BARÓMETRO ciberseguridadTIC

Estado de Ciberseguridad en España 2025

Introducción

La ciberseguridad en España afronta uno de los momentos más complejos de su historia reciente. La superficie de exposición crece sin pausa, impulsada por la aceleración tecnológica, la digitalización de procesos, la dependencia de terceros y la proliferación de nuevos modelos de trabajo y consumo. Mientras tanto, los atacantes —cada vez más organizados, mejor financiados y apoyados en herramientas de automatización e inteligencia artificial— elevan el nivel de sofisticación a un ritmo que muchas empresas no pueden igualar.

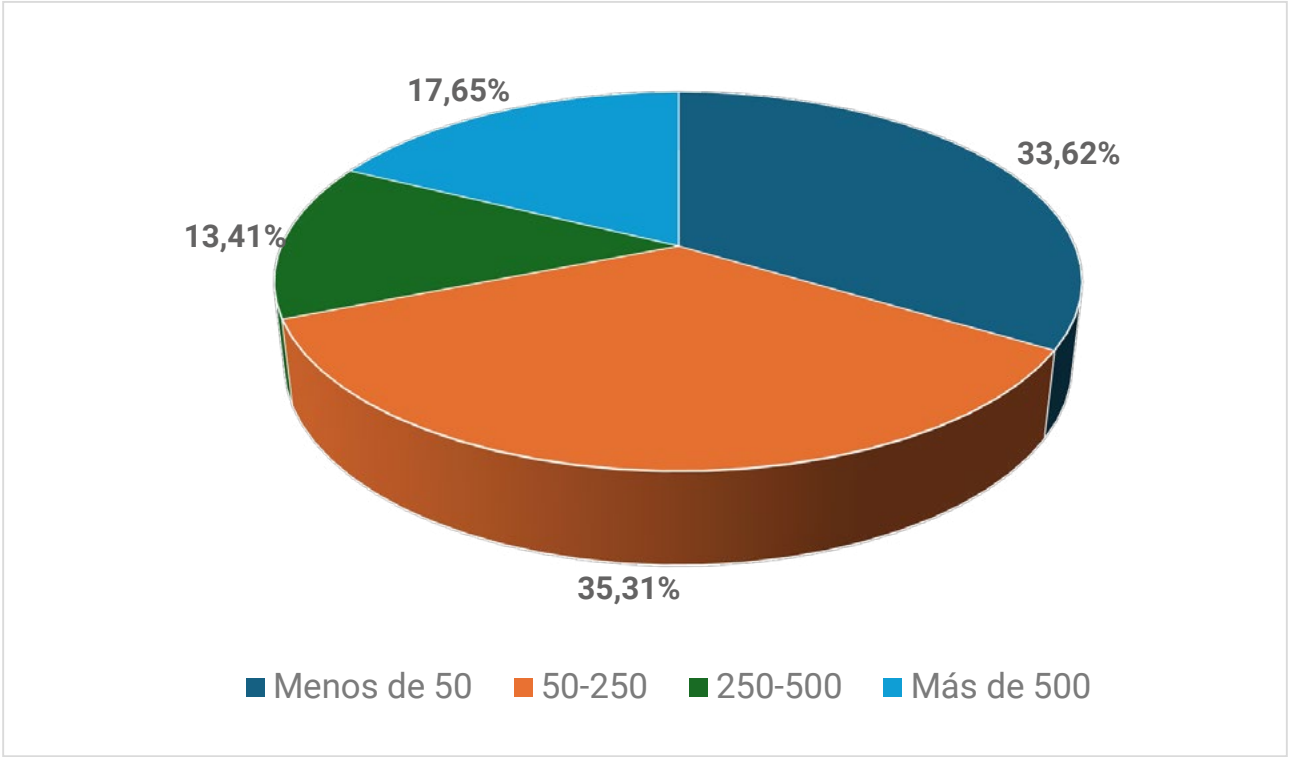
A este escenario se suma un problema estructural: la brecha de talento, que se agrava año tras año y limita la capacidad de los equipos para operar, vigilar y responder con eficacia. La consecuencia es un ecosistema empresarial sometido a una presión creciente, obligado a tomar decisiones tácticas en un entorno regulatorio cada vez más exigente (NIS2, DORA, CRA, ENS, GDPR...) y en medio de un mercado que no deja de generar nuevas siglas, tecnologías y promesas de protección.

En este contexto, el estudio “Estado de la Ciberseguridad en España 2025”, elaborado junto con Secure&IT, nace con un propósito claro: comprender cómo están reaccionando las empresas españolas ante esta realidad compleja. Queremos saber qué amenazas les inquietan, qué tecnologías están desplegando, cómo organizan el gobierno de la seguridad, qué percepción tienen del impacto regulatorio y, en definitiva, hasta qué punto se sienten preparadas para un escenario donde la incertidumbre —tecnológica, geopolítica y operativa— forma ya parte del día a día.

> Las empresas españolas avanzan en ciberseguridad, pero lo hacen a distintas velocidades

Este informe analiza los resultados pregunta a pregunta, identifica tendencias, destaca brechas y pone contexto a los datos para construir una visión precisa del estado actual de la ciberseguridad en nuestro país. El objetivo no es sólo medir, sino también ayudar a interpretar hacia dónde se dirige el mercado y qué prioridades marcarán la agenda de los próximos años.

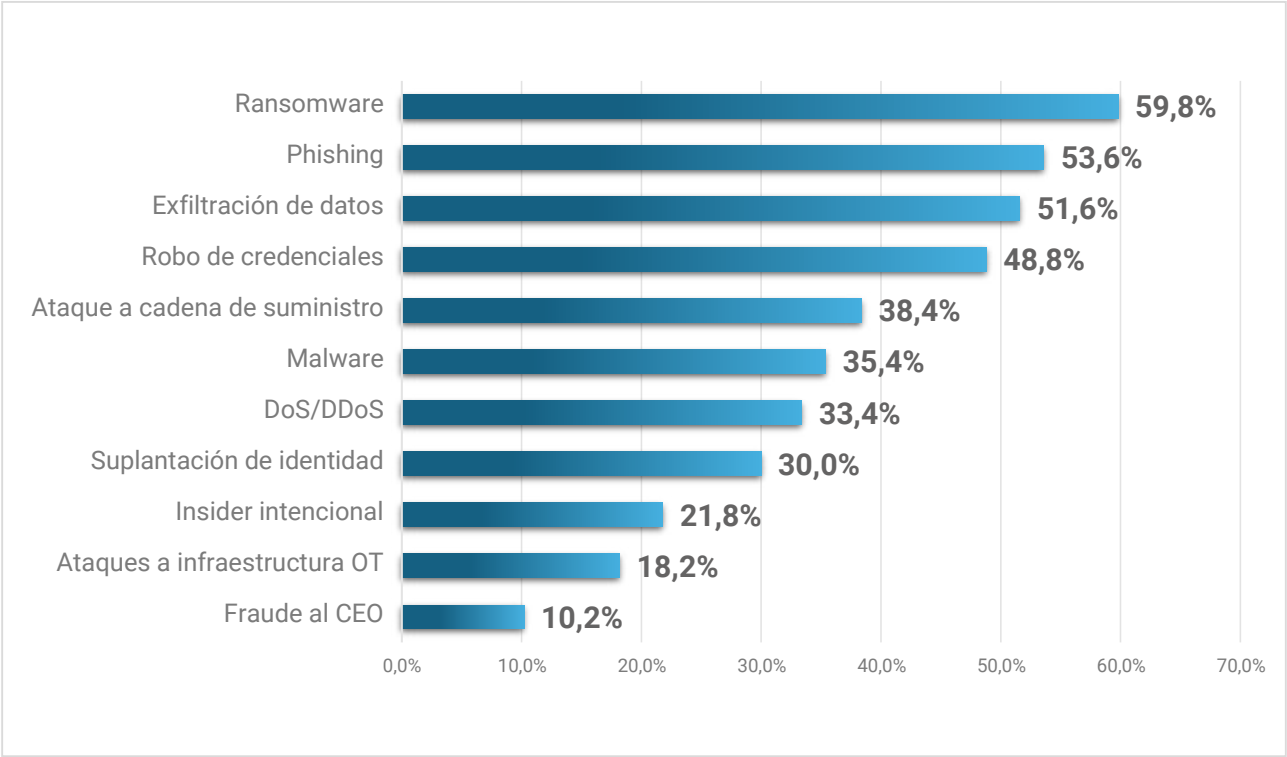
Perfil de la muestra: sectores y tamaño de empresa



La composición de la muestra ofrece una visión clara del tejido empresarial español y ayuda a contextualizar el resto del estudio. En cuanto a sectores, el grupo más numeroso es "Otros", que reúne el 39,4 % de las respuestas y refleja la diversidad de organizaciones participantes. Tras él aparecen sectores tradicionalmente críticos como la sanidad (20 %), las finanzas (16,8 %) y el transporte (10,4 %). Aunque con menor peso, energía (8 %) y agua (5,4 %) completan un bloque que aporta una perspectiva relevante sobre la interoperabilidad IT/OT, especialmente al cruzarlo con la baja preocupación declarada por los riesgos industriales.

Por tamaño, la muestra está claramente dominada por la pyme: un 33,6 % de las organizaciones tiene menos de 50 empleados y un 35,3 % se sitúa entre 50 y 250. En conjunto, casi siete de cada diez empresas son pequeñas o medianas, un dato clave para entender las limitaciones de inversión, recursos y especialización que se observan a lo largo del estudio. Las compañías de 250 a 500 empleados representan el 13,4 %, y las de más de 500 alcanzan el 17,7 %, aportando la visión de organizaciones más reguladas y con estructuras de ciberseguridad más consolidadas.

¿Qué tipo de ataque te preocupa más?

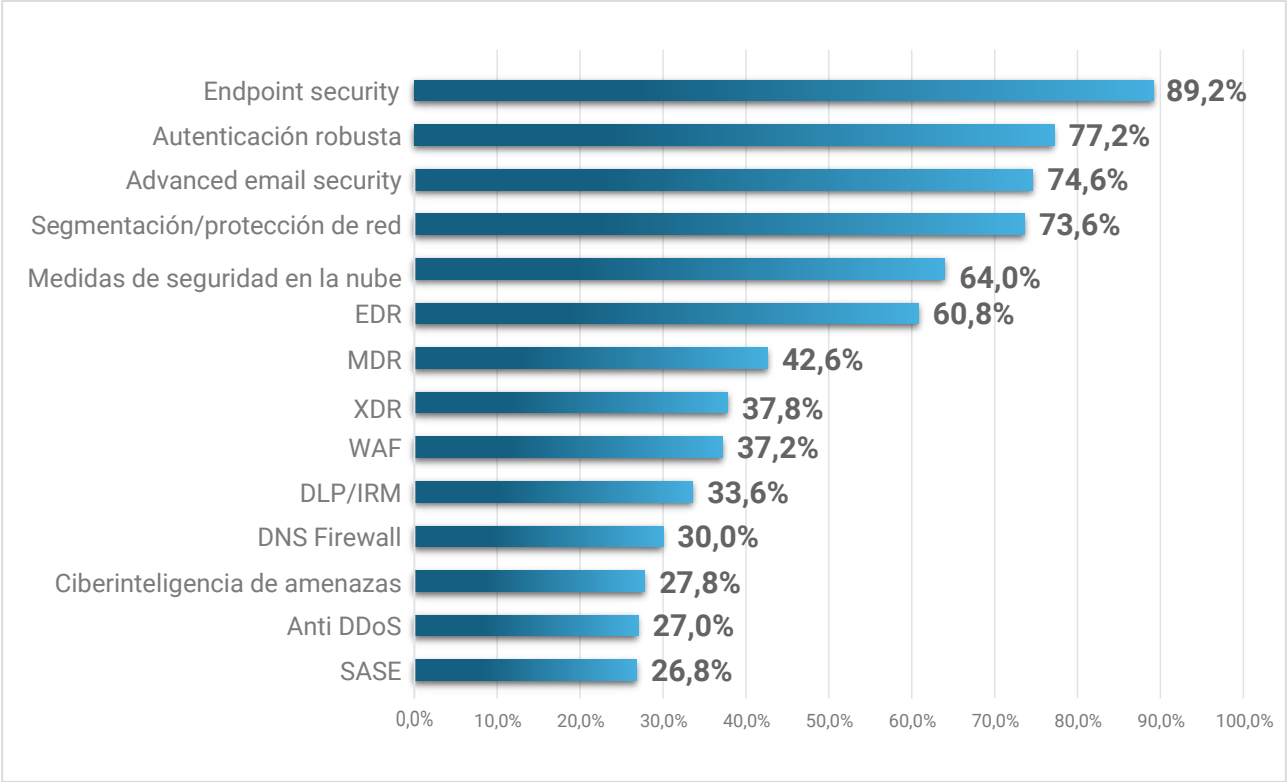


El ransomware continúa siendo la principal preocupación de las empresas españolas: un 59,8 % lo sitúa como la amenaza que más inquieta, muy por encima del resto. A corta distancia aparecen el phishing (53,6 %), la exfiltración de datos (51,6 %) y el robo de credenciales (48,8 %), lo que confirma que la seguridad del usuario y de la identidad siguen siendo los puntos más frágiles en la mayoría de organizaciones. También destaca el avance de los ataques a la cadena de suministro (38,4 %), un reflejo directo de los incidentes recientes que han afectado a proveedores y servicios críticos.

El dato más llamativo llega con los ataques a infraestructura OT, mencionados sólo por el 18,2 %. La cifra sorprende si se tiene en cuenta que cerca de la mitad de la muestra pertenece a sectores donde la tecnología industrial es esencial —sanidad, energía, transporte o agua—. Todo apunta a que el riesgo OT sigue infravalorado o, simplemente, se percibe como un problema ajeno al área de ciberseguridad.

En conjunto, los resultados muestran un enfoque todavía muy centrado en las amenazas clásicas de TI y una menor sensibilidad hacia los riesgos operativos que pueden comprometer el propio funcionamiento del negocio.

¿Qué tecnologías tienes implantadas?

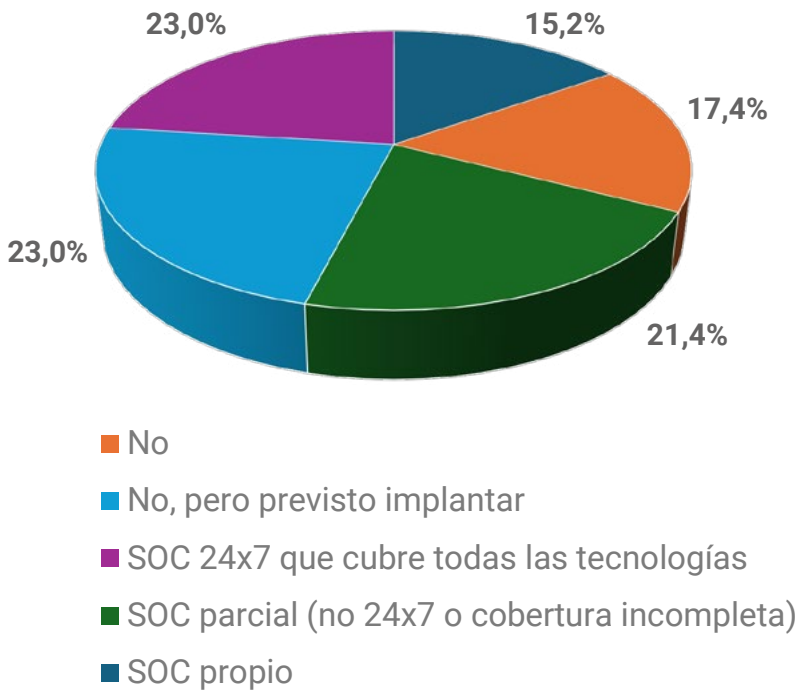


La fotografía tecnológica muestra un escenario muy heterogéneo, donde conviven soluciones básicas, herramientas maduras y tecnologías que aún están en adopción temprana. La gran mayoría de las empresas cuenta con endpoint security (89,2 %), autenticación robusta (77,2 %) y seguridad avanzada del email (74,6 %), un trío que refleja tanto la presión del phishing como la necesidad de reforzar la identidad digital. También es elevado el uso de segmentación o protección de red (73,6 %), lo que indica que el control del tráfico y la compartimentación siguen siendo pilares fundamentales.

Las herramientas más avanzadas muestran una implantación desigual. El EDR alcanza un 60,8 %, cifra relevante pero aún baja si se tiene en cuenta el nivel actual de amenazas. Sólo el 42,6 % utiliza servicios MDR, y apenas un 26,8 % adopta SASE, una tecnología que debería ganar peso en entornos híbridos y distribuidos. La seguridad en la nube (64 %) evidencia que muchas organizaciones ya han dado el salto, pero probablemente sin una estrategia completa de plataforma.

Los datos ponen de manifiesto un ecosistema donde las bases están razonablemente cubiertas, pero la modernización avanza a distintas velocidades, especialmente en áreas clave como la detección avanzada, la gestión de identidades y los modelos de seguridad orientados al cloud y al Zero Trust.

¿Cuentas con un Centro de Operaciones de Seguridad que gestione las tecnologías anteriores?

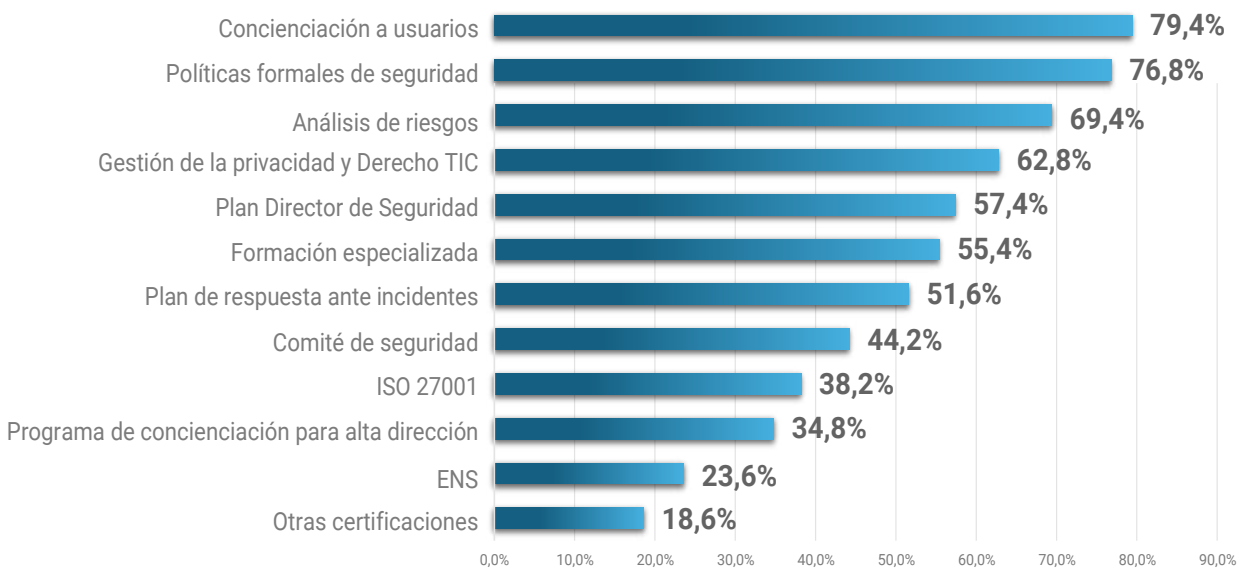


La fotografía del SOC en las empresas españolas revela un escenario fragmentado y, en muchos casos, insuficiente para el nivel actual de amenaza. Un 17,4 % reconoce directamente que no dispone de ningún servicio de monitorización, una cifra elevada si se tiene en cuenta la frecuencia y rapidez de los ataques actuales. El modelo predominante es el SOC 24x7 con cobertura completa, pero sólo alcanza al 23 % de los encuestados, mientras que otro 21,4 % opera un SOC parcial.

Resulta llamativo que el SOC propio solo esté presente en el 15,2 % de las organizaciones, lo que confirma que mantener capacidades internas de monitorización, detección y respuesta sigue siendo costoso y complejo, especialmente para empresas medianas. La mezcla de modelos —servicios externalizados, coberturas horarias limitadas y ausencia total en algunos casos— muestra que todavía existe una brecha importante entre las necesidades de seguridad y la capacidad real de muchos equipos.

De forma que la madurez del SOC sigue avanzando, pero a un ritmo desigual. La externalización crece, el 24x7 gana peso, pero aún hay demasiadas organizaciones sin vigilancia suficiente para responder con rapidez a un incidente.

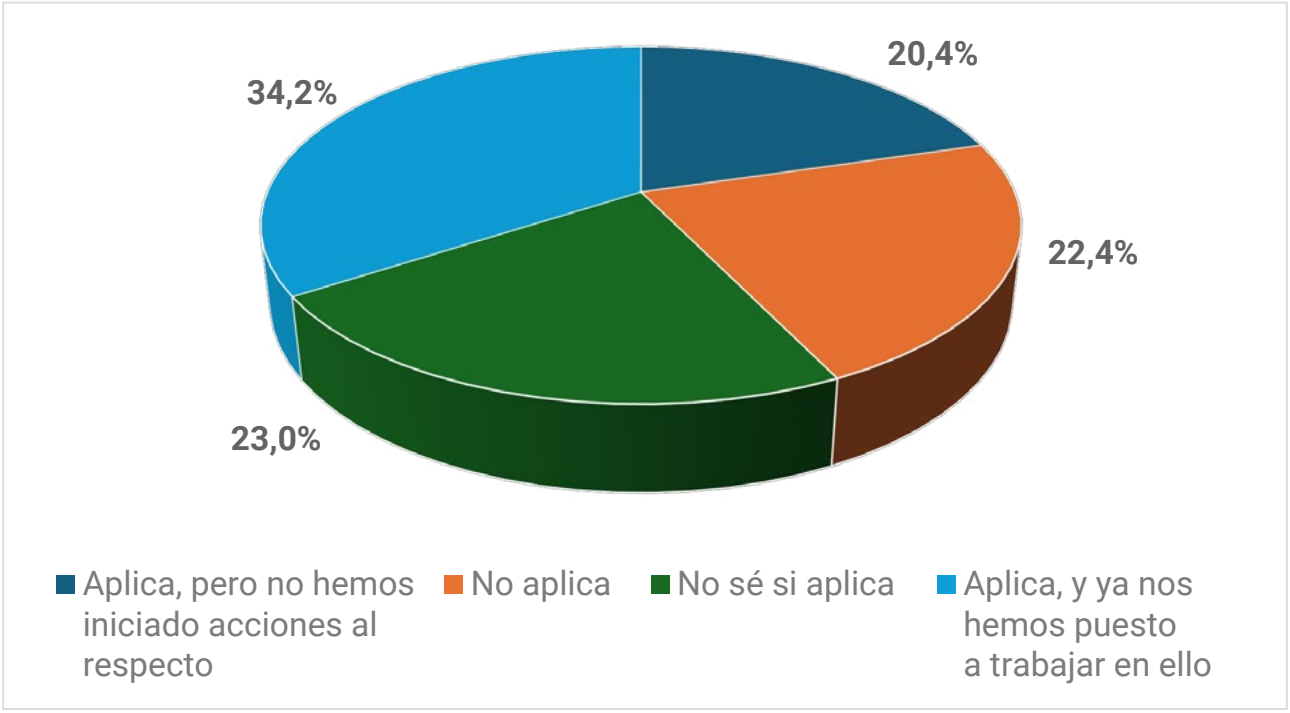
Gobierno de la ciberseguridad



El gobierno de la ciberseguridad en las empresas españolas combina avances claros con importantes carencias estructurales. La medida más extendida es la concienciación a usuarios, presente en un 79,4 % de las organizaciones, seguida por las políticas formales de seguridad (76,8 %) y el análisis de riesgos (69,4 %). Estos datos muestran que las bases están, en general, bien asentadas. También destaca el peso de la gestión de la privacidad (62,8 %) y de la formación especializada (55,4 %), señales de que la seguridad empieza a verse como una función transversal.

Sin embargo, la madurez no es uniforme. Sólo un 51,6 % dispone de un plan de respuesta ante incidentes, una cifra baja si se compara con la frecuencia de ataques, y apenas un 44,2 % cuenta con un comité de seguridad, imprescindible para coordinar decisiones y priorizar inversiones. La certificación ISO 27001 apenas llega al 38,2 %, y el ENS al 23,6 %, lo que evidencia que la certificación formal sigue siendo un reto, sobre todo fuera del sector público. Los datos reflejan un gobierno de la ciberseguridad que avanza, pero con estructuras aún poco consolidadas y una falta de mecanismos formales que permitan coordinar de forma eficaz la gestión del riesgo.

¿Sabes si la Directiva NIS2 aplica a tu empresa? ¿Se han iniciado acciones para su cumplimiento?

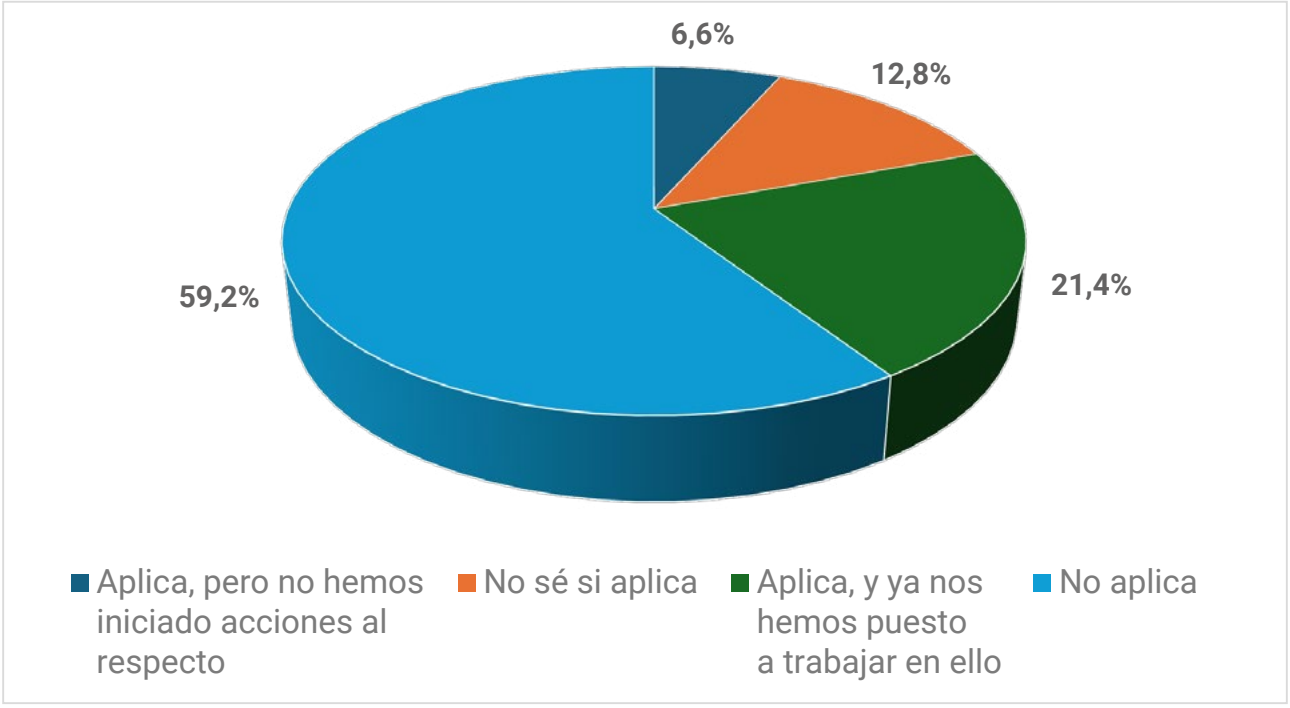


Los datos reflejan que la Directiva NIS2 ya está claramente en el radar de muchas organizaciones, aunque el grado de avance es desigual. Un 34,2 % de las empresas afirma que la directiva les aplica y que ya han puesto en marcha acciones para su cumplimiento, lo que indica que más de un tercio ha comenzado a adaptar sus procesos, controles y estructuras a las nuevas exigencias regulatorias. Sin embargo, un 20,4 % reconoce que, aunque NIS2 sí les afecta, todavía no ha iniciado acciones, una brecha significativa entre conocimiento y ejecución.

A estos grupos se suma un 23 % que declara no saber si la directiva les aplica, un porcentaje elevado teniendo en cuenta que NIS2 amplía de forma sustancial el perímetro de sectores esenciales e importantes y refuerza la responsabilidad de la dirección. Este dato sugiere que muchas organizaciones, especialmente pymes y empresas fuera de los sectores tradicionalmente regulados, aún no han analizado en profundidad su encaje en la normativa. Por último, un 22,4 % considera que NIS2 no les aplica, una percepción que podría cambiar a medida que avance la transposición nacional.

Los resultados dibujan un escenario de toma de conciencia creciente, pero todavía incompleto. NIS2 ya ha activado planes de adaptación en una parte relevante del mercado, aunque persiste un volumen significativo de empresas que no ha pasado de la fase de identificación o que aún no tiene claro su impacto real.

¿Aplica DORA a tu organización? ¿Se han iniciado acciones para el cumplimiento de este reglamento?

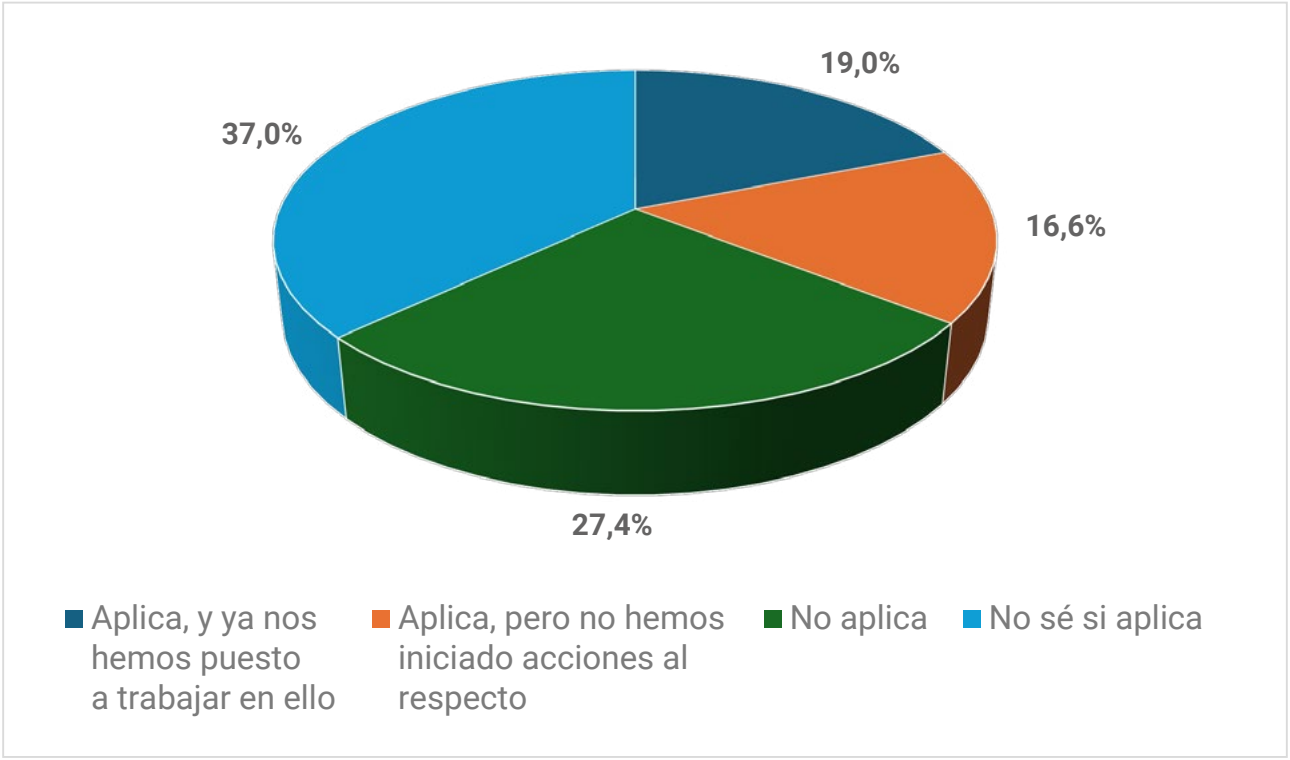


La situación de DORA, el Reglamento de Resiliencia Operativa Digital, presenta un escenario claramente distinto al de otras regulaciones como NIS2, marcado por un perímetro de aplicación más acotado y, al mismo tiempo, por un elevado nivel de desconocimiento fuera del sector financiero. Un 59,2 % de las organizaciones encuestadas considera que DORA no les aplica, un dato coherente con el enfoque del reglamento, centrado principalmente en entidades financieras, aseguradoras y en sus proveedores tecnológicos críticos.

Sin embargo, entre las organizaciones potencialmente afectadas, el grado de avance es todavía limitado. Solo un 21,4 % afirma que DORA les aplica y que ya han iniciado acciones para su cumplimiento, mientras que un 6,6 % reconoce que, aun estando dentro del ámbito del reglamento, no ha comenzado todavía ningún plan de adaptación. A estas cifras se suma un 12,8 % que declara no saber si DORA les afecta, lo que pone de relieve la complejidad del marco y las dudas que siguen existiendo, especialmente entre proveedores tecnológicos que prestan servicio a entidades reguladas.

En conjunto, los resultados muestran que DORA avanza a dos velocidades. Mientras las entidades financieras más maduras ya trabajan en su cumplimiento, una parte relevante del ecosistema tecnológico aún no ha calibrado el impacto que el reglamento tendrá sobre sus procesos, su gestión de terceros y su relación con clientes sujetos a supervisión.

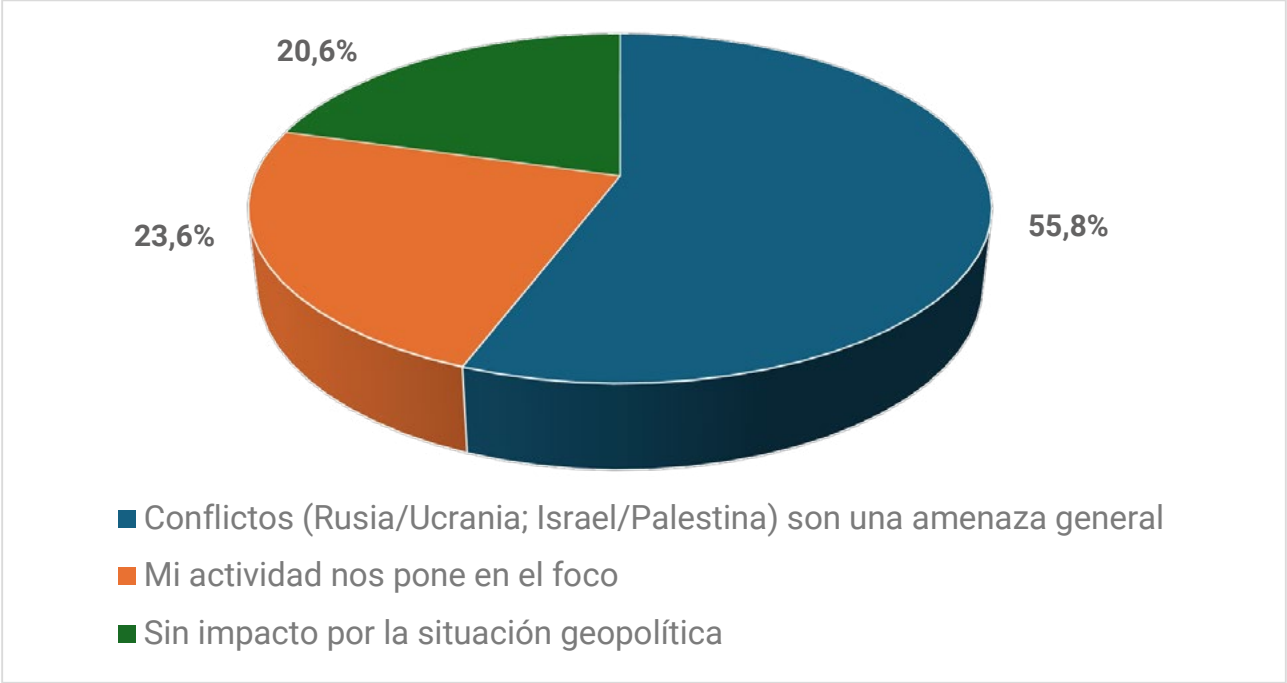
¿Sabes si la Ley de Ciberresiliencia (CRA) aplica a tu empresa? ¿Se han iniciado acciones para su cumplimiento?



Según los datos de la encuesta, existe un conocimiento aún limitado sobre el alcance real de la Ley de Ciberresiliencia. Sólo un 19 % afirma que la norma les aplica y ya han puesto en marcha acciones, mientras que un 16,6 % reconoce que también les afecta, pero todavía no ha iniciado ningún plan de adaptación. Un 27,4 % asegura que no les aplica, aunque es probable que parte de estas respuestas procedan de organizaciones que aún no han analizado en detalle sus obligaciones. Con diferencia, el dato más relevante es que el 37 % no sabe si la CRA les afecta, una cifra elevada que evidencia la falta de claridad regulatoria para muchas empresas, especialmente las de menor tamaño.

Este nivel de desconocimiento contrasta con el impacto que la ley tendrá en el diseño, producción y mantenimiento de productos digitales y servicios conectados. La CRA no es una regulación marginal: establece requisitos obligatorios de seguridad por defecto, actualizaciones, gestión de vulnerabilidades y documentación técnica. Que casi cuatro de cada diez organizaciones desconozcan si están sujetas a la norma subraya la necesidad de una mayor labor de divulgación y de acompañamiento por parte del sector.

¿Cómo crees que afecta la situación geopolítica a la ciberseguridad de tu organización?

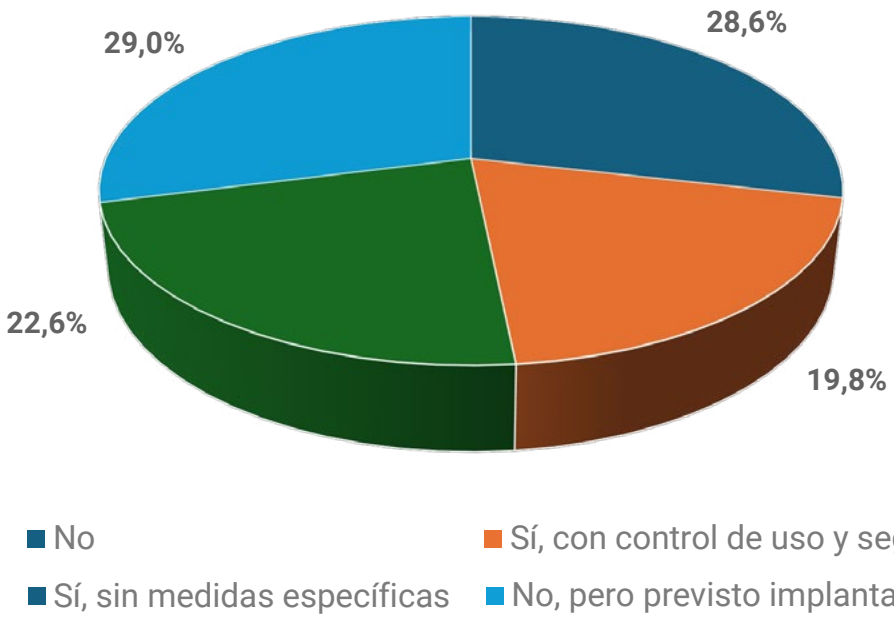


La percepción sobre el impacto de la situación geopolítica es clara: para la mayoría de las empresas españolas, los conflictos internacionales y la tensión entre bloques tienen un efecto directo en su riesgo digital. Un 55,8 % afirma que los conflictos actuales —como Rusia-Ucrania o Israel-Palestina— han incrementado notablemente el nivel de amenaza. Este dato refleja que las organizaciones son cada vez más conscientes de que la ciberseguridad ya no depende únicamente de atacantes oportunistas, sino también de actores vinculados a Estados o grupos alineados con intereses geoestratégicos.

Un 23,6 % asegura que su actividad les coloca especialmente en el foco, un indicador relevante para sectores críticos, organizaciones con operaciones internacionales o empresas tecnológicas que dan servicio a clientes estratégicos. En muchos casos, esta preocupación se vincula a campañas de desinformación, espionaje industrial y ataques dirigidos a la cadena de suministro.

Sólo un 20,6 % considera que la situación geopolítica no tiene impacto en su seguridad, lo que confirma que la mayoría identifica ya el contexto internacional como un factor de riesgo estructural. La lectura global indica que las empresas han interiorizado que la ciberseguridad está cada vez más conectada con los movimientos geopolíticos y con un escenario internacional volátil donde aumentan las operaciones ofensivas y la presión sobre sectores esenciales.

¿Haces uso en tu empresa de herramientas de IA generativa?

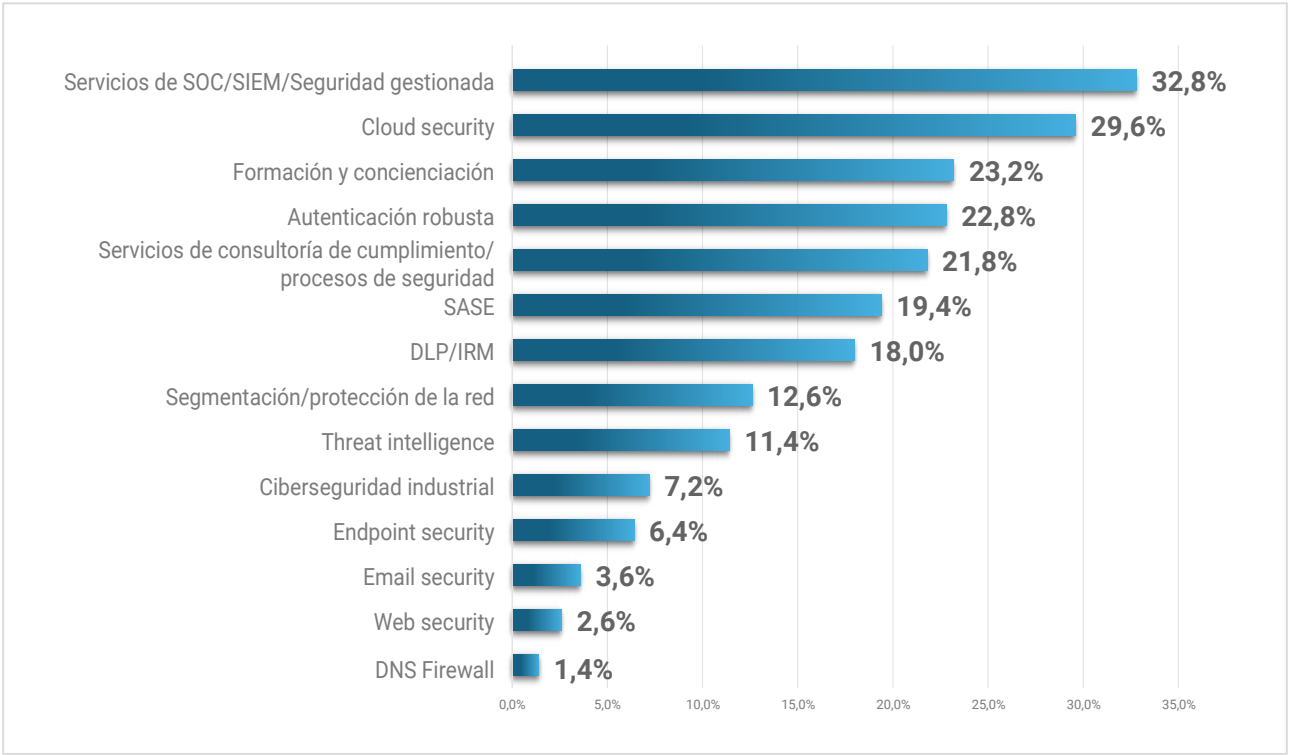


El uso de IA generativa en las empresas españolas avanza, pero todavía con una implantación desigual y, en muchos casos, sin un marco claro de control. Un 28,6 % afirma que no utiliza este tipo de herramientas, mientras que un 29 % reconoce que aún no las emplea, pero prevé incorporarlas a corto plazo. Esto significa que casi seis de cada diez organizaciones están en fase inicial o exploratoria, un dato coherente con el ritmo de adopción que se observa en el tejido empresarial español, especialmente en pymes.

Entre quienes sí han dado el paso, el panorama está dividido. Un 19,8 % asegura que utiliza IA generativa con políticas de uso y medidas de seguridad, lo que refleja un nivel de madurez más elevado y una aproximación consciente al riesgo asociado a estas herramientas. Sin embargo, el 22,6 % declara que la usa sin controles específicos, una cifra preocupante en un momento en el que la filtración accidental de datos, la pérdida de trazabilidad y el uso indebido de modelos externos son riesgos ampliamente documentados.

En conjunto, los datos muestran que la IA generativa ya forma parte del día a día de muchas organizaciones, pero con un grado de improvisación notable. La mitad de las empresas que la utilizan carece de medidas formales para garantizar un uso seguro, lo que evidencia la necesidad urgente de políticas internas claras, formación y marcos de gobernanza antes de escalar su adopción.

¿Cuáles son los próximos proyectos de ciberseguridad previstos en tu organización?

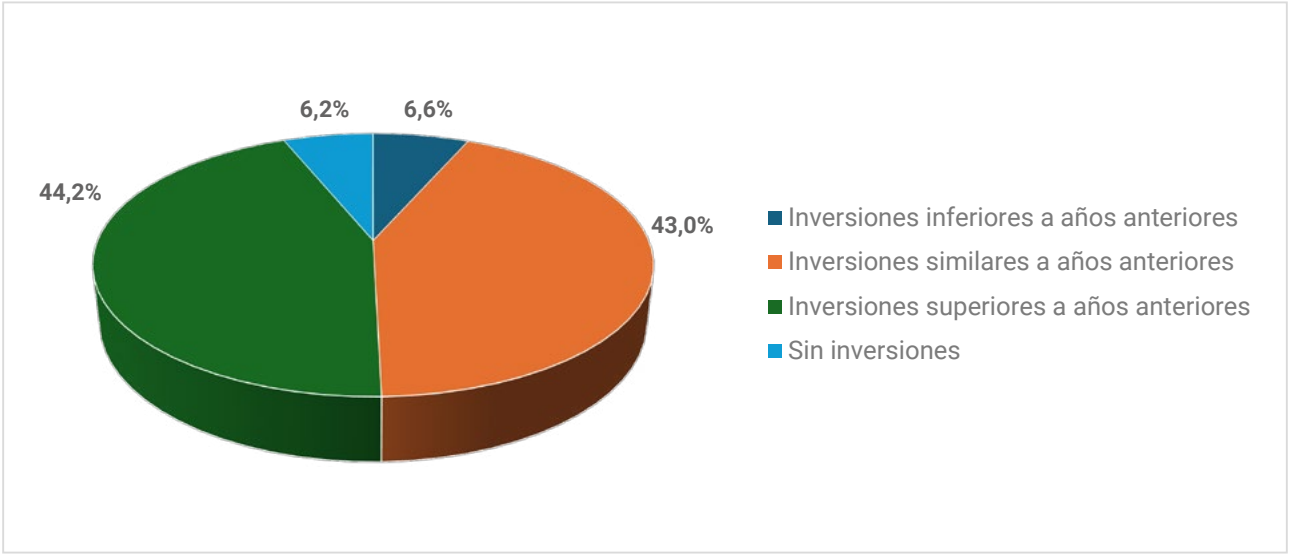


Los proyectos prioritarios para los próximos meses ofrecen una imagen clara de hacia dónde se dirigen las inversiones en ciberseguridad. La iniciativa más repetida es la autenticación robusta, seleccionada por un 32,8 %, lo que confirma que la identidad sigue siendo el punto débil de muchas organizaciones y el eje sobre el que girará gran parte de la modernización del entorno de acceso. La seguridad en la nube aparece como la segunda gran línea de trabajo (29,6 %), un dato coherente con la migración constante de aplicaciones y datos hacia entornos híbridos y multicloud.

Otros proyectos con peso son DLP/IRM (18 %), impulsados por la preocupación por la filtración de información, y los despliegues de endpoint security (6,4 %) y email security (3,6 %), que, aunque ya están implantados en la mayoría de empresas, siguen recibiendo mejoras y actualizaciones. Resulta significativo que la ciberseguridad industrial apenas alcance un 7,2 %, pese al peso de sectores como sanidad, energía o transporte dentro de la muestra. Esto refuerza la idea de que el riesgo OT sigue sin tener la prioridad que requiere.

Los datos dibujan una agenda marcada por la identidad, la nube y la protección del dato, mientras que áreas críticas como OT o DNS Firewall (1,4 %) siguen siendo minoritarias.

¿Qué niveles de inversión en ciberseguridad tendrá tu organización este año?



Las empresas españolas muestran una tendencia claramente continuista —e incluso ligeramente al alza— en materia de inversión en ciberseguridad. La respuesta mayoritaria es que el presupuesto será superior al de años anteriores, opción escogida por un 44,2 % de los encuestados. Este dato refleja que la presión regulatoria, el aumento de la superficie de ataque y la dependencia de proveedores tecnológicos están empujando a muchas organizaciones a reforzar sus recursos, especialmente en protección del dato, identidad y monitorización.

Muy cerca se sitúa el 43 %, que afirma que la inversión será similar, lo que sugiere que una buena parte del tejido empresarial mantiene un nivel de gasto estable, sin recortes, pero también sin grandes saltos estratégicos. En conjunto, más del 87 % declara que mantendrá o incrementará el presupuesto, lo que confirma que la ciberseguridad sigue siendo un área resistente incluso en contextos de incertidumbre económica.

En el lado más vulnerable encontramos dos cifras preocupantes: un 6,6 % indica que sus inversiones serán inferiores, y un 6,2 % asegura directamente que no habrá inversión. Aunque minoritarios, estos porcentajes suelen corresponder a pymes y organizaciones con estructuras menos maduras, donde la seguridad depende de mínimos operativos y donde los riesgos suelen gestionarse de forma reactiva.

La fotografía global es positiva: la ciberseguridad se consolida como una prioridad presupuestaria, pero persisten bolsas de infra-inversión que mantienen abierta una brecha significativa en el mercado español.