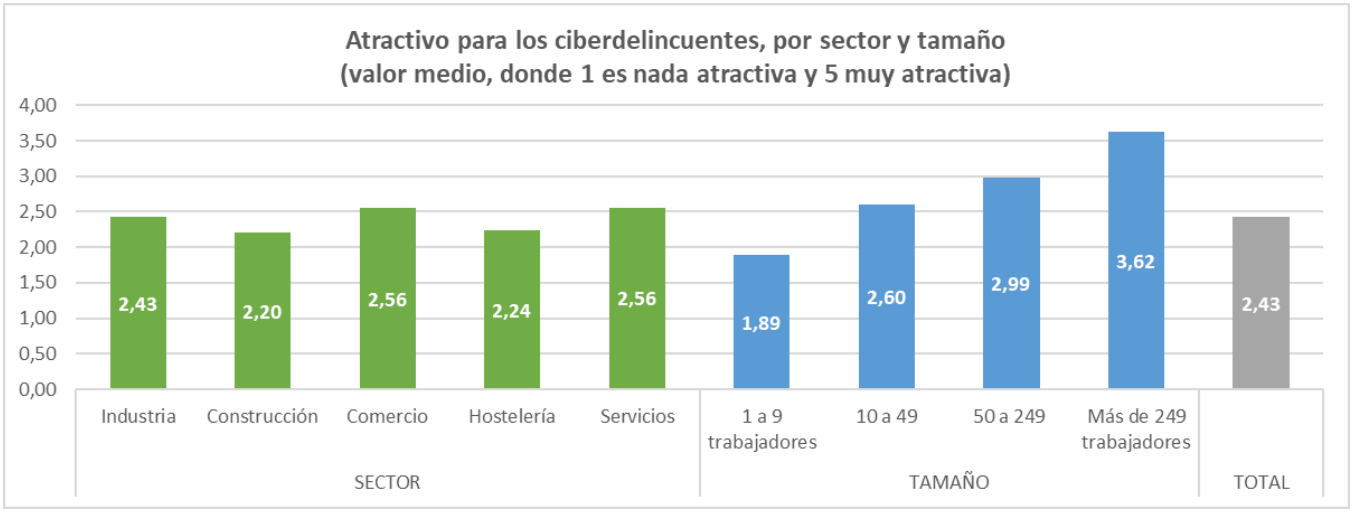
Más de la mitad de las empresas (55,1%) se considera poco o nada atractiva para los ciberdelincuentes, un 23,1% cree que está en riesgo, y un 21,8% se sitúa en una situación intermedia. Como resultado, **en promedio, las empresas españolas consideran que el riesgo de sufrir un ciberataque es bajo (2,43 puntos).**

Sin embargo, esta percepción del riesgo aumenta con el tamaño de la empresa. Así, si bien las microempresas se consideran, en promedio, poco atractivas para los ciberdelincuentes (1,89), las empresas más grandes perciben un riesgo elevado (3,62).

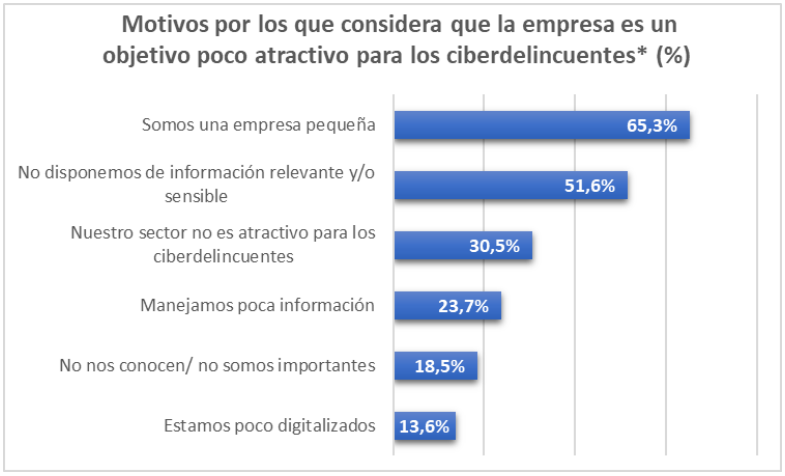


Fuente: Cámara de Comercio de España.

Por sectores, no se advierten disparidades reseñables.



Fuente: Cámara de Comercio de España.



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

Fuente: Cámara de Comercio de España.

Un tamaño reducido (65,3%) o no manejar información sensible o relevante (51,6%), son las razones más señaladas por las compañías que consideran que no están en el foco de atención de los ciberdelincuentes.

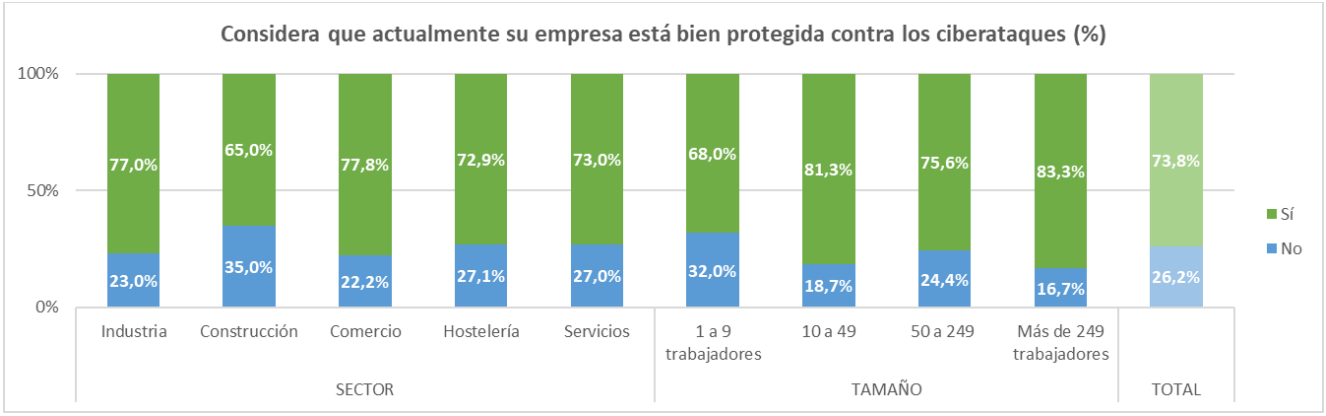
Una proporción menor considera que su sector no es atractivo para los ciberdelincuentes (30,5%), que maneja poca información (23,7%) o simplemente que son desconocidas o poco importantes (18,5%).

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

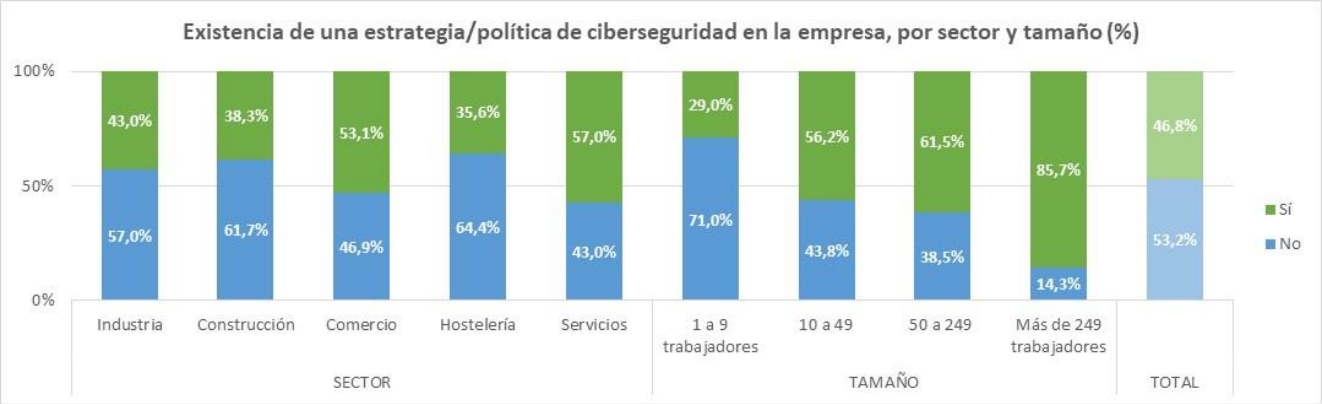
El 73,8% de las empresas considera que está bien protegida contra los ciberataques en la actualidad, aunque esta proporción es algo menor entre las microempresas (68,0%) y las compañías que pertenecen al sector de la construcción (65,0%).



Fuente: Cámara de Comercio de España.

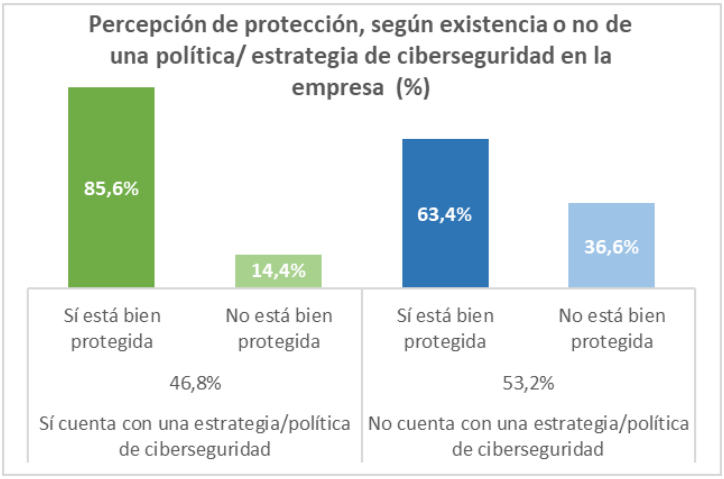
En cuanto a la planificación, algo menos de la mitad (46,8%) afirman tener definida formalmente una política/ estrategia específica de ciberseguridad. Atendiendo a la distribución por tamaño, **se evidencia una relación directa entre la existencia de una política/ estrategia de seguridad y el tamaño de la empresa:** la planificación está más presente cuanto más grande es la empresa. En este sentido, es menor en microempresas (29,0%), entre las pequeñas (56,3%) y medianas (61,5%), y notablemente mayor en las más grandes (85,7%).

Por sector, en las empresas de hostelería la planificación está menos presente (35,6%), y es más relevante entre las de servicios (57,0%).



Fuente: Cámara de Comercio de España.

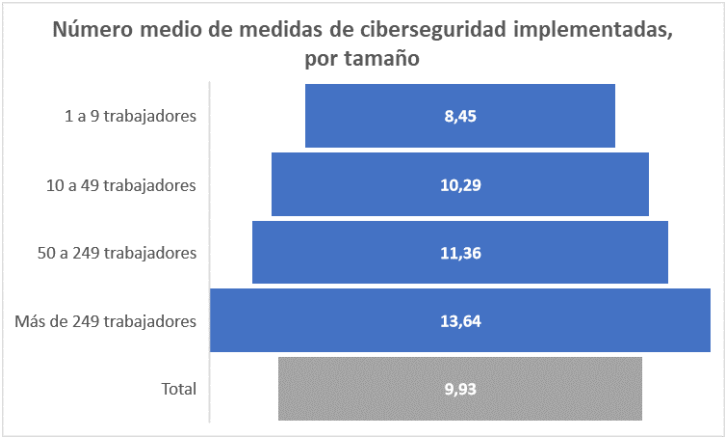
Si se analiza la percepción de seguridad ante los ciberataques en función de la existencia o no de una estrategia/ política definida de ciberseguridad, se observa que **aquellas compañías que cuentan con una planificación de estas características se sienten más seguras.** Así, en este grupo, el 85,6% de las empresas consideran que están bien protegidas, en tanto que este porcentaje cae al 63,4% entre las que no tienen una estrategia o política al respecto.



Fuente: Cámara de Comercio de España.

En lo que respecta a las medidas de ciberseguridad adoptadas, la empresa promedio desarrolla en la actualidad 10 actuaciones encaminadas a prevenir los ciberataques.

Desagregando por número de trabajadores, puede afirmarse que cuanto mayor es su tamaño, más medidas de ciberseguridad tiene implantadas.



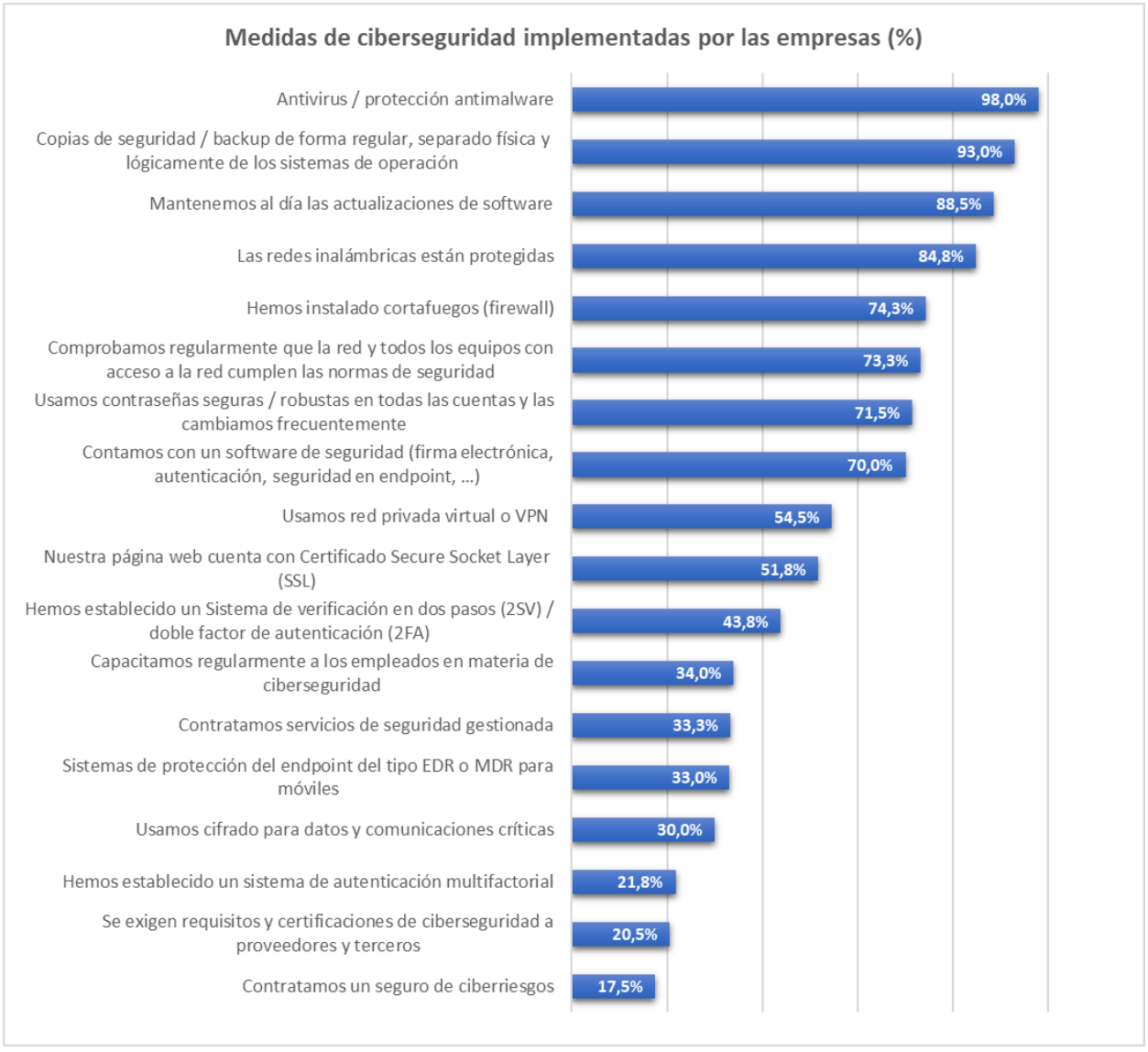
Fuente: Cámara de Comercio de España.

▶ Medidas de ciberseguridad implementadas

Sobre la tipología de las medidas implementadas, **la gran mayoría de las compañías ya dispone de antivirus / protección *antimalware* (98,0%), copias de seguridad / *backup* de forma regular, separado física y lógicamente de los sistemas de operación (93,0%), actualizaciones de *software* al día (88,5%), y redes inalámbricas protegidas (84,8%).**

También, algo menos de las tres cuartas partes dispone de cortafuegos (74,3%), verifican regularmente que sus redes y equipos con acceso cumplan con las normas de seguridad (73,3%), usan contraseñas seguras y las cambian con frecuencia (71,5%) y cuentan con un software de seguridad (70,0%). En menor medida, las empresas utilizan red privada virtual (54,5%), su página web cuenta con Certificado *Secure Socket Layer* (51,8%) o han establecido un sistema de verificación en dos pasos/doble factor de autentificación (43,8%).

Finalmente, hay que destacar que tan solo el 34,0% de las compañías desarrolla regularmente actividades de capacitación para los empleados.



Fuente: Cámara de Comercio de España.

Para prácticamente todas las medidas de seguridad analizadas, el uso aumenta conforme se incrementa el tamaño de la empresa.

Esta disparidad es más evidente, como era de esperar, entre aquellas actuaciones menos frecuente en el conjunto de empresas consultadas. Así, el cifrado para datos y comunicaciones críticas es utilizado por un 71,4% de las compañías con más de 249 trabajadores, en tanto que esta medida es aplicada por solo un 13,5% de las microempresas. La implementación de sistemas de protección del *endpoint* del tipo EDR o MDR para móviles es otro ejemplo de ello: este sistema es utilizado por un 71,4% de las empresas más grandes, mientras que entre las de menos de 10 trabajadores este porcentaje desciende al 23,0%.

Medidas de ciberseguridad implementadas en la actualidad, por tamaño (%)

	1 a 9 trabajadores	10 a 49	50 a 249	más de 249 trabajadores
Antivirus / protección antimalware	97,0%	100,0%	100,0%	95,2%
Copias de seguridad / backup de forma regular, separado física y lógicamente de los sistemas de operación	89,0%	98,8%	93,6%	100,0%
Mantenemos al día las actualizaciones de software	83,0%	95,0%	91,0%	97,6%
Las redes inalámbricas están protegidas	79,5%	90,0%	87,2%	95,2%
Hemos instalado cortafuegos (firewall)	63,5%	75,0%	88,5%	97,6%
Comprobamos regularmente que la red y todos los equipos con acceso a la red de la empresa cumplen las normas de segurida	67,0%	75,0%	79,5%	88,1%
Usamos contraseñas seguras / robustas en todas las cuentas y las cambiamos frecuentemente	66,0%	77,5%	73,1%	83,3%
Contamos con un software de seguridad (firma electrónica, autenticación, seguridad en endpoint, ...)	61,0%	76,3%	78,2%	85,7%
Usamos red privada virtual o VPN	38,0%	51,3%	80,8%	90,5%
Nuestra página web cuenta con Certificado Secure Socket Layer (SSL)	44,0%	47,5%	65,4%	71,4%
Hemos establecido un Sistema de verificación en dos pasos (2SV) / doble factor de autenticación (2FA)	35,5%	46,3%	50,0%	66,7%
Capacitamos regularmente a los empleados en materia de ciberseguridad	23,5%	43,8%	39,7%	54,8%
Contratamos servicios de seguridad gestionada	21,0%	32,5%	47,4%	66,7%
Sistemas de protección del endpoint del tipo EDR o MDR para móviles	23,0%	26,3%	44,9%	71,4%
Usamos cifrado para datos y comunicaciones críticas	13,5%	32,5%	47,4%	71,4%
Hemos establecido un sistema de autenticación multifactorial	16,0%	18,8%	25,6%	47,6%
Se exigen requisitos y certificaciones de ciberseguridad a proveedores y terceros	13,0%	20,0%	28,2%	42,9%
Contratamos un seguro de ciberriesgos	12,0%	22,5%	15,4%	38,1%

Fuente: Cámara de Comercio de España.

Barreras a la mejora de la ciberseguridad

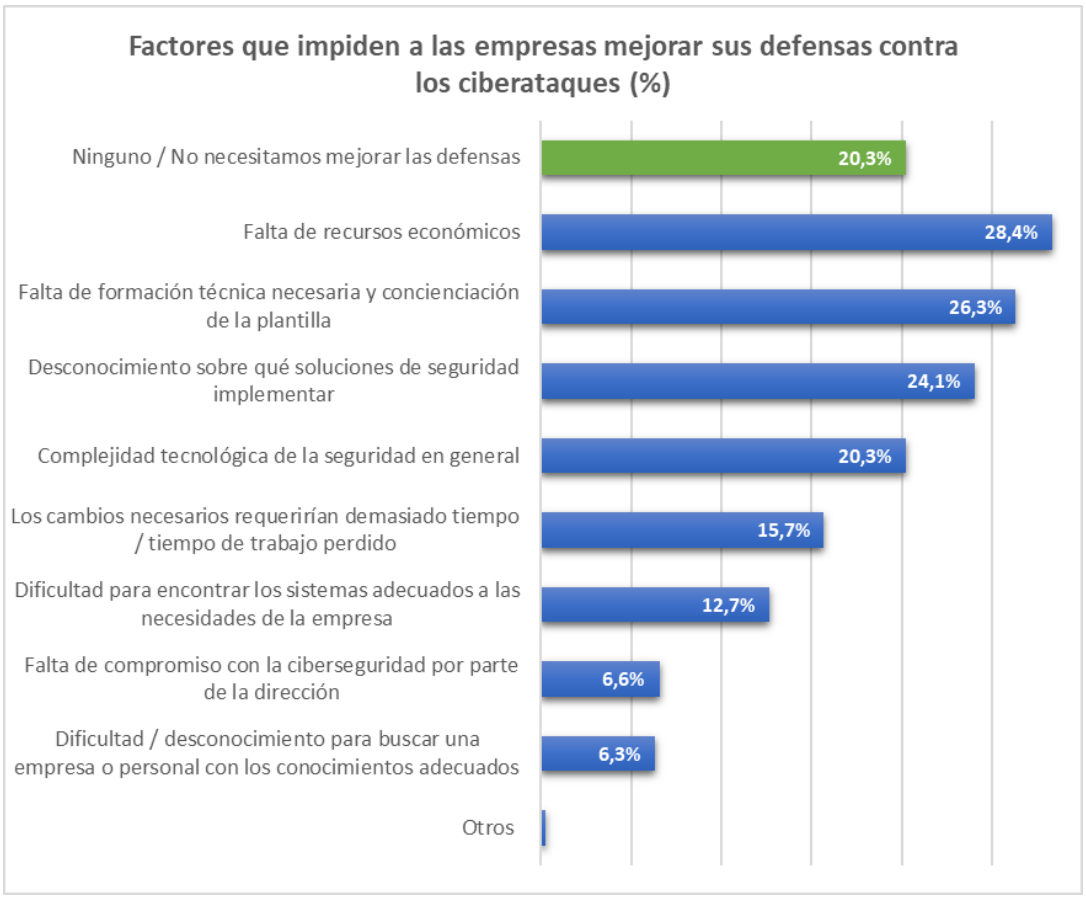
En este apartado se indaga sobre la existencia de posibles barreras que obstaculizan o impiden la mejora de la ciberseguridad en las empresas.

▶ Elementos que impiden a las empresas mejorar sus defensas ante las ciberamenazas

Consultadas por los **factores clave que les impiden mejorar las defensas ante las ciberamenazas, la escasez de recursos económicos es el más señalado (28,4%)**. **Le siguen muy de cerca elementos relacionados principalmente con la falta de conocimiento en la materia:** falta de formación técnica y concienciación de la plantilla (26,3%), desconocimiento sobre las soluciones a implementar (24,1%) y, aunque en menor grado, la complejidad tecnológica de la seguridad en general (20,3%).

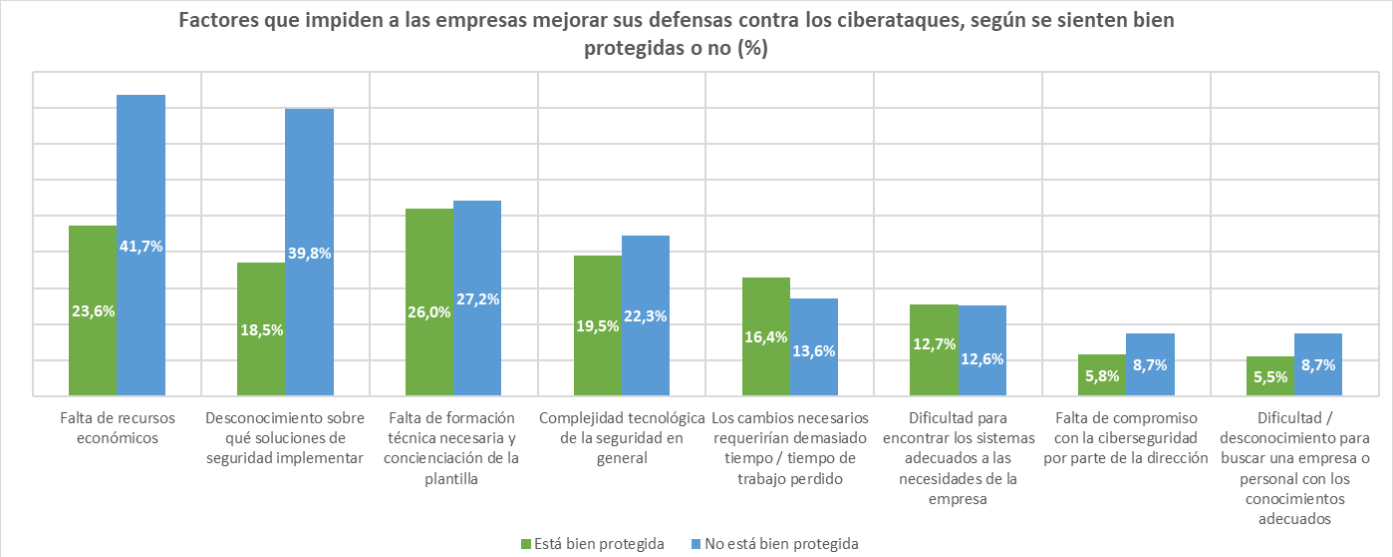
Un 15,7% de las compañías destaca el tiempo de trabajo que implicarían los cambios y el 12,7% menciona la dificultad para encontrar los sistemas adecuados para las necesidades de su empresa.

Cabe destacar, asimismo, que **una quinta parte de empresas manifiesta que no necesita mejorar sus defensas contra los ciberataques (20,3%).**



Fuente: Cámara de Comercio de España.

Desagregando por la capacidad de protección ante los ciberataques manifestada por las empresas, **se advierten dos impedimentos claros para mejorar la seguridad entre aquellas empresas que declaran no estar bien protegidas: la falta de recursos económicos (41,7%) y el desconocimiento sobre qué soluciones de seguridad deben implementar (39,8%).**



Fuente: Cámara de Comercio de España.

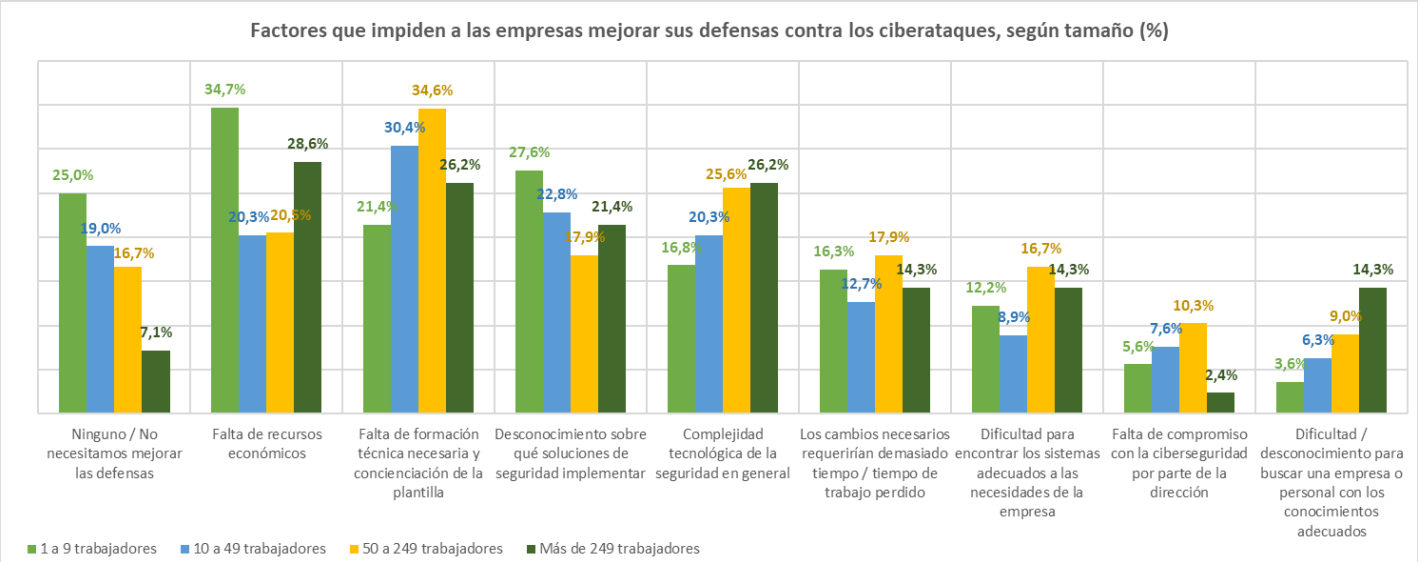
En relación con las características de las empresas, la importancia de los diferentes factores que impiden a las empresas defenderse mejor contra los ciberataques varía en función del número de trabajadores.

La **falta de recursos económicos** es el elemento limitante más señalado por las microempresas (34,7%) y por las compañías de más de 249 trabajadores (28,6%). Por su parte, en el tramo de entre 10 y 249 empleados adquiere un peso mayor la **falta de formación técnica necesaria y concienciación de la plantilla:** del 34,6% en las de 50 a 249 y del 30,4% en las de 10 a 49 trabajadores.

La **complejidad tecnológica de la seguridad en general** y la **dificultad / desconocimiento para buscar una empresa o personal con los conocimientos adecuados**, son elementos que se perciben como más limitantes para mejorar la protección según crece el tamaño de la empresa.

Ocurre lo contrario entre las empresas que consideran que ya se encuentran bien protegidas, es decir, que no que necesitan mejorar sus defensas: la proporción desciende cuando más grande es la compañía. Así, mientras que una cuarta parte de las microempresas estima que no tienen margen de mejora, esta opción es elegida por tan solo un 7,1% de las compañías de mayor tamaño.

Por sector, las diferencias más reseñables se observan en la relevancia atribuida al factor económico. Concretamente, las empresas hosteleras acusan más que el resto de los sectores la escasez de recursos económicos como un limitante para mejorar sus defensas contra los ciberataques (37,9%). En el extremo opuesto se sitúan las compañías de servicios, entre las que solo un 21,3% apuntan en esta dirección.



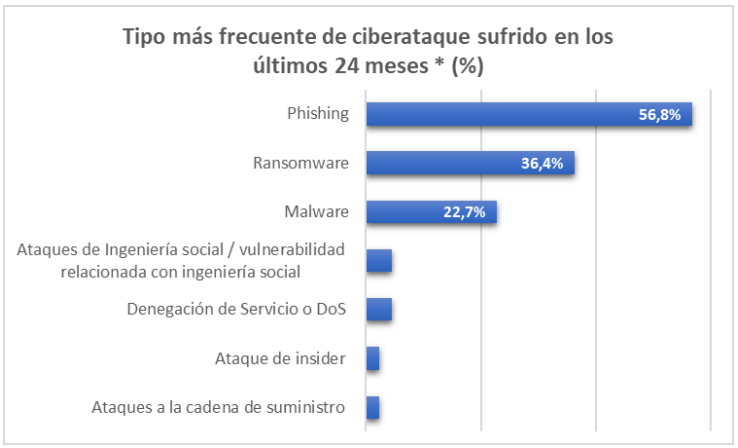
Fuente: Cámara de Comercio de España.

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 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 (11,0%) 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) (56,8%), el *ransomware* ("secuestro" de archivos y equipos, los hace inaccesibles a menos que se pague un rescate) (36,4%) y el *malware* (infecta el ordenador y lo deja inservible) (22,7%).



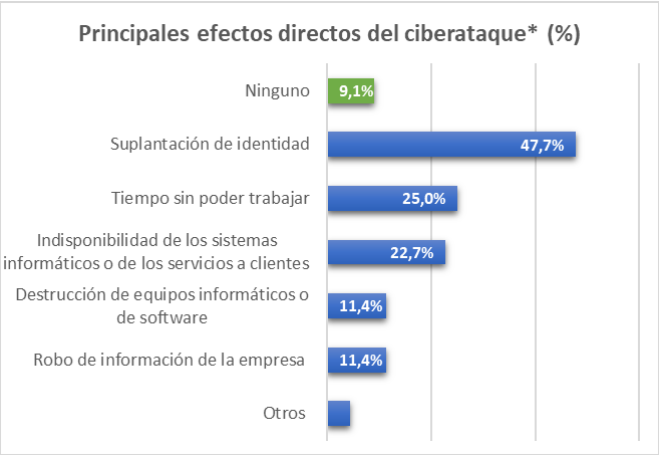
* Empresas que han sufrido un ciberataque en los últimos 24 meses.

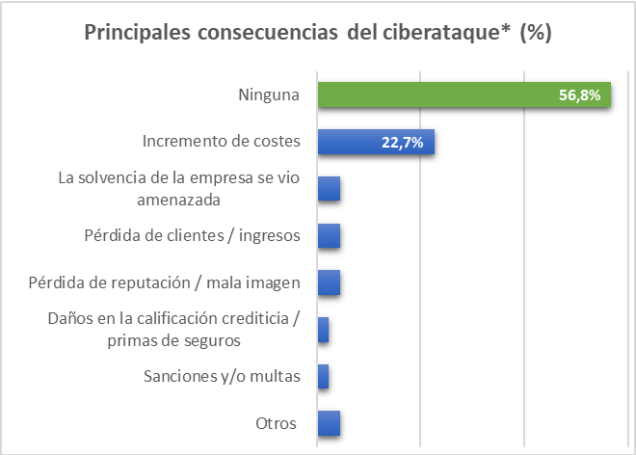
Fuente: Cámara de Comercio de España.

▶ Efectos directos y consecuencias

De las empresas que han sufrido un ciberataque, en el 90,9% de los casos este ataque tuvo algún efecto directo inmediato y en el 43,2% alguna consecuencia posterior. Entre los efectos más frecuentes se encuentra la suplantación de identidad (47,7%), seguido a distancia por el tiempo de trabajo perdido (25,0%) y la indisponibilidad de los sistemas informáticos o los servicios a los clientes (22,7%).

En lo que respecta a las consecuencias, destaca la **elevada proporción de empresas en las que los ciberataques no tuvieron repercusiones reseñables (56,8%)**. Por su parte, el incremento de los costes es la consecuencia más señalada por las compañías que sí resultaron afectadas (22,7%).





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

Fuente: Cámara de Comercio de España.

▶ Posibilidad de sufrir un nuevo ciberataque

Consultadas por la probabilidad de sufrir un nuevo ciberataque durante los próximos 12 meses, un 40,9% de estas empresas perciben un riesgo bajo o nulo, un 31,8% lo considera probable o muy probable, y un 27,3% se sitúa en una posición intermedia.

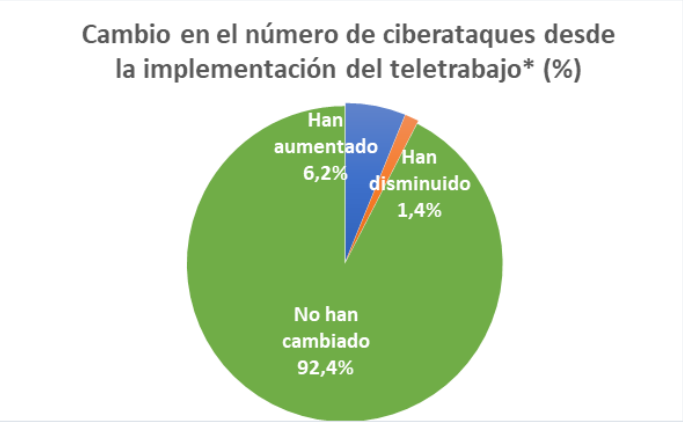
* Empresas que han sufrido un ciberataque en los últimos 24 meses.

Fuente: Cámara de Comercio de España.

▶ Teletrabajo y vulnerabilidad ante los ciberataques

En el 52,8% de las empresas consultadas existe la posibilidad de teletrabajar. Dentro de este grupo, la gran mayoría declara que su implementación no ha supuesto un incremento en su vulnerabilidad ante los ciberataques. Así, **un 92,4% manifiesta que el número de ciberataques no se ha modificado con el establecimiento de esta modalidad** y solo un 6,2% declara que se ha incrementado.

Fuente: Cámara de Comercio de España.

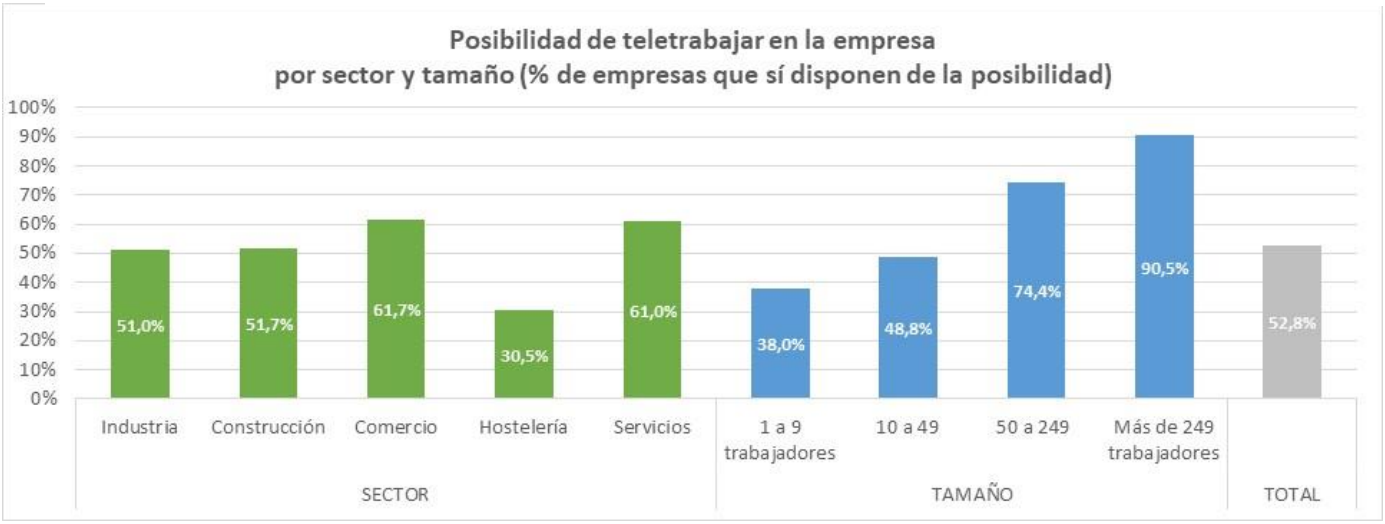


* Empresas que han implantado el teletrabajo.

Fuente: Cámara de Comercio de España.

Existe una relación claramente positiva y creciente entre la posibilidad de teletrabajar y el tamaño de las empresas. En este sentido, la presencia del trabajo remoto asciende desde el 38,9% de las microempresas hasta el 90,5% entre las compañías de más de 249 trabajadores.

Según sectores, las empresas comerciales (61,7%) y de servicios (61,0%) son las que más ofrecen esta posibilidad, en contraposición a las de hostelería donde el teletrabajo está presente en solo el 30,5%.



Fuente: Cámara de Comercio de España.

El futuro: inversión prevista en ciberseguridad

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

▶ Previsión de incremento de la inversión en seguridad

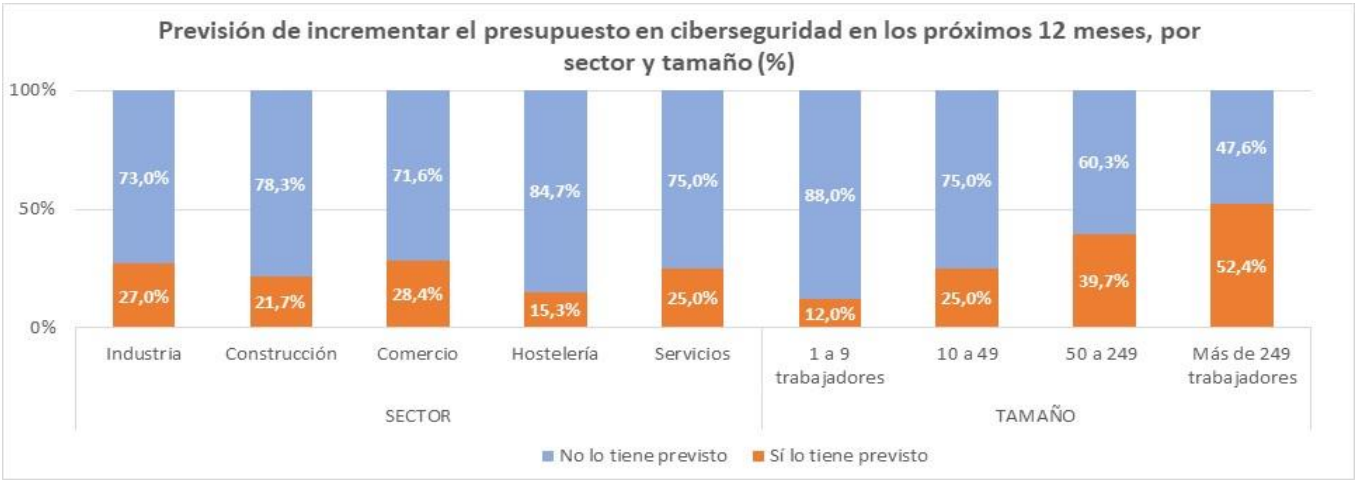
Fuente: Cámara de Comercio de España.

Tal y como se señaló anteriormente, el 73,8% de las empresas considera que se encuentra bien protegida contra los ciberataques en la actualidad. A ello se añade que algo más de la mitad (55,3%) se percibe poco o nada atractiva para los ciberdelincuentes y que tan solo un 11,0% de ellas ha sufrido algún ciberataque en los últimos 24 meses.

Esta percepción de ausencia o escaso peligro se refleja en las inversiones que las compañías esperan asignar a ciberseguridad en los próximos 12 meses: **el 75,7% no tiene previsto incrementar su presupuesto en la materia.**

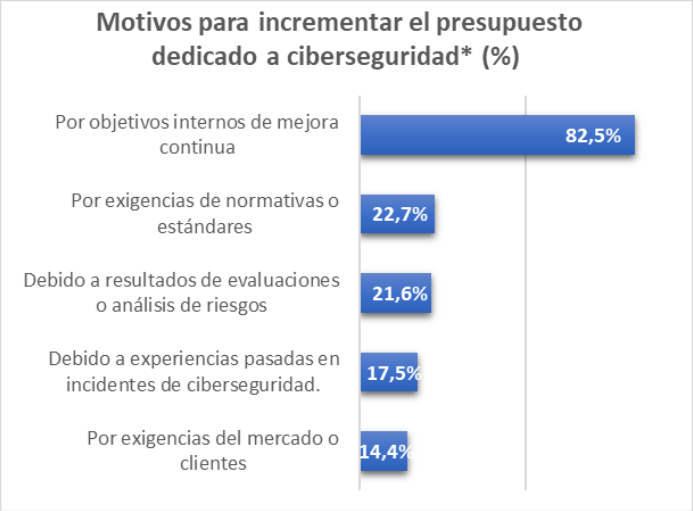
Los resultados varían al desagregar por tamaño, cuando se advierte claramente que **la disposición a incrementar la inversión en ciberseguridad en los próximos 12 meses se eleva conforme lo hace el número de trabajadores.** Así, entre las microempresas, tan solo un 12,0% tiene previsto aumentar el presupuesto, en tanto que esta cifra asciende al 52,4% entre las empresas más grandes.

El análisis por sectores revela que no se observan disparidades reseñables entre ellos. La hostelería, en particular, presenta una disposición menor que el resto a invertir en ciberseguridad en el futuro (15,3%).



Fuente: Cámara de Comercio de España.

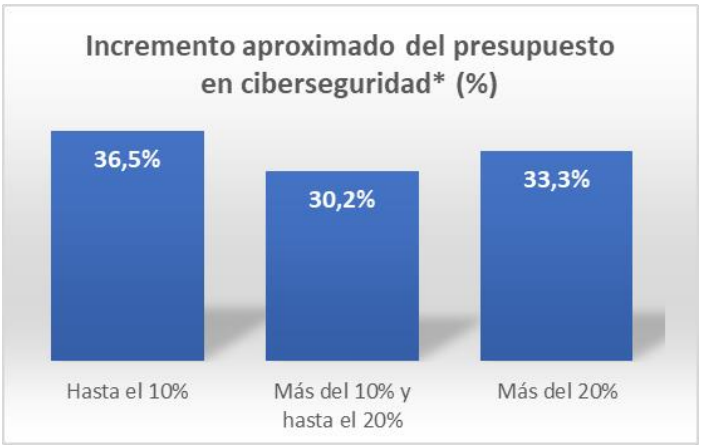
Entre las empresas que sí aumentarán el presupuesto en ciberseguridad durante el próximo año, la gran mayoría señala a los objetivos internos de mejora continua como motivo principal para ello (82,5%).



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

Fuente: Cámara de Comercio de España.

En cuando al aumento previsto, la subida presupuestaria promedio será del 23,5%. Con mayor detalle, un 36,5% plantea un crecimiento del 10% o menos con respecto al presupuesto del año en curso, y solo una tercera parte tiene previsto un incremento mayor del 20%.



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

Fuente: Cámara de Comercio 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 el último trimestre de 2023.

La muestra se compone de 400 empresas de al menos un asalariado en todo el territorio nacional geográfico (representación de la mayor parte de CCAA) y de todos los sectores de actividad, distribuidas de acuerdo con 2 criterios de desagregación: sector (Industria, Construcción, Comercio, Hostelería y Servicios) y tamaño (1 a 9 trabajadores, 10 a 49 trabajadores, 50 a 249 trabajadores, 250 y más trabajadores).

El margen de error máximo para un nivel de confianza del 95% es de ±2,05%. Los resultados por tamaño y sector son orientativos, dado que la muestra no proporciona resultados estadísticamente significativos en estos casos.

Fecha de cierre del documento: mayo de 2024.

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