Informe ciberseguridad en las pymes españolas

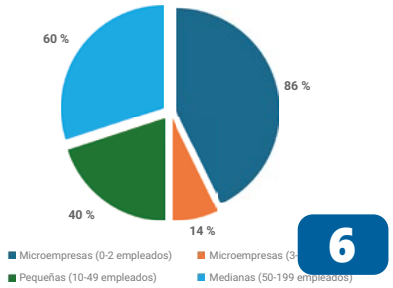
Editorial

Ciberseguridad en las pymes: un reto pendiente para la economía española

Tribuna de Opinión COIT

Ciberseguridad en las pymes españolas: bienvenidos al salvaje oeste digital

Gráficos



La ciberseguridad de la pyme en España

Tribuna de opinión iCraitas

Ciberseguridad en la pyme española: una exposición creciente y una madurez insuficiente

Samsung

"La ciberseguridad para pymes debe ser sencilla, accesible y gestionable"

Sophos

"Muchas pymes solo reaccionan cuando ya sufren un ataque"

Vodafone Empresas

"Muchas pymes no son conscientes del impacto real que puede tener un ciberataque"

Tribuna Women4Cyber

La brecha de talento en la ciberseguridad y la voluntad individual para disminuirla

Ciberseguridad en las pymes: un reto pendiente para la economía española

Las pequeñas y medianas empresas son el corazón de la economía española. La mayoría son microempresas con menos de diez empleados, un tamaño que, si bien permite agilidad y cercanía con el cliente, limita enormemente su capacidad de protegerse frente a los riesgos digitales. La ciberseguridad, más que un lujo, se ha convertido en una necesidad estratégica que muchas pymes aún no logran asumir plenamente.

Aunque la conciencia sobre las amenazas crece, la preparación real sigue siendo desigual. Muchas microempresas confían en que los ciberdelincuentes no las considerarán objetivos atractivos, mientras que las medianas y grandes reconocen que un fallo de seguridad puede afectar seriamente su reputación y su continuidad. La falta de recursos, de formación y de personal especializado impide que buena parte de las pymes adopte medidas básicas de protección, como sistemas de copias de seguridad, actualizaciones de software o formación de empleados.

El impacto de los ciberataques no es solo teórico. Un porcentaje importante de las pymes considera que un ataque podría poner en riesgo la continuidad de su negocio, y las consecuencias económicas y reputacionales pueden ser severas. Aun así, la inversión en ciberseguridad sigue siendo limitada y, en muchos casos, se priorizan otras áreas consideradas más urgentes o rentables.

La comparación con el entorno europeo muestra que las pymes españolas sienten la amenaza con más intensidad, aunque han sufrido menos ataques directos. Esto evidencia un espacio de mejora; no basta con percibir el riesgo, es imprescindible traducir esa preocupación en acciones concretas. La formación, la tecnología y la planificación estratégica son claves para lograr una protección eficaz y sostenida.

España necesita un enfoque decidido. La ciberseguridad debe convertirse en parte integral de la estrategia de cualquier pyme, respaldada por políticas públicas, asesoramiento profesional y herramientas accesibles. La digitalización y la seguridad van de la mano: sin la segunda, la primera queda incompleta, y sin ambas, la competitividad se ve comprometida. La resiliencia digital no es un objetivo opcional, sino un requisito para que nuestras pymes sigan siendo motor económico y fuente de confianza en un mercado cada vez más digitalizado.

Ciberseguridad en las pymes españolas: bienvenidos al salvaje oeste digital

Si las pequeñas y medianas empresas españolas fueran un poblado del Lejano Oeste, el panorama actual sería preocupante: los bandidos ya no entran a caballo, sino disfrazados de correos de *phishing* impecables, SMS urgentes o enlaces que prometen facturas, sorteos o gestiones rutinarias. Y mientras tanto, muchos negocios siguen pensando: "A mí no me va a pasar", "no soy tan importante" o "los ciberdelincuentes van a por peces gordos". Pero ese es, precisamente, el mayor error.

La realidad es que las pymes son hoy el objetivo principal del cibercrimen. Más de tres cuartas partes de los ataques que se producen en el mundo se dirigen a empresas, no a particulares. Y España no es una excepción: cuanto más digital es el negocio, mayor es su exposición. Las pymes manejan datos, pagos, accesos, proveedores, empleados conectados desde distintos lugares... y para un atacante, todo ello es oro puro.

Un negocio más lucrativo que el narcotráfico

Resulta casi inquietante descubrir que el cibercrimen ya mueve más dinero que el tráfico de armas, drogas y personas juntos. La estimación global apunta a un coste anual de cientos de miles de millones de euros, con una previsión de crecimiento que lo colocaría, si fuera un país ficticio, como la tercera economía más grande del planeta. Cada segundo, el mundo pierde más de 300.000 dólares por ataques, fraudes o brechas.

Ainoa Celaya, CEO en Lunamic
Decana del COIT-AORM

Un ritmo que demuestra que este "Salvaje Oeste" digital está lejos de ser una exageración.

Tus datos sí importan —y mucho

En la *Dark Web*, la información personal y corporativa tiene un precio sorprendentemente bajo: desde unos pocos céntimos por credenciales simples hasta varios cientos de dólares por accesos bancarios, historiales médicos o pasaportes. Y aunque el precio no sea alto, el valor real está en lo que permite hacer: suplantar identidades, acceder a cuentas corporativas, robar dinero, manipular operaciones o abrir puertas a ataques más complejos. Es decir: no es el dato en sí, sino lo que habilita.

El perímetro de seguridad ya no existe

Antes, una empresa podía entender la seguridad como un muro alrededor de su oficina. Hoy, ese concepto se ha desintegrado. El teletrabajo, las aplicaciones en la nube, los servicios externos, los dispositivos móviles, los proveedores conectados y la omnicanalidad han hecho que la superficie de ataque se multiplique. Gestionar activos dispersos, empleados híbridos, nubes públicas, redes sociales corporativas y entornos móviles exige nuevas estrategias, porque cada punto débil es una potencial entrada para un atacante.

¿Qué puede hacer una pyme para sobrevivir en este Oeste digital?

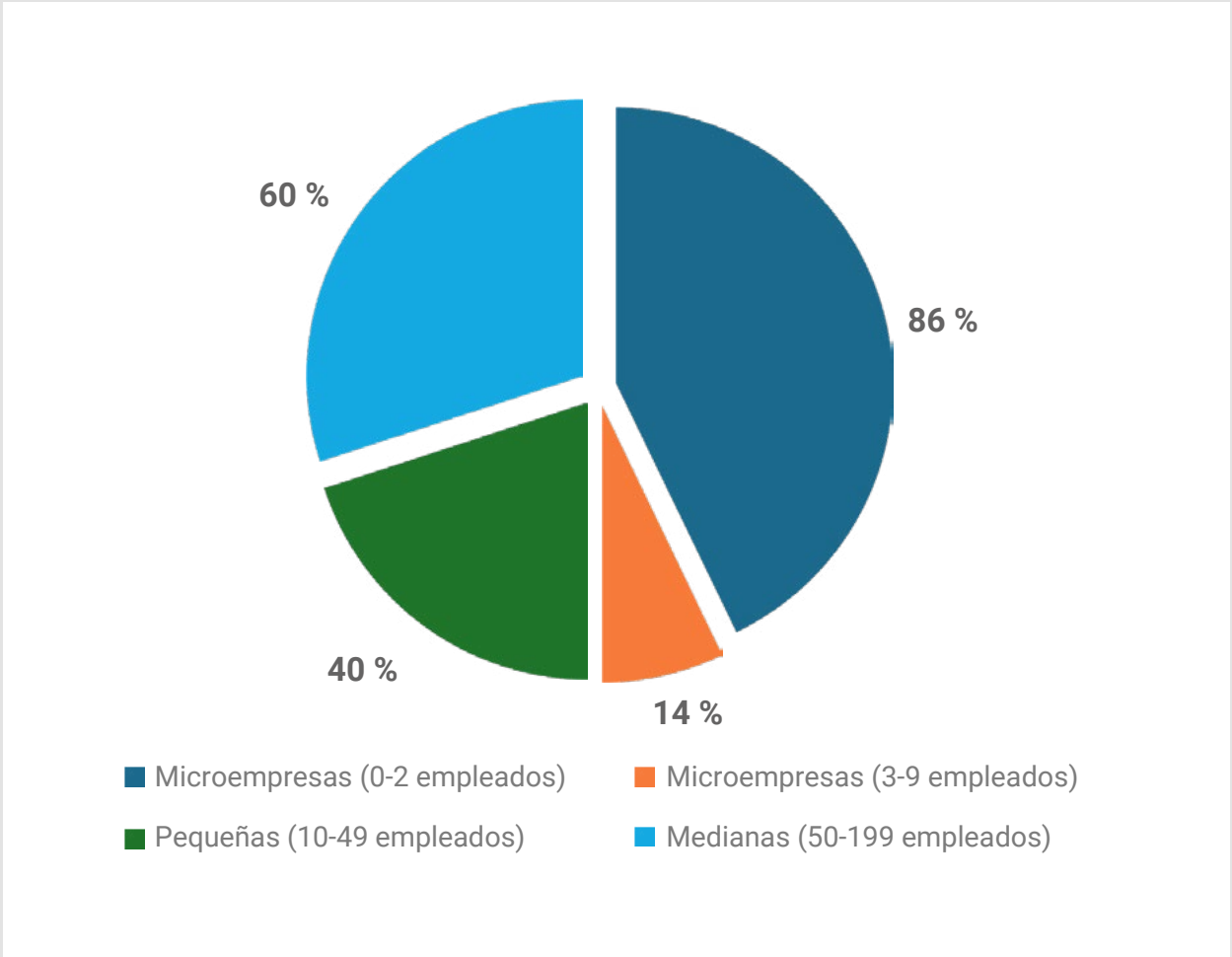
Sobrevivir no exige fortunas ni grandes departamentos de TI. Exige orden, estrategia y continuidad. Algunas claves esenciales:

- **Inventario real y actualizado** de todos los activos tecnológicos, incluyendo móviles, aplicaciones en la nube y "*shadow IT*".
- **Gestión sistemática de vulnerabilidades:** detectar, priorizar y corregir fallos antes de que lo haga un atacante.
- **Formación práctica y continua** a todos los trabajadores incluyendo a los jefes y directivos (eso también va con ellos), que siguen siendo el "eslabón más débil".
- **Control de accesos e identidades,** con contraseñas robustas y autenticación multifactor.
- **Monitorización y detección temprana**, porque la clave ya no es evitar el 100 % de los incidentes, sino reducir el impacto.
- **Protección de la huella digital**, redes sociales y aplicaciones móviles, donde abunda el fraude.

En este Salvaje Oeste 2.0, las pymes no necesitan ser fortalezas infranqueables. Pero sí necesitan dejar de ser bancos sin sheriff. La ciberseguridad se ha convertido en una pieza fundamental para proteger la reputación, la continuidad y la confianza del negocio. Y la buena noticia es que, con medidas adecuadas y constancia, cualquier pyme puede estar mucho mejor preparada que la mayoría.

En definitiva: en un mundo donde los ataques no descansan, la preparación es el nuevo revólver del empresario. Y conviene llevarlo siempre cargado.

1. Distribución de las pymes por tamaño

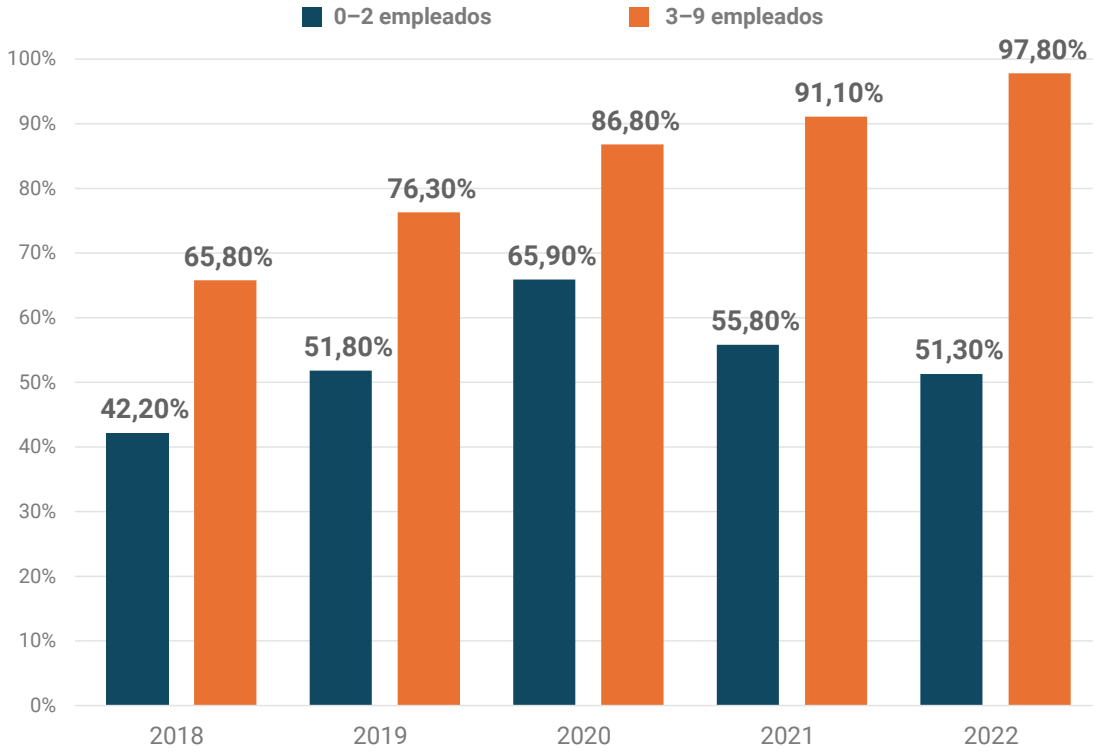


La gran mayoría de las empresas en España son microempresas con menos de 10 empleados, limitando su capacidad de inversión en ciberseguridad. Las pequeñas y medianas empresas, aunque minoritarias, cuentan con más recursos para protegerse frente a ciberataques.

Fuente: Instituto Nacional de Estadística (INE) – Directorio Central de Empresas (DIRCE)

MÁS INFORMACIÓN

2. Ciberseguridad en microempresas según tamaño

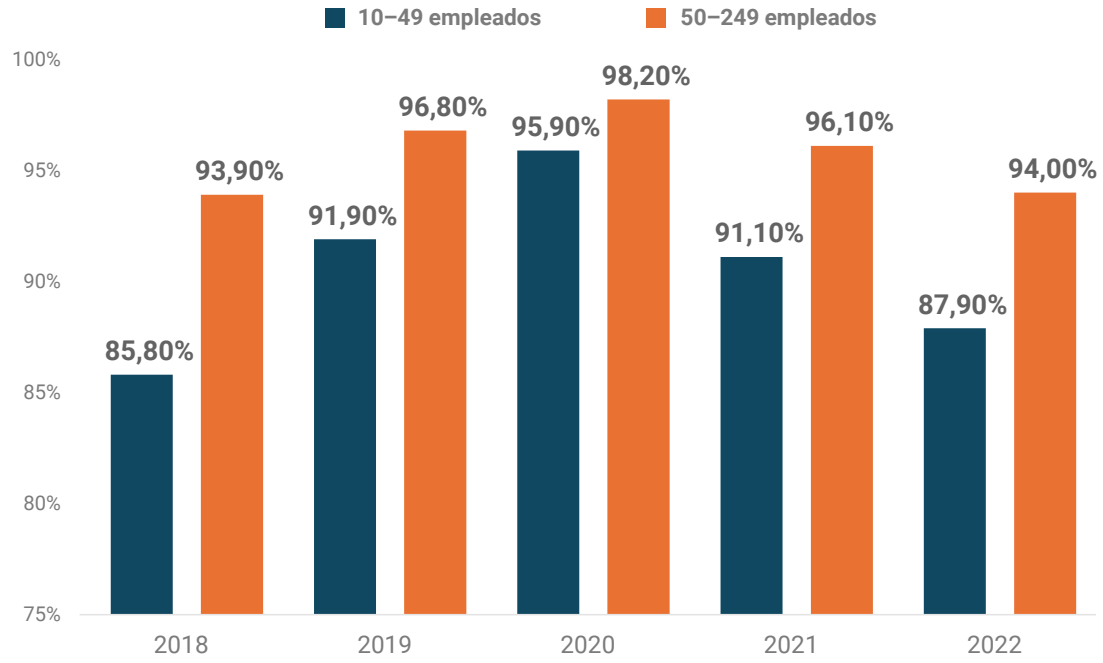


Las microempresas más grandes adoptan más medidas de seguridad TIC. Ambas crecieron hasta 2020, pero las más pequeñas muestran estancamiento posterior, indicando limitaciones de recursos y formación.

Fuente: ONTSI – Informe de Digitalización de la PYME 2024

MÁS INFORMACIÓN

3. Ciberseguridad en pequeñas y medianas empresas

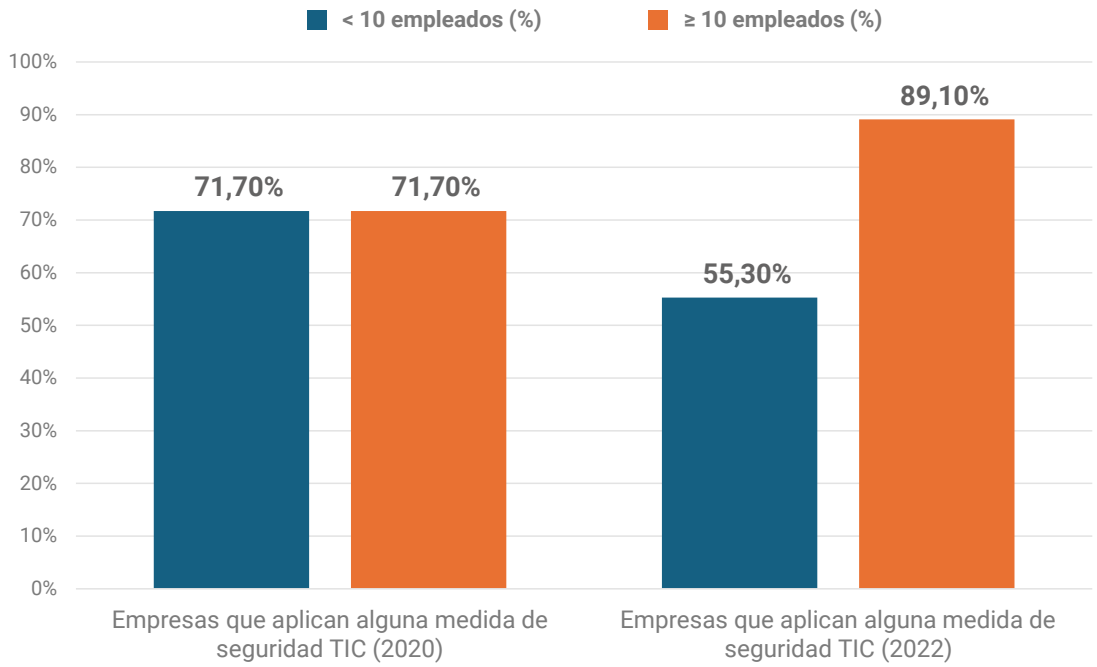


Las empresas medianas mantienen altos niveles de seguridad TIC, mientras que las pequeñas presentan ligeros descensos. El tamaño favorece una adopción más estable y sostenida de medidas de ciberseguridad.

Fuente: ONTSI – Informe de Digitalización de la PYME 2024

MÁS INFORMACIÓN

4. Adopción de medidas de seguridad TIC por tamaño

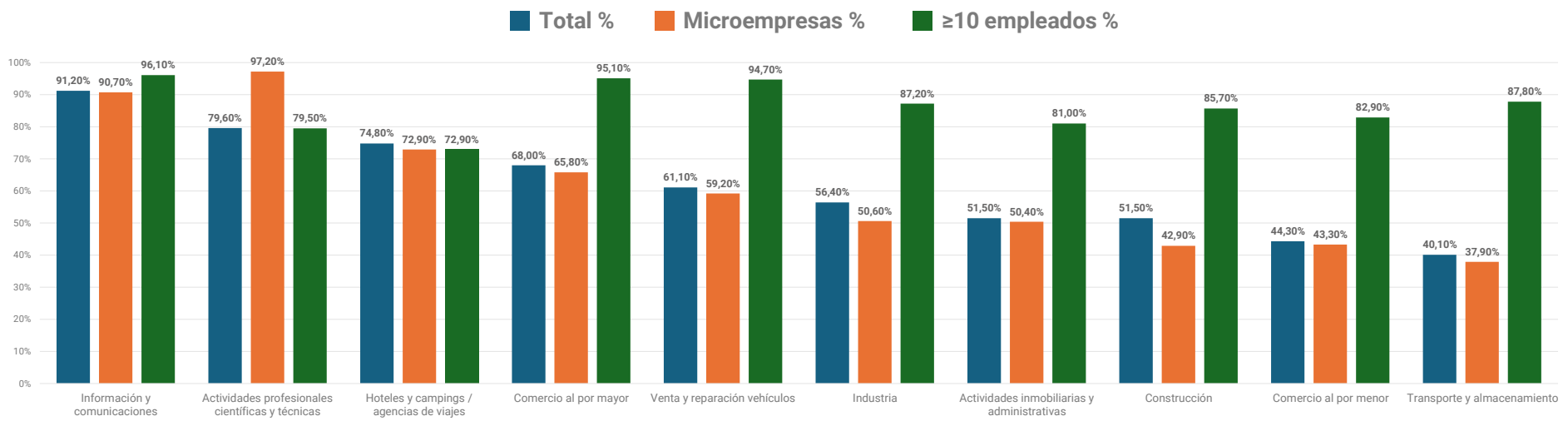


Entre 2020 y 2022, las empresas grandes incrementaron su adopción de seguridad TIC, mientras que las microempresas disminuyeron. Esto refleja dificultades de las más pequeñas para mantener medidas actualizadas.

Fuente: ONTSI

MÁS INFORMACIÓN

5. Empresas con medidas de seguridad TIC por sector

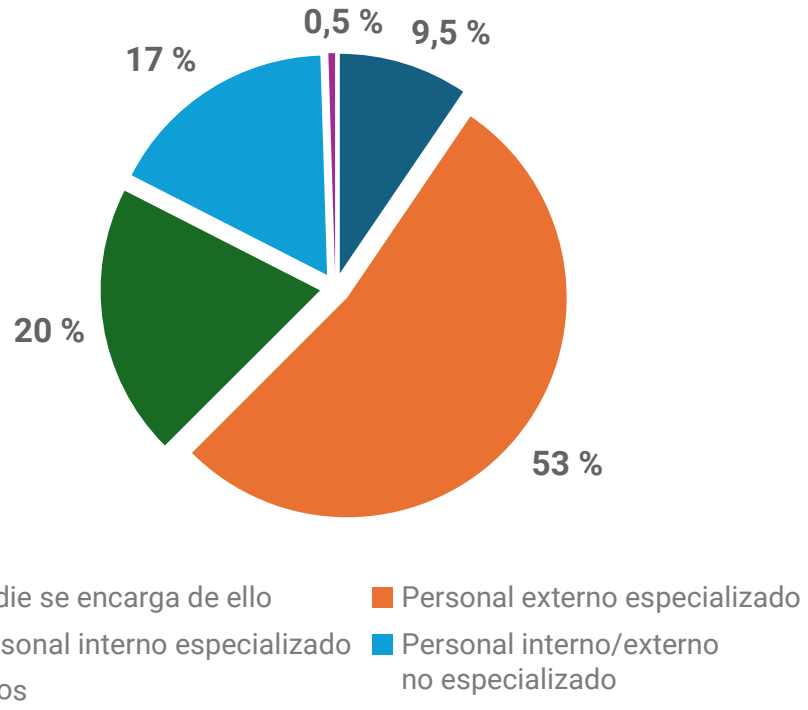


La adopción de seguridad TIC varía por sector. Tecnología e industria presentan mayor cobertura, mientras comercio y servicios muestran menor implantación, sobre todo en microempresas.

Fuente: ONTSI – Informe de Digitalización de la PYME 2024

MÁS INFORMACIÓN

6. Quién gestiona la ciberseguridad en la empresa

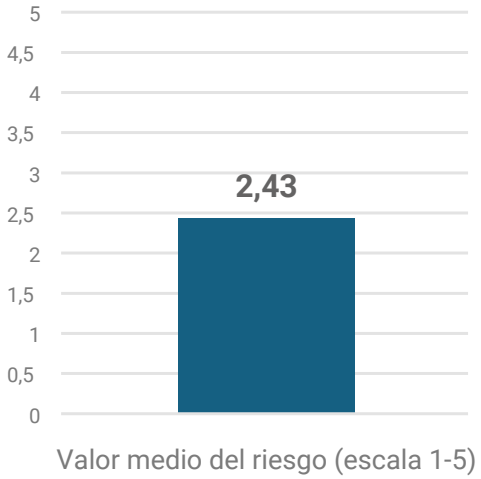


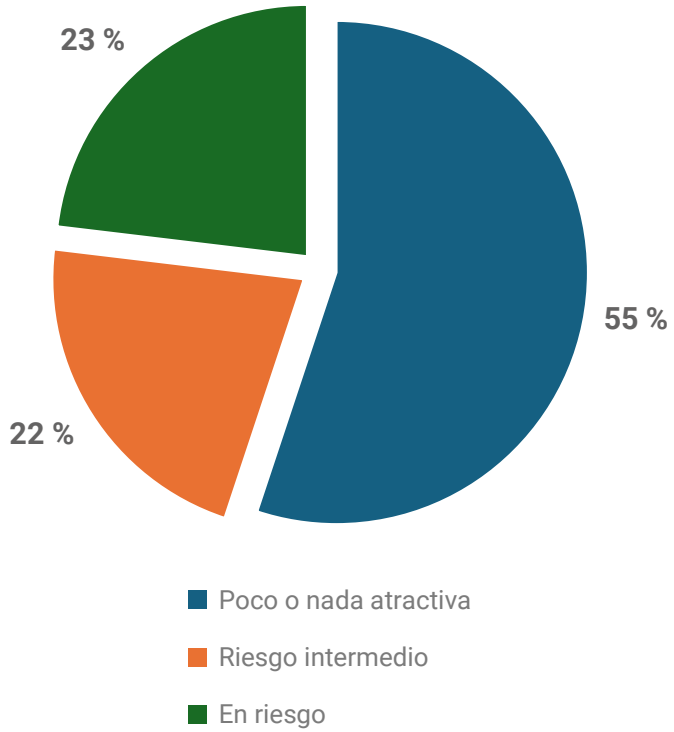
La mayoría de las empresas españolas cuenta con personal especializado para gestionar la ciberseguridad, predominando los proveedores externos. Sin embargo, un porcentaje importante sigue dependiendo de personal no especializado o no tiene asignada ninguna responsabilidad, lo que aumenta su vulnerabilidad frente a amenazas.

Fuente: Cámaras de España. Observatorio de Competitividad Empresarial

MÁS INFORMACIÓN

7. Percepción del riesgo de ciberataque



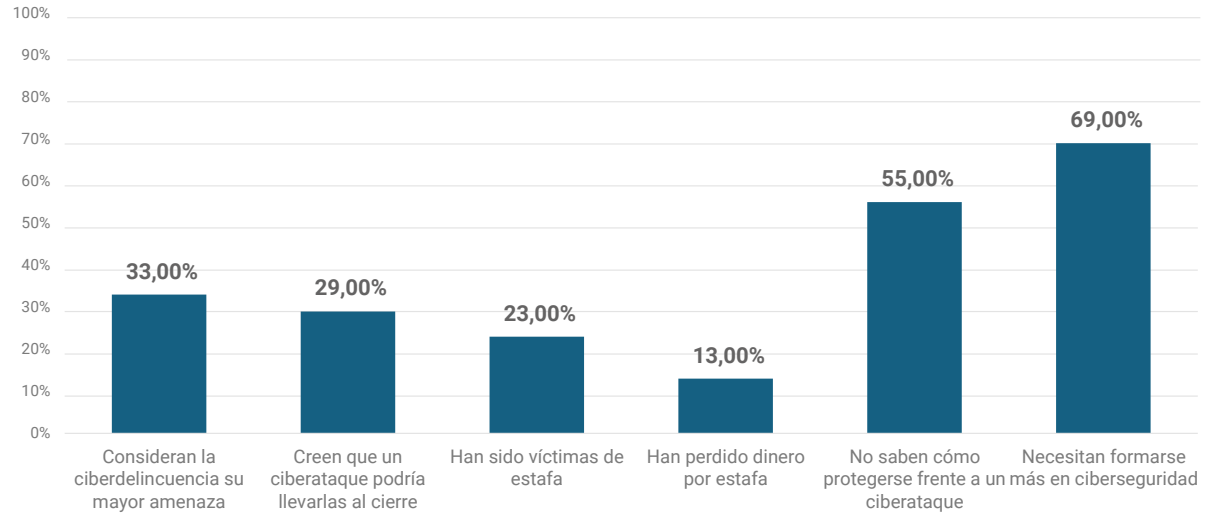


La mayoría de las empresas españolas se percibe con bajo riesgo frente a ciberdelincuentes, aunque esta percepción aumenta con el tamaño, las microempresas tienden a sentirse poco atractivas para los atacantes, con un valor promedio de 1,89, mientras que las empresas más grandes perciben un riesgo mucho mayor, alcanzando un promedio de 3,62.

Fuente: Cámaras de España. Observatorio de Competitividad Empresarial

MÁS INFORMACIÓN

8. Nivel de riesgo y percepción de ciberseguridad en pymes

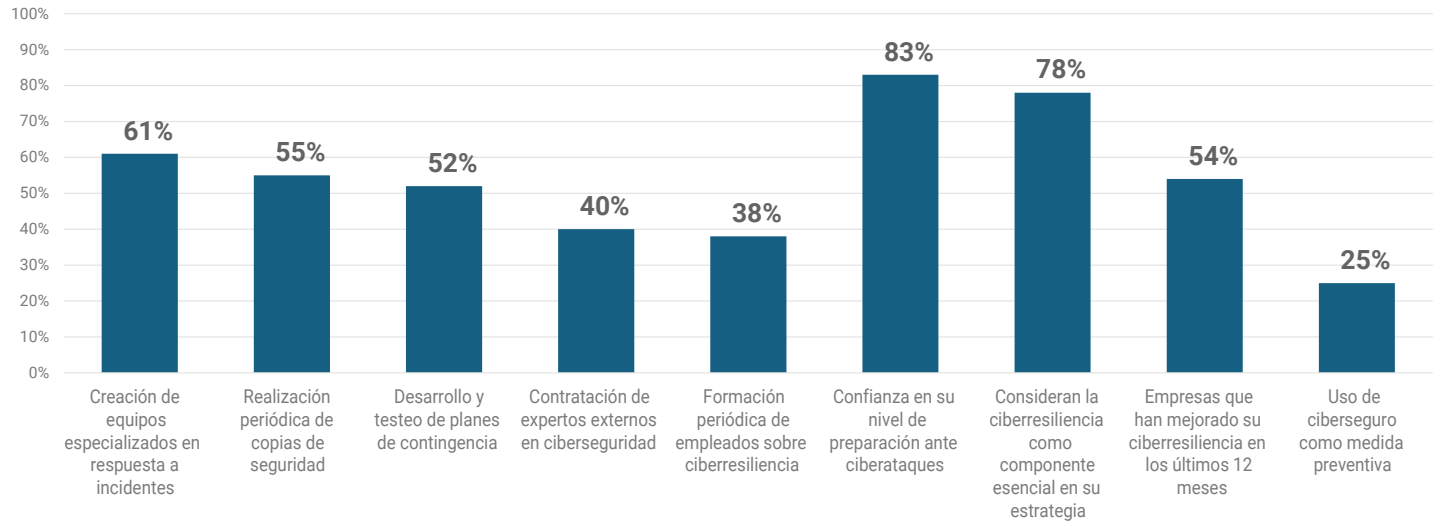


Un tercio de las pymes percibe la ciberdelincuencia como su principal amenaza y más de la mitad no sabe cómo protegerse. La necesidad de formación sigue siendo alta.

Fuente: Mastercard España 2025

MÁS INFORMACIÓN

9. Medidas preventivas adoptadas por las empresas españolas

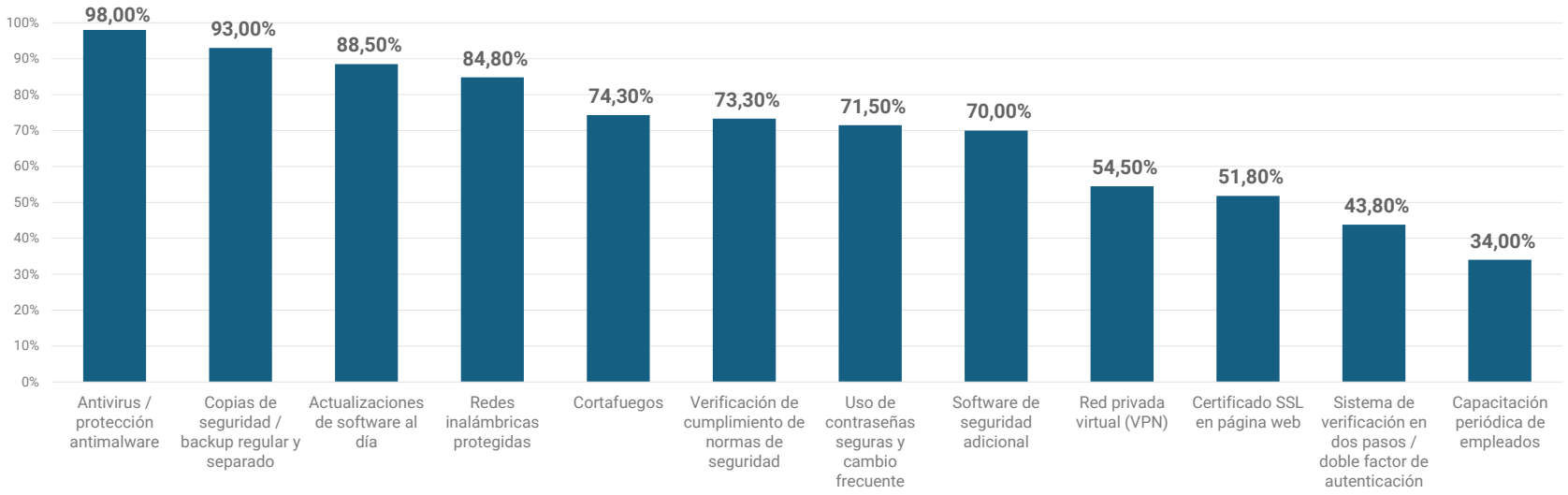


Las empresas españolas han implementado principalmente medidas como equipos especializados, copias de seguridad y planes de contingencia. Aunque el uso de ciberseguros es menor, la mayoría confía en su nivel de preparación y considera la ciberresiliencia un componente estratégico esencial.

Fuente: Hiscox – Informe de Ciberpreparación 2024

MÁS INFORMACIÓN

10. Medidas de ciberseguridad implementadas

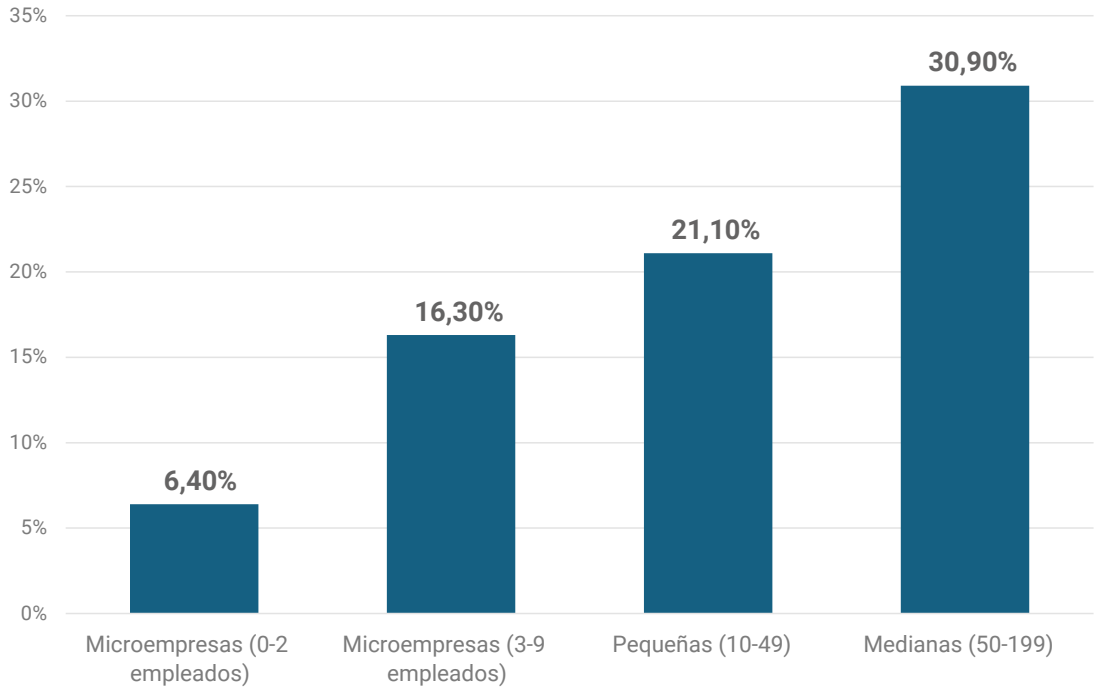


La mayoría de las empresas españolas ya ha adoptado medidas básicas de ciberseguridad, como antivirus, copias de seguridad y actualizaciones de software. Sin embargo, medidas avanzadas como doble factor de autenticación o capacitación continua del personal tienen una adopción menor, mostrando un margen de mejora en la preparación frente a ciberataques.

Fuente: Cámaras de España. Observatorio de Competitividad Empresarial

MÁS INFORMACIÓN

11. Uso de inteligencia artificial en seguridad TIC

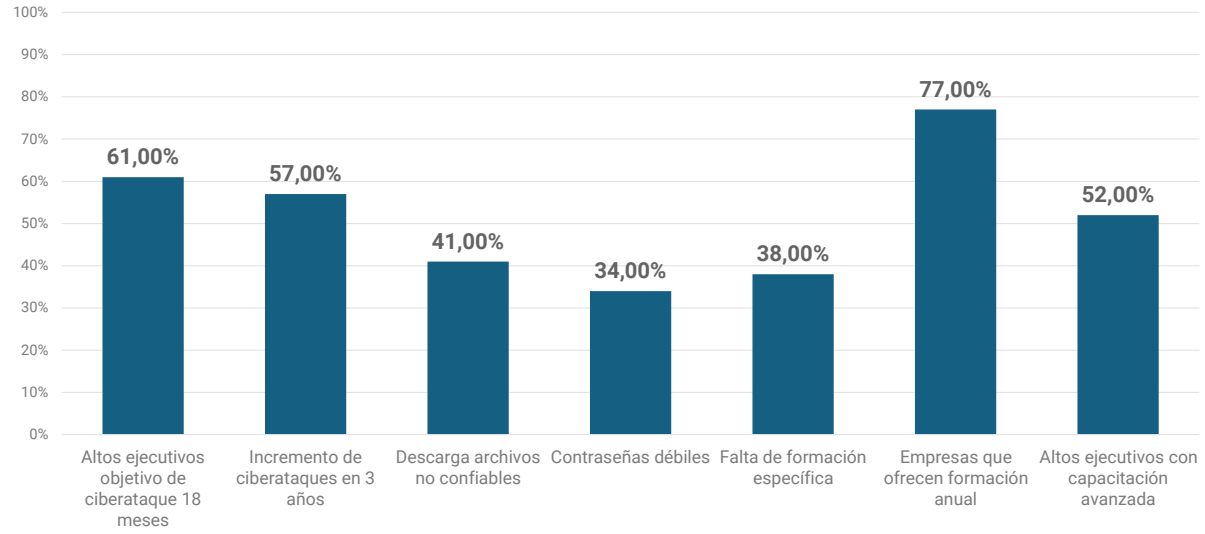


El uso de IA en ciberseguridad crece con el tamaño de la empresa. Las microempresas tienen gran margen de mejora, mientras las medianas avanzan más rápido en su implementación.

Fuente: ONTSI – Informe de Digitalización de la PYME 2024

MÁS INFORMACIÓN

12. Impacto de ciberataques y brechas de formación en líderes de pymes

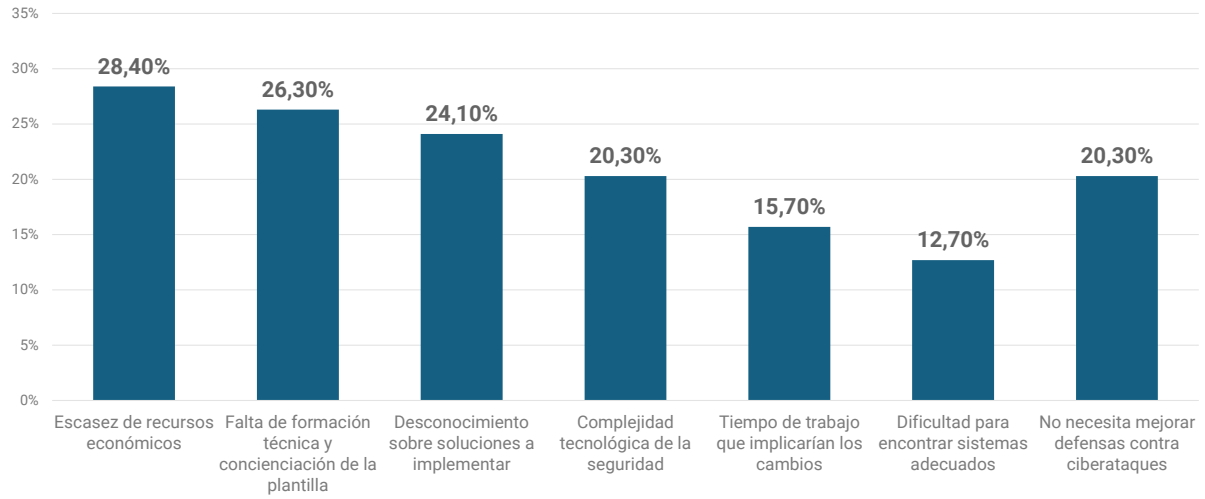


La exposición de los altos ejecutivos a ciberataques sigue siendo alta, con vulnerabilidades ligadas a prácticas inseguras y falta de formación avanzada.

Fuente: Aranda 2024 a través de Anales del Instituto de Actuarios Españoles

MÁS INFORMACIÓN

13. Factores que limitan la mejora de la ciberseguridad

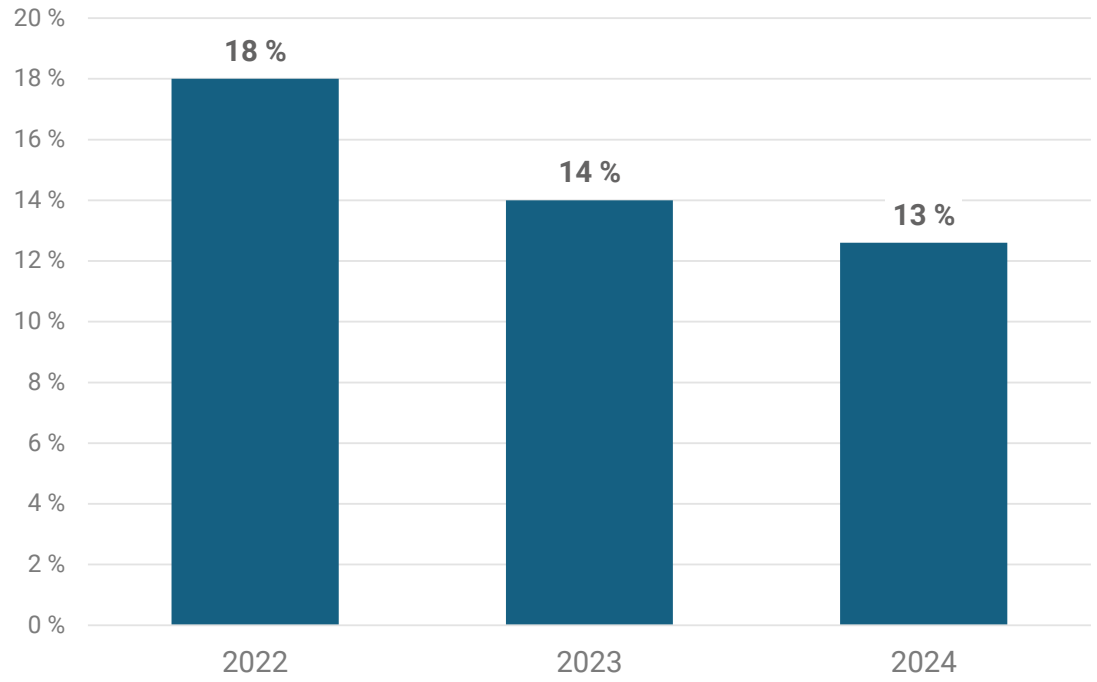


Las principales barreras para mejorar la ciberseguridad en las empresas españolas son la falta de recursos económicos y de conocimiento técnico, seguida de la complejidad tecnológica y la carga de trabajo. Un 20 % considera que no necesita mejorar sus defensas, reflejando percepciones diversas sobre el riesgo.

Fuente: Cámaras de España. Observatorio de Competitividad Empresarial

MÁS INFORMACIÓN

14. Incremento de presupuestos de ciberseguridad en pymes

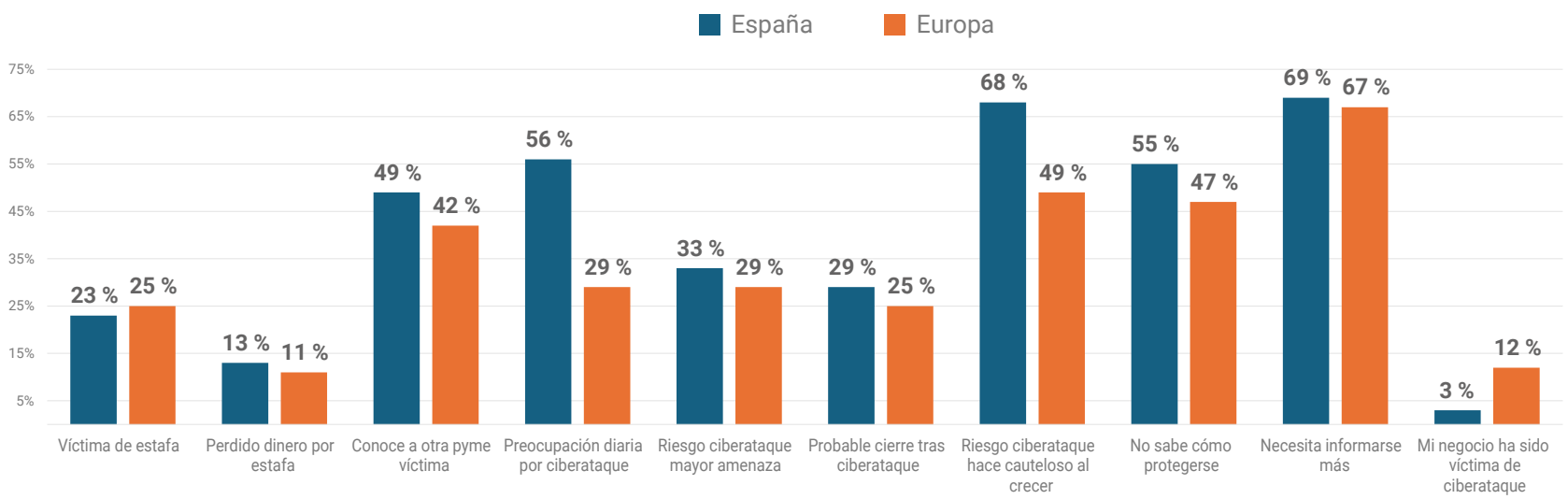


Una parte significativa de las pymes planea aumentar sus presupuestos en ciberseguridad para 2025, reflejando la creciente conciencia sobre los riesgos digitales.

Fuente: PwC 2024 a través de Anales del Instituto de Actuarios Españoles

MÁS INFORMACIÓN

15. Comparación España – Europa sobre ciberseguridad

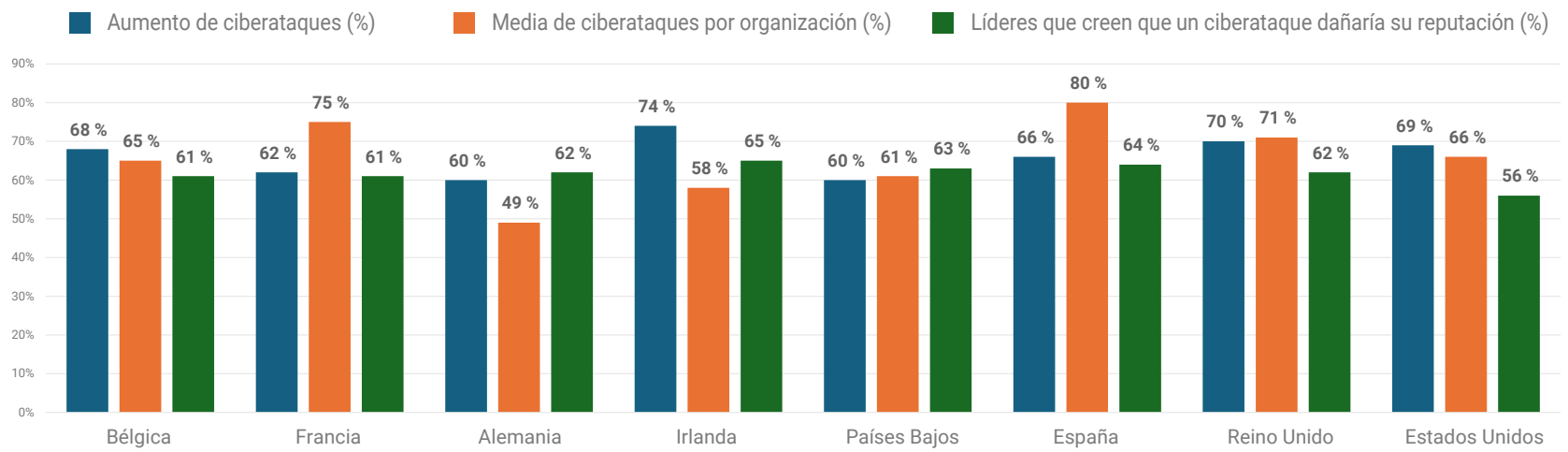


Las pymes españolas muestran mayor preocupación por los ciberataques que la media europea, aunque han sufrido menos ataques directos. La percepción de riesgo impulsa la formación y la cautela.

Fuente: Mastercard España 2025

MÁS INFORMACIÓN

16. Comparativa internacional de ciberataques y percepción de riesgo



España presenta cifras elevadas en el incremento de ciberataques y en la media de ataques por organización, liderando en algunos indicadores. Además, el 64 % de los líderes españoles considera que un ciberataque puede afectar significativamente a la reputación de su empresa, situándose entre los países más sensibles en este aspecto. La comparativa evidencia diferencias regionales y subraya la presión y preocupación que enfrentan las empresas en distintos mercados.

Fuente: Hiscox – Informe de Ciberpreparación 2024

MÁS INFORMACIÓN

Ciberseguridad en la pyme española: una exposición creciente y una madurez insuficiente

El ecosistema de ciberseguridad en la pyme española atraviesa en 2024–2025 un punto de presión evidente: la digitalización crece, pero la capacidad de protección no evoluciona al mismo ritmo. Casi seis de cada diez pymes han sufrido al menos un ataque en el último año, con empresas que reportan varios incidentes anuales, evidenciando brechas sistémicas en controles, procesos y cultura organizativa.

El vector predominante sigue siendo el correo electrónico: *phishing*, fraude del CEO y manipulación de pagos. A ello se añaden campañas automatizadas potenciadas por inteligencia artificial, que generan contenidos más verosímiles y difíciles de filtrar. El ransomware, aunque menos frecuente que en grandes corporaciones, continúa siendo un riesgo crítico por su impacto sobre sistemas no segmentados y entornos con *backups* insuficientemente verificados.

El impacto económico directo —estimado en torno a 50.000 euros para un incidente significativo— refleja interrupciones operativas, pérdida de datos, recuperación técnica y degradación de la confianza de clientes y proveedores. Para una pyme con márgenes ajustados, este impacto compromete su continuidad y cumplimiento contractual.

Déficit estructural

Solo un 20-30 % de pymes dispone de estrategia definida o modelo de gestión documentado. La mayoría opera con controles

Javier Carvajal, CEO de icraitas

parciales: protección perimetral básica, ausencia de gestión de identidades, contraseñas sin políticas robustas, inventarios incompletos y *backups* sin pruebas de restauración. Cerca de dos tercios no realizan formación en ciberseguridad, convirtiendo al usuario final en el punto de fallo más habitual.

La expansión del *cloud* añade complejidad: configuraciones incorrectas, permisos excesivos, falta de supervisión de terceros y dependencia de integraciones sin evaluación de riesgos. El uso creciente de IA introduce vectores adicionales, especialmente en modelos sin controles de privacidad ni evaluación de amenazas.

Regulación y capacidades gestionadas

La entrada en vigor de NIS2, el refuerzo del Esquema Nacional de Seguridad y la mayor exigencia de grandes organizaciones hacia sus proveedores obligan a justificar niveles mínimos de gobernanza, trazabilidad y protección. Paralelamente, servicios gestionados como SOC as a Service, detección y respuesta (MDR) o gestión de identidades permiten externalizar capacidades y elevar la madurez sin incrementar excesivamente la carga interna.

> El reto es pasar de una aproximación reactiva a un modelo operativo basado en riesgos

Del diagnóstico a la acción

El reto es pasar de una aproximación reactiva a un modelo operativo basado en riesgos: establecer inventarios de activos, segmentar redes, implantar autenticación multifactor, verificar *backups* periódicamente, definir políticas de acceso y adoptar formación continua. La tecnología es necesaria, pero insuficiente sin procesos, métricas y responsables claros.

Las pymes que han implantado estas medidas básicas reducen el tiempo medio de detección de amenazas de más de seis meses a menos de 48 horas. Además, el cumplimiento normativo les abre acceso a licitaciones públicas y cadenas de suministro que, de otro modo, quedarían vetadas.

En este escenario donde la exposición aumenta y la regulación se endurece, la ciberseguridad se convierte en requisito operativo, no solo defensivo. Solo las pymes que fortalezcan su arquitectura de seguridad podrán sostener su continuidad y competitividad en los próximos años.

"La ciberseguridad para pymes debe ser sencilla, accesible y gestionable"

Enrique Martínez, director de gran cuenta de Administraciones públicas en Samsung

Con años de experiencia en soluciones tecnológicas, Samsung acompaña a las pymes españolas en su camino hacia una ciberseguridad eficaz. "A menudo las pymes piensan que a ellas no les va a pasar, pero la realidad es que todas pueden ser atacadas", afirma Enrique Martínez, director de gran cuenta de Administraciones públicas. Martínez destaca que muchas pymes carecen de medios y conocimientos para protegerse y que la clave está en la simplicidad y la accesibilidad: servicios gestionados por *partners* permiten externalizar la seguridad y centrarse en el negocio principal.

Aunque el panorama de amenazas se ha vuelto más complejo con *ransomware* y ataques basados en inteligencia artificial, Samsung ofrece soluciones integrales que combinan dispositivos seguros, plataformas de gestión y formación del personal. "No es caro ni complicado para una pyme protegerse frente a ciberataques", asegura Martínez. Su propuesta, Samsung Nox, integra seguridad desde el diseño del hardware hasta la gestión del software, facilitando que las pequeñas y medianas empresas accedan a niveles de protección comparables a los de grandes corporaciones.

"Muchas pymes solo reaccionan cuando ya sufren un ataque"

Fernando Casares, *distributor manager* de Sophos Iberia, analiza la situación de la ciberseguridad en las pymes españolas y alerta sobre la vulnerabilidad de estas empresas. "Es más rentable atacar a 300 empresas pequeñas que a una grande, y el esfuerzo real es el mismo". Casares subraya que muchas pymes aún adoptan un enfoque reactivo, invirtiendo solo cuando el riesgo se vuelve evidente, y destaca la importancia de apoyarse en *partners* de confianza que puedan orientarles en la implementación de soluciones de seguridad. Además, recalca que el factor humano sigue siendo el principal desafío y que la concienciación continua, mediante simulaciones de *phishing* y formación práctica, es clave para que los empleados se conviertan en aliados en la protección de la empresa.

Fernando Casares, *distributor manager* de Sophos Iberia

Sophos ofrece soluciones integrales de *endpoint*, *firewall* y servicios gestionados, combinadas con un equipo de expertos disponible 24/7, democratizando la seguridad incluso para las pymes con recursos limitados. Casares enfatiza que "la ciberseguridad de una pyme debe ser la misma que la de una gran empresa, porque los daños que puede sufrir son mucho más graves".

"Muchas pymes no son conscientes del impacto real que puede tener un ciberataque"

Roberto Lara, director de la unidad de ciberseguridad en Vodafone Empresas, advierte de que muchas pymes españolas todavía no comprenden el impacto real que puede tener un incidente digital en su actividad diaria. Aunque la sensibilidad ha crecido en los últimos años, persiste un enfoque reactivo marcado por la falta de presupuesto, de estrategia y de conocimiento especializado. Lara recuerda que un ataque de *ransomware* puede paralizar por completo a una empresa pequeña e incluso llevarla al cierre, y señala que muchas pymes funcionan como parte de cadenas de suministro de grandes corporaciones, lo que incrementa su exposición. También alerta de que amenazas como el *phishing*, el *ransomware* y el fraude al CEO se han vuelto más accesibles gracias a la inteligencia artificial.

Roberto Lara, director de la Unidad de Ciberseguridad en Vodafone Empresas

Para afrontar este escenario, Vodafone Empresas apuesta por democratizar la ciberseguridad con soluciones automatizadas, sencillas de aplicar y adaptadas a organizaciones con recursos limitados.

La brecha de talento en la ciberseguridad y la voluntad individual para disminuirla

Todos tenemos un papel que jugar para colmar la brecha de falta de talento en ciberseguridad. "Individualmente somos una gota. Juntos somos el mar" (Ryunosuke Satoro).

Vanessa Ventresca, CEO de Almainnova Group

Solventar la brecha de talento es algo que solo podremos hacer juntos como país de manera coordinada y sinérgica, todos aportando para lograr un mismo fin, ya que, como decía el gran jugador Pelé, ninguna persona puede ganar un partido por sí mismo. Sólo si entendemos cómo está el sector, de dónde venimos, los porqués de la falta de talento y la situación de las empresas, de los entes gubernamentales, de los medios de comunicación especializados, de los inversores en ciberseguridad, de las startups del sector, de las entidades educativas, de las personas que no conocen mucho sobre la ciberseguridad y, por último, pero no menos importante, de los cibertalentos, se podrá actuar estratégicamente en cada uno de los grupos mencionados, tomando acciones contundentes para que España se convierta en una nación de cibertalentos que año a año disminuya las diferencias entre la demanda y

la oferta de profesionales del sector, aprovechando esta crisis como oportunidad para salir reforzados. ¡Es ahora el momento!

Para apoyar este fin quisiéramos compartir tres acciones que cada uno de nosotros podemos ejecutar a nivel individual para ayudar ya que, aunque no lo veamos de manera directa, la falta de talento en el sector nos convierte a los españoles en fáciles objetivos de los cibercriminales, colocándonos individual y colectivamente en riesgo.

"La ciberseguridad es una carrera relativamente nueva y con múltiples maneras de acceder a ella y ejercerla: debemos crear más referentes, asesorar y mentorizar a las nuevas generaciones"

Animemos a las niñas y los niños, los adolescentes y a los estudiantes universitarios a empezar a trabajar en el sector de la ciberseguridad. Tenemos la oportunidad de que ese 28,36% de jóvenes en desempleo en 2023 encuentre un hogar laboral donde crear una vida y que ese 10 % de jóvenes considerados Ni-Ni puedan llegar a sentirse útiles y parte de la sociedad en puestos de trabajo dignos.

Visibilicemos a los que día a día trabajan para que estemos ciberseguros, que son los cibertalentos ya establecidos. Si los jóvenes no encuentran referentes no podrán llegar a ser lo que no pueden ver. La ciberseguridad es una carrera relativamente nueva y con múltiples maneras de acceder a ella y ejercerla: debemos crear más referentes, asesorar y mentorizar a las nuevas generaciones, señalando el camino que deben andar para llegar a este mundo. El programa de mentoring de woman4cyber Spain y el CAP (CiberAsesoramientoProfesional) de CybertalentSpain son algunas iniciativas en las que se asesora individualmente para que cada persona encuentre su sitio en la ciberseguridad.

Apoyemos en la creación de espacios donde los trabajadores de la ciberseguridad se sientan en ambientes laborales sanos y protegidos, aplicando los planes de prevención de riesgos laborales y psicosociales para ellos. El trabajo de combatir a los malos es arduo y demandante. Requiere estar siempre en alerta, especialmente para los CISO, en quienes recae injustamente la responsabilidad cuando una empresa cae en manos de los criminales. El síndrome del quemado está muy presente en el sector. Apoyemos a los trabajadores con salarios más acordes a sus capacidades para que, una vez cosechado el talento, no tengan la necesidad de irse fuera de su país.

Con estas breves recomendaciones podremos seguir andando el camino hacia la reducción de la brecha y el progreso económico para el sector y para España. Hay mucho trabajo por delante y, mucho más que podemos hacer: solo tenemos que seguir corriendo juntos y en armonía la carrera.