# Ciberseguridad en la práctica:

# ¿Qué molesta, qué falta y qué ayuda realmente?

Puntos críticos de las pymes en Europa y África

kaspersky

kaspersky.es

# Índice



**Metodología**
Kaspersky encargó a Arlington Research una encuesta online con responsables de ciberseguridad en organizaciones de menos de 500 empleados en Europa y África. El estudio se realizó en agosto y septiembre de 2025 con 880 entrevistas (600 en Europa y 280 en África). En Europa se encuestó a responsables en Alemania, Austria, Suiza, Reino Unido, Francia, España, Italia, Grecia, Rumanía y Serbia. En África participaron Marruecos, Argelia, Túnez, Camerún, Senegal y Costa de Marfil.

# Top 5 resultados

1. **El 65% de las pequeñas y medianas empresas en Europa y África** cuentan con estrategias teóricas o con objetivos dispersos que no se traducen en una protección real. En España, el **74%** de las empresas tiene una estrategia de ciberseguridad, pero solo el **27%** la tiene completamente implementada (frente al **29%** a nivel global).
2. **El 29% de los encuestados considera** que llevar un seguimiento de todas las ciberamenazas ya supone un trabajo a tiempo completo; en España, este porcentaje es del **28%**. Además, el **18%** afirma no disponer de una plataforma fiable, segura y asequible, porcentaje que desciende al **13%** en el caso de España.
3. **Un 22% reconoce que no cuenta con personal cualificado**, o no lo suficiente, para gestionar y operar las soluciones de ciberseguridad. Concretamente en España, esta cifra es del **18%**.
4. **Un 34% necesita entender mejor cómo optimizar** su capacidad de respuesta durante un incidente; esta cifra en España se eleva al 38%.
5. **Un 21% recibe tantas alertas que no sabe distinguir cuáles requieren atención inmediata**, en el caso de España la cifra se reduce al **10%**.

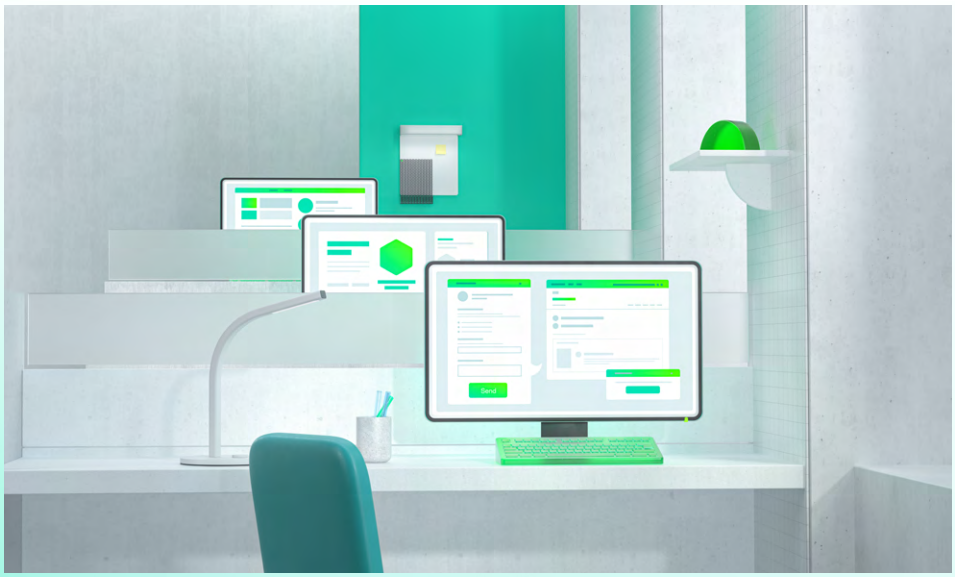
# Introducción

**¿Qué resulta más frustrante, qué falta y qué es realmente útil en materia de ciberseguridad?** Muchas pymes todavía no tienen respuestas claras. Para muchas, la seguridad digital aún se percibe como un rompecabezas costoso y poco claro, lleno de tecnicismos. Resulta frustrante, cara y difícil de entender. Y mientras, el panorama de amenazas sigue evolucionando rápidamente.

Según el Boletín de Seguridad 2024 de Kaspersky, los sistemas de la compañía detectaron una media de **467.000 archivos maliciosos cada día**, un 14% más que en 2023. Solo las detecciones de troyanos aumentaron un 33% y los programas de descarga (droppers) se dispararon un 150%.

Asimismo, el último Informe de Amenazas a Pymes de Kaspersky confirma esta tendencia en Europa y África. En Europa, Austria lideró con un 40% de detecciones de aplicaciones potencialmente no deseadas, seguida de Italia (25%), Alemania (11%), España (10%) y Portugal (6%). En África, Marruecos encabezó con un 41 %, seguida de Túnez (24%) y Argelia (16%).

El mensaje es claro: las pymes ya no solo están en el radar de los ciberdelincuentes;  se han convertido en uno de sus objetivos prioritarios. Pero ¿dónde están los principales puntos débiles en materia de ciberseguridad?



Casi el **75 %** de las pymes están navegando a ciegas, confiando en planes poco claros que no ofrecen una protección real.

# De la pizarra a la realidad

## Estrategias que se quedan en el papel

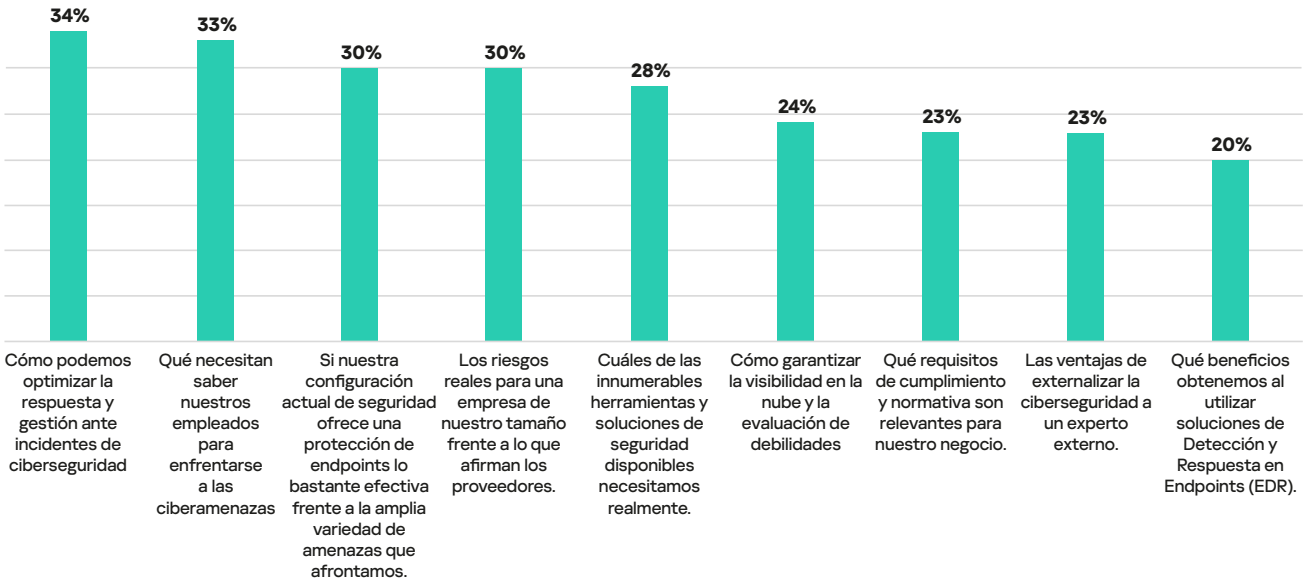
La estrategia de ciberseguridad, así como la implementación de soluciones efectivas, se ven bloqueadas en muchas pymes de Europa y África debido a la falta de conocimientos y al escepticismo generalizado hacia los proveedores de seguridad. A pesar de la gran presencia de la ciberseguridad en los consejos de administración y en las presentaciones de los fabricantes, la realidad de las pequeñas y medianas empresas es muy distinta.

Menos de un tercio de las pymes en Europa y África (29%) afirma tener una estrategia integral de ciberseguridad plenamente implementada; en España, la cifra es ligeramente menor (27%). Sin embargo, un 46% reconoce que su estrategia existe más en teoría que en la práctica, porcentaje que asciende hasta el 62% en España. Además, un 19% trabaja únicamente con objetivos aislados, sin estrategia real en Europa y África (12% en España). Por último, un 5% de las pymes de Europa y África confiesa no tener ninguna dirección en este ámbito. En resumen, el 71% de las pymes en Europa y África - y el 74% en España - operan prácticamente a ciegas.

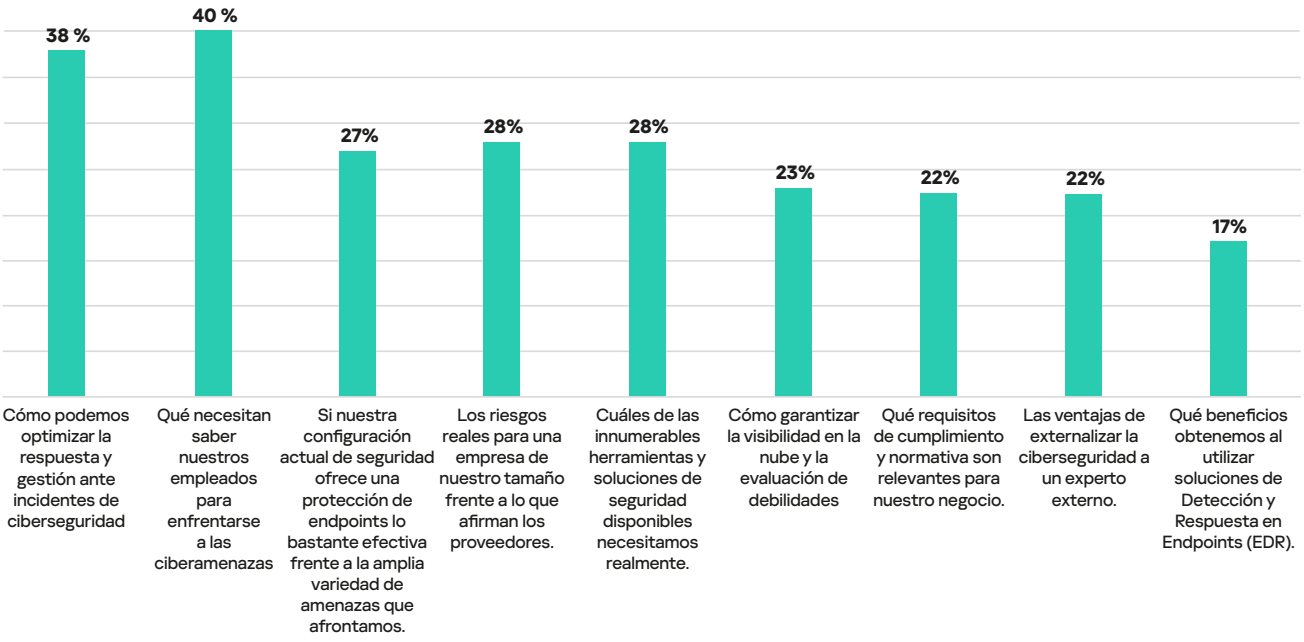
## Los responsables quieren entender mejor la ciberseguridad

Esta desconexión resulta aún más preocupante si se combina con la poca confianza que muestran muchos equipos de TI en sus propias defensas. En torno a un tercio, un 34% para Europa y África y un 38% para España, afirma que necesita mejorar su capacidad de respuesta y resolución de incidentes. Casi la misma proporción (33%), que asciende a un 40% para España, considera que falta formación a los empleados sobre cómo actuar frente a las amenazas digitales. Casi una de cada tres organizaciones, un 30% en el conjunto, y un 27% en España, no tiene claro si su protección de endpoints es lo bastante efectiva frente a la amplia variedad de amenazas actuales, y una de cada cinco, (20%) admite no entender plenamente las ventajas de contar con soluciones de detección y respuesta en endpoints (17% en España).

**Lo que los responsables de decisión quieren comprender mejor**




**Lo que los responsables de decisión en España quieren comprender mejor**




Este escepticismo se extiende al propio mercado. Algo menos de un tercio, un 30% en Europa y África y un 28% concretamente en España, duda de que los riesgos descritos por los proveedores reflejen de verdad los peligros a los que se enfrentan empresas de su tamaño. Mientras tanto, la falta de prioridades claras mantiene a muchas organizaciones atrapadas en un modo reactivo. Menos de un tercio, un 28%, quiere comprender mejor cuáles de las innumerables herramientas y soluciones de ciberseguridad disponibles necesitan realmente, y un 23% (22% para España) tiene dificultades para identificar qué requisitos de cumplimiento o regulatorios se aplican en su caso.

## Europa

En Europa, las pymes del Reino Unido son las más propensas a tener una estrategia, aunque a menudo resulta más teórica que práctica, con un 67%. Les siguen España, con un 62%, y Alemania, con un 53%, frente al 48% de la media en esta región. Alemania también muestra la mayor dependencia de objetivos en lugar de una estrategia (25% frente a 18%).

La incertidumbre sobre la protección de endpoints es mayor en Rumanía, con un 43%, y en Serbia, con un 40%, frente al 31% general de Europa y 27% en España. En el caso de Rumanía, un 38% de las pymes se muestran especialmente preocupadas por diferenciar los riesgos reales para su tamaño de las afirmaciones de los proveedores, un nivel superior al 30% de la media europea y al 28% registrado en España.

## África Occidental y Central

En Camerún, el 28% de los profesionales de ciberseguridad trabajan siguiendo objetivos específicos en lugar de una estrategia definida, una cifra superior al 22% observado en la región africana en general.

Las carencias de conocimiento son más frecuentes en Marruecos (47%) y Camerún (42%), donde las pymes tienen dificultades para optimizar su capacidad de respuesta y resolución ante incidentes, frente al 37% en África en general. En Túnez, casi la mitad, un 45%, no está segura de que su configuración actual ofrezca la protección de endpoints suficiente, frente al 29% del promedio africano. Las pymes argelinas muestran con más frecuencia insuficiente comprensión sobre los riesgos reales para su tamaño en comparación con lo que afirman los proveedores, un 38% frente al 33% en toda la región.

Marruecos también destaca por contar con más pymes que no saben con certeza qué herramientas y soluciones necesitan realmente, un 37% frente al 31% de la media africana. El cloud discovery y la evaluación de vulnerabilidades son retos mayores en Camerún, con un 38%, en Senegal, con un 35%, y en Marruecos, con un 32%, frente al 29% de la media general. En Senegal, la incertidumbre respecto al cumplimiento es especialmente alta, con un 40% frente al 24%.

Las pymes de Camerún presentan el mayor desconocimiento sobre las ventajas de externalizar la ciberseguridad, con un 35% frente al 26% de la media regional. Senegal es el país que más dificultades tiene para reconocer los beneficios del uso de soluciones de detección y respuesta en endpoints (EDR), con un 35% frente al 19% de la media africana.

Los MSP y los distribuidores pueden actuar como asesores de confianza, ayudando a cubrir las brechas de conocimiento y a impulsar una preparación empresarial proactiva.

# La desconexión entre la alta dirección, el departamento de TI y los socios externos

## Sobrecarga, falta de personal y escaso apoyo

La ciberseguridad debería ser una prioridad empresarial, pero aún se sigue viendo como una tarea meramente técnica. Mientras los ejecutivos de la alta dirección debaten sobre presupuestos y prioridades, los equipos de TI de las pymes en Europa y África se enfrentan a un desafío muy distinto: un 18% carece de una plataforma de ciberseguridad fiable, accesible y asequible (13% en España. No es de extrañar que para un 29% de los responsables de TI en total, y 28% en España, el simple hecho de hacer un seguimiento de las amenazas potenciales se haya convertido ya en un trabajo de tiempo completo. El 21% de las organizaciones recibe tal cantidad de alertas del sistema que ya no puede distinguir cuáles requieren atención inmediata, aunque esta cifra se reduce al 10% en el caso de España. Al mismo tiempo, un 18% en total, y un 13% en España, afirma dedicar más tiempo a resolver problemas de su software de seguridad que a defenderse de amenazas reales.

**El último informe de Kaspersky sobre amenazas a pymes** revela que, en **Europa**, las principales amenazas **fueron puertas traseras** con un 24%, **troyanos** con un 17% y programas de descarga **no catalogados como virus** con un 16%. **En África**, el panorama cambia, con los programas de descarga **no considerados virus dominando** con un 55%, **seguidos de objetos peligrosos** con un 14% y **troyanos** con un 13%.

El reto se agrava por la falta de personal cualificado: un 22% de las pymes reconoce que no dispone de suficientes profesionales preparados para gestionar y operar sus soluciones de seguridad (18% en España). La mayoría depende de equipos de TI generalistas, un 36% en total (30% en España), o de especialistas en ciberseguridad integrados en esos equipos (28% frente a un 33% en España). Solo un 29% cuenta con un equipo dedicado exclusivamente a la ciberseguridad (32% en España), y apenas un 8% en total (5% en España) depende principalmente de socios externos para diseñar y ejecutar sus programas de protección.

Las percepciones también moldean la realidad. Las compañías con equipos internos dedicados registran los niveles más altos de satisfacción: un 81% califica su rendimiento como bueno o muy bueno, en el caso de España llega al 95%. Donde los especialistas están integrados en los equipos de TI, la satisfacción es del 76%, que asciende hasta un 90% en el mercado español. En cambio, cuando son terceros quienes diseñan y gestionan la ciberseguridad, solo un 67% da una valoración positiva, lo que deja a un tercio de las pymes decepcionadas con el desempeño de sus socios. Esta insatisfacción puede explicar por qué tan pocas los consideran aliados estratégicos.

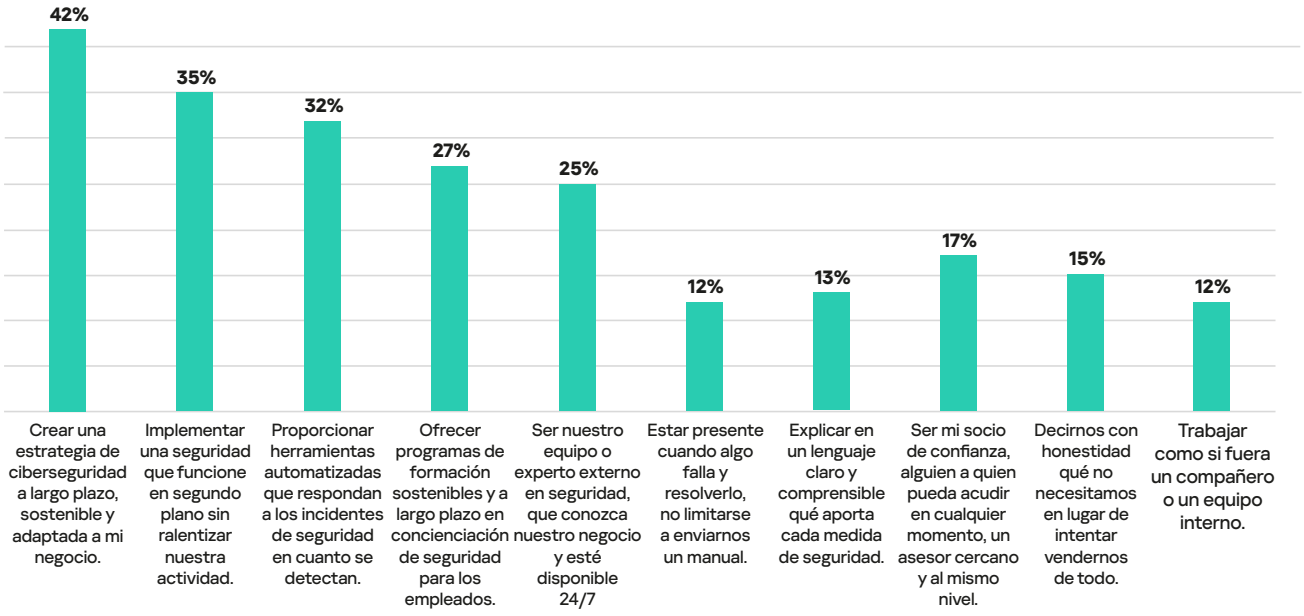
A nivel directivo, el apoyo es limitado. Más de una cuarta parte, un 27% en general y un 32% en España, de los encuestados afirma que sus colegas en la alta dirección no comprenden la relevancia empresarial de la ciberseguridad. El resultado es que en muchas pymes la seguridad digital sigue estancada en lo puramente tecnológico en lugar de tratarse como una prioridad compartida a nivel corporativo.

# Socios externos: de proveedores a aliados

Muchas empresas todavía dependen en gran medida de sus propios recursos internos y reconocen en privado que preferirían contar con ayuda: un 12% de las pymes en general y un 8% en España, afirma que le gustaría que un socio externo gestionara su ciberseguridad, aunque no dispone de ninguno. Incluso cuando se recurre a apoyo externo, los proveedores suelen ser tratados solo como "bomberos" o instaladores de herramientas, llamados para resolver incidencias puntuales, en lugar de ser considerados responsables de la visión estratégica. Sin embargo, las expectativas de las pymes son notablemente coherentes y dibujan la necesidad de una colaboración que vaya mucho más allá de las soluciones a corto plazo. Más de un tercio, un 34% en general, y casi la mitad en España, 42%, anhela un socio capaz de construir estrategias sostenibles a largo plazo, que evolucionen junto con su negocio en lugar de reaccionar al último incidente. Una cuarta parte, un 25% en total y un 27% en España, subraya la importancia de la formación continua de los empleados en concienciación, ya que son tan objetivo de los ciberdelincuentes como lo son los sistemas.

Otros enfatizan la presencia y la confianza. Aproximadamente una de cada cinco empresas, un 22% en general y un 25% en España, quiere contar con un experto que realmente entienda su entorno y esté disponible en todo momento, no solo en horario laboral o después de abrir un ticket de soporte. Otro 20%, 17% en España, busca a alguien cercano, un asesor que forme parte del equipo y ofrezca respuestas honestas en lugar de discursos comerciales. Y un 17% (15% en España) está simplemente agotado de las ventas agresivas. Quieren a alguien dispuesto a decir "no necesitas eso", alguien que simplifique en lugar de complicar.

**Qué debe aportar un socio ideal según los encuestados españoles**




Los proveedores de servicios gestionados (MSP) y los distribuidores pueden asumir el papel de asesores de confianza, cerrando brechas de conocimiento, guiando la toma de decisiones y ayudando a que las empresas pasen de una defensa reactiva a una preparación proactiva.

## Europa

En Europa, los profesionales del Reino Unido son los más frustrados con el esfuerzo que requiere hacer un seguimiento de las amenazas, un 42% frente al 31% general en esta región. La escasez de personal es más grave en Rumanía, con un 32% frente al 21%, y en Alemania, con un 30% frente al 21%. Además, los profesionales italianos reciben tantas alertas que no pueden estar seguros de si son graves o no, un 33% frente al 20%. Serbia se enfrenta tanto a una sobrecarga de alertas, con un 28%, como a la falta de plataformas fiables y asequibles, con un 30% frente al 16%.

Los equipos internos de TI dominan en Suiza, con un 47% frente al 36% en el conjunto europeo. Los socios externos son más habituales en Grecia, con un 18% frente al 7%. En España, un 42% quiere un socio que construya estrategias personalizadas y a largo plazo, frente al 33%. Las herramientas automatizadas que responden de inmediato a los incidentes son más valoradas en Alemania, con un 40%, en el Reino Unido, con un 38%, y en Rumanía, con un 38%, frente al 31% general.

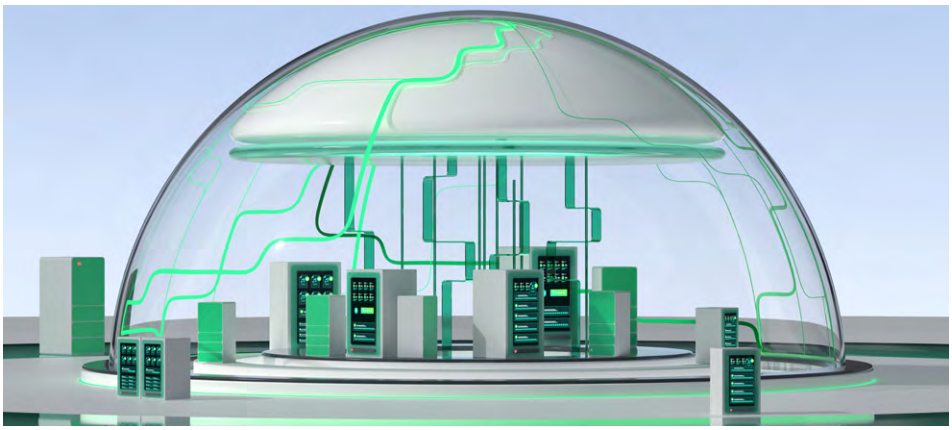
La formación en concienciación de los empleados a largo plazo tiene mayor resonancia en el Reino Unido, con un 32% frente al 25% en esta región. En Francia, un 28% quiere un equipo externo de expertos disponible las 24 horas, mientras que en Alemania se da mayor importancia a los socios que intervienen activamente en las crisis, con un 28% frente al 20%.

Las explicaciones en un lenguaje claro tienen más peso en Francia, con un 28%, y en Austria, con un 27%, frente al 21% general. La idea de un socio de confianza resulta especialmente atractiva en Grecia, con un 30%, y en el Reino Unido, con un 28%. En Suiza, un 27% valora a los socios que les dicen qué no necesitan, frente al 18%, mientras que en Serbia un 33 % prefiere a especialistas que trabajen como colegas internos, frente al 17%.

## España

En España el 28% de los profesionales están frustrados con el esfuerzo que requiere hacer un seguimiento de las amenazas. La escasez de personal preocupa al 18% de los profesionales. El 10% reciben tantas alertas que no pueden estar seguros de si son graves o no, y el 13% echa en falta tener plataformas fiables y asequibles.

En cuanto a quién se encarga de diseñar y controlar la ciberseguridad de las empresas, en el 30% de los casos son departamentos de TI propios. Los socios externos son poco habituales, con tan solo el 5% de los casos. Un 42% quiere un socio que construya estrategias personalizadas y a largo plazo. Otro 32% valora tener herramientas automatizadas que responden de inmediato a los incidentes. La formación en concienciación de los empleados a largo plazo también es muy valorada (27%). Uno de cada cuatro (25%) quiere un equipo externo de expertos disponible las 24 horas. Finalmente, un 12% da mayor importancia a los socios que intervienen activamente en las crisis.



## África Occidental y Central

En África, los profesionales de ciberseguridad en Camerún tienden más a trabajar hacia objetivos concretos que a seguir una estrategia clara (28% frente al 22% en esta región).

La falta de experiencia es más frecuente en Marruecos (47%) y Camerún (42%), donde las pymes tienen más dificultades para optimizar la respuesta y resolución de incidentes (frente al 37% en la región). En Túnez, casi la mitad (45%) duda de si su configuración actual ofrece suficiente protección de endpoints (frente al 29%). En Argelia, las pymes muestran con más frecuencia falta de claridad sobre los riesgos reales a los que se enfrentan según su tamaño, en comparación con lo que prometen los proveedores (38% frente al 33%).

Marruecos también destaca por el mayor número de pymes que no tienen claro qué herramientas y soluciones necesitan realmente (37% frente al 31% en esta región). La gestión de la nube y la evaluación de vulnerabilidades son un reto mayor en Camerún (38%), Senegal (35%) y Marruecos (32%) en comparación con casi un tercio en la región (29%). En Senegal, la incertidumbre en materia de cumplimiento normativo es especialmente alta (40% frente al 24%).

Las pymes de Camerún son las que muestran mayor desconocimiento sobre las ventajas de la externalización (35% frente al 26% en esta región), mientras que en Senegal las mayores dificultades están en comprender los beneficios de la detección y respuesta en endpoints (EDR) (35% frente al 19%).

# Conclusión

Hablar claro sobre ciberseguridad significa ir más allá de las palabras de moda y reconocer las verdaderas frustraciones, carencias y necesidades de las pymes. Lo que resulta molesto, lo que falta y lo que realmente ayuda queda perfectamente reflejado en este informe: equipos sobrecargados, estrategias solo sobre el papel, débil apoyo del liderazgo, pero también una visión clara de lo que las empresas esperan de socios de confianza. El camino a seguir es transformar estos puntos ciegos en resiliencia, mediante soluciones prácticas, una orientación honesta y la combinación adecuada de experiencia y tecnología, ya sea interna o proporcionada por un socio externo de confianza.

# Kaspersky para pymes

**La cartera de Kaspersky cubre un amplio abanico de clientes**, desde microempresas hasta grandes corporaciones, combinando soluciones tecnológicas avanzadas con la experiencia única de sus servicios de Inteligencia de Amenazas y otras áreas. Kaspersky recomienda:

**Kaspersky Small Office Security para microempresas**. Está diseñado para ofrecer una protección de nivel profesional, fácil de desplegar y gestionar, incluso sin contar con un administrador de TI en plantilla. La solución protege frente a los riesgos más relevantes: evita pérdidas financieras, bloquea el acceso a sitios falsos o maliciosos, protege los datos sensibles frente al robo y defiende contra ataques de ransomware.

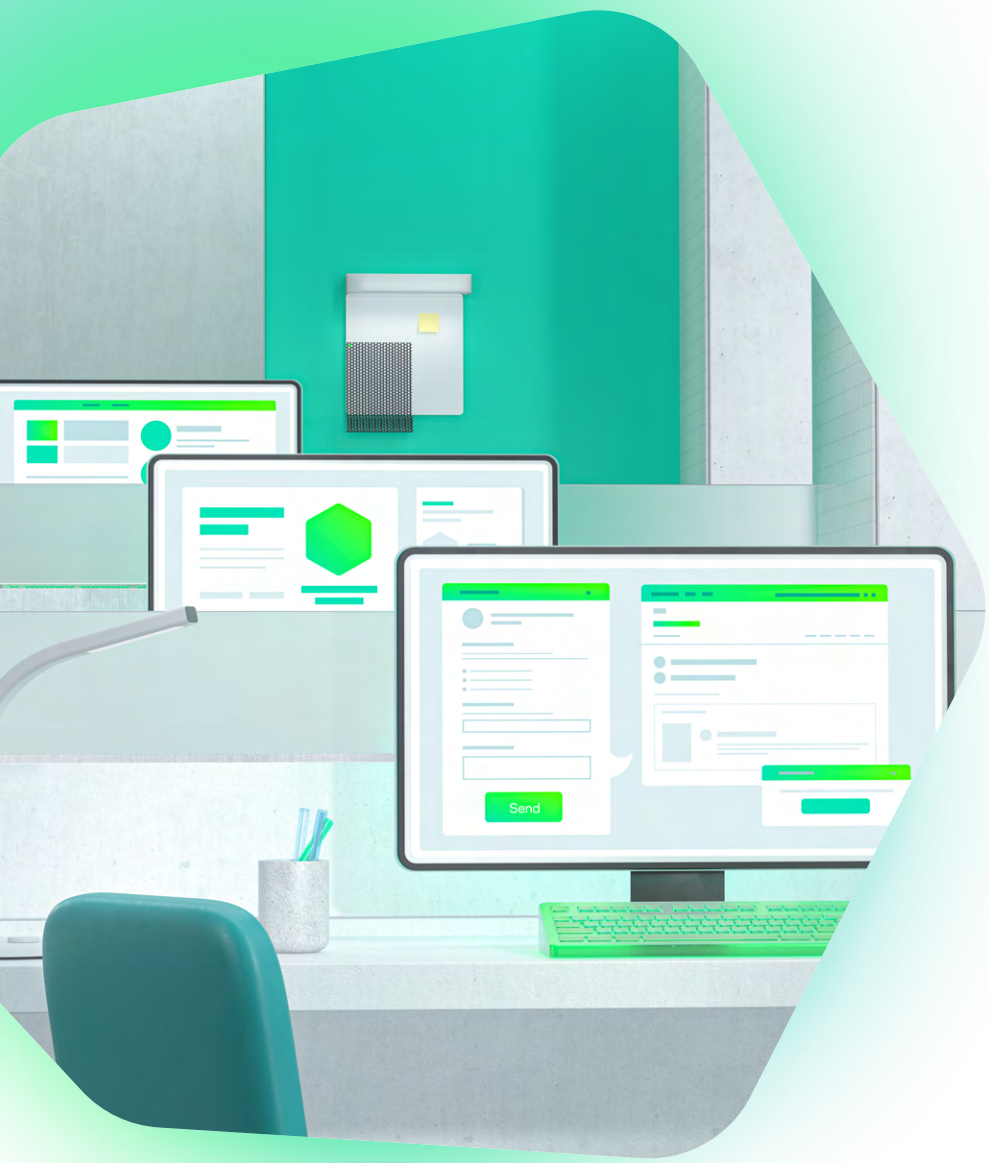
**Kaspersky Next para pequeñas y medianas empresas**. Combina una protección avanzada de endpoints con la capacidad de investigación y respuesta de EDR (Endpoint Detection and Response) y XDR (Extended Detection and Response). Este enfoque integrado proporciona protección en tiempo real, visibilidad práctica de las amenazas y la transparencia que las organizaciones necesitan para detectar, analizar y neutralizar ataques antes de que causen daños.

**Más información sobre cómo las empresas pueden reforzar su seguridad está disponible en Kaspersky Daily, en la última entrada del blog sobre "Security Hardening"**. El fortalecimiento de la seguridad hace referencia a un conjunto de prácticas diseñadas para proteger la infraestructura de TI minimizando la superficie de ataque, es decir, maximizando la seguridad de los sistemas existentes sin depender siempre de herramientas adicionales de protección. Este artículo analiza estrategias esenciales que cualquier organización puede adoptar para limitar su exposición a los ciberataques, especialmente aquellas que cuentan con pocos o ningún recurso dedicado a la ciberseguridad.

## Kaspersky

Kaspersky es una compañía global de ciberseguridad y privacidad digital fundada en 1997. Con más de mil millones de dispositivos protegidos hasta la fecha frente a ciberamenazas emergentes y ataques dirigidos, la amplia experiencia de Kaspersky en inteligencia de amenazas y seguridad se transforma de forma constante en soluciones y servicios innovadores para proteger a particulares, empresas, infraestructuras críticas y gobiernos de todo el mundo. El porfolio completo de seguridad de la compañía incluye una protección líder de la vida digital para dispositivos personales, productos y servicios de seguridad especializados para empresas, así como soluciones Cyber Immune para hacer frente a amenazas digitales sofisticadas y en constante evolución. Ayudamos a millones de usuarios y a cerca de 200.000 clientes corporativos a proteger lo que más les importa.

**Más información en www.kaspersky.es**




News about cyber threats: securelist.com/securelist.lat
IT security news: kaspersky.es/blog/
IT security for SMBs: kaspersky.es/small-to-medium-business-security

kaspersky

kaspersky.es