

beazley

En portada Transformación tecnológica y ciberriesgo 2025

Datos de España



Nuestro estudio

La encuesta de este año se realizó entre el 06.01.25 y el 17.01.25

En 2021, la encuesta se realizó entre encuestados del Reino Unido y Estados Unidos. En 2022 y 2023, la base muestral también incluyó a encuestados de Canadá y Singapur, y en 2024 se amplió para incluir a encuestados de Francia, Alemania y España.

Hemos preguntado a 3.500 empresarios sobre sus mayores preocupaciones en materia de **riesgos empresariales** y cómo de **resilientes** se sienten ante los siguientes riesgos:

- Ciberriesgos
- Riesgo de disrupción tecnológica
- Riesgo de obsolescencia tecnológica
- Riesgo de propiedad intelectual

En enero de 2025 llevamos a cabo esta investigación con directivos de empresas mundiales (compradores de seguros) de distintos sectores industriales.

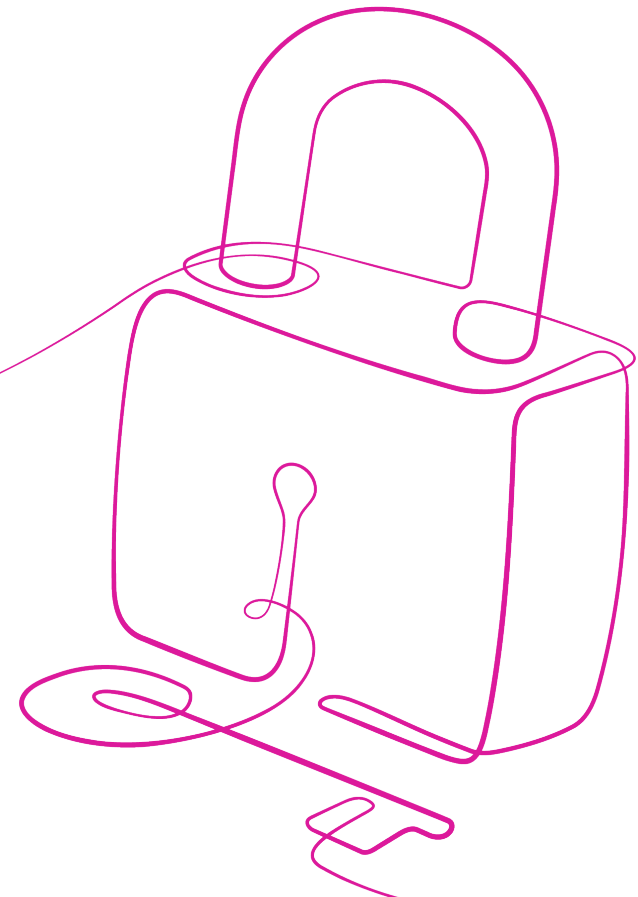
- Sanitario y ciencias de la vida
- Industria, comercio minorista y mayorista, alimentación y bebidas
- Construcción e inmobiliario
- Hostelería, ocio y entretenimiento
- Financiero y servicios profesionales
- Energía y servicios públicos, transporte marítimo y almacenamiento
- Sector público y educación
- Tecnología, medios de comunicación y telecomunicaciones
- Transporte: logística, carga, aviación

Percepción

Aumenta la preocupación por los riesgos ciber y tecnológicos; además, los directivos se sienten más preparados para afrontar estos riesgos.

Realidad

Muchas empresas están expuestas y no preparadas para las amenazas digitales, que evolucionan a gran velocidad.



Las empresas con sede en España se enfrentan a innumerables riesgos ciber y tecnológicos que exigen una continua gestión del riesgo.

Las empresas necesitan ayuda para aplicar una **defensa en profundidad** y aumentar su resiliencia.

27%

Identifica los ciberriesgos como su mayor amenaza este año, frente al 29% en 2024. Aún así, el 87% se siente preparado* para hacer frente a estos riesgos, frente al 83% de 2024.

34%

Planea invertir en mejorar la ciberseguridad este año, frente al 23% en 2024.

26%

Clasifica el riesgo de obsolescencia tecnológica como su principal amenaza cibernética y tecnológica este año, en comparación con el 23% en 2024.

83%

Reconoce que su empresa tiene previsto mejorar la ciberseguridad con sus proveedores externos tras los ciberincidentes sistémicos de gran repercusión.

87%

Está de acuerdo en que la IA tendrá un impacto positivo en las perspectivas económicas de su empresa este año, mientras que el 69% está de acuerdo en que la IA sustituirá puestos de trabajo en su empresa en los próximos 18 meses.

24%

Califica el riesgo de propiedad intelectual como su mayor amenaza este año, frente al 21% de 2024. Al mismo tiempo, su sensación de resiliencia frente a este riesgo aumenta, ya que solo el 10 % no se siente preparado**, frente al 20 % en 2024.

* Respuestas “muy y medianamente preparadas” combinadas.

** Respuestas “no muy bien y nada preparadas” combinadas.

¿Qué nos muestran los datos?

- Muchas empresas sobrestiman su resiliencia frente a los riesgos cibernéticos y tecnológicos.
- Son muchas las organizaciones que no están suficientemente preparadas para un ciberincidente o robo de datos.
- Las empresas quieren mejorar su ciberseguridad.
- Crece el optimismo en torno a los beneficios empresariales de la IA.
- Disminuye la preocupación por el riesgo de obsolescencia tecnológica.

Conclusiones del informe

Para los corredores

- 1. La ciberresiliencia es más que una cobertura de seguro**
Las empresas necesitan una ciberseguridad por capas y un apoyo preventivo, reactivo y adaptativo que les ayude antes, durante y después de un incidente cibernético; y no solo limitarse a contratar un ciberseguro.
- 2. Responsabilidad frente a terceros**
La interconectividad tecnológica actual crea vulnerabilidades en los proveedores que dan lugar a responsabilidad civil frente a terceros, desde el riesgo cibernético y la interrupción de la actividad empresarial hasta las reclamaciones contra los D&O y la pérdida de reputación.
- 3. Las tensiones políticas aumentan el ciberriesgo**
A medida que aumentan las tensiones geopolíticas y cambian las relaciones, también lo hace el riesgo cibernético, ya que las amenazas de los Estados nación crean nuevas vulnerabilidades que los ciberdelincuentes pueden explotar.

Para las empresas

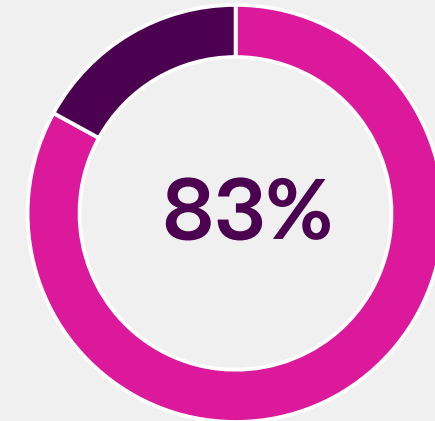
- 1. Una preocupación creciente para los accionistas**
A medida que aumenta el ciberriesgo, también lo hace el riesgo de incidentes y daños a la reputación. Las malas decisiones en materia de ciberseguridad deben hacer frente ahora a un mayor escrutinio, exponiendo a las empresas a consecuencias financieras y operativas.
- 2. Todas las miradas puestas en la propiedad intelectual y la privacidad de los datos**
Las normativas nacionales sobre propiedad intelectual y privacidad de datos son diferentes por región y crean riesgos para las empresas que operan a escala internacional, ya que, sin darse cuenta, podrían infringir la nueva legislación. Sin embargo, la preocupación por el riesgo disminuye.
- 3. Aprovechar el poder de la IA**
El 39% de los ejecutivos españoles prevé invertir en nuevas tecnologías este año, y **el 69%** anticipa pérdidas de empleo inducidas por la IA en los próximos 18 meses. Las empresas deben estar atentas a las mejores prácticas con los riesgos relacionados con la IA.

El espejismo de la ciberseguridad

Las empresas de todo el mundo se enfrentan a innumerables riesgos cibernéticos y tecnológicos.

Conexiones vulnerables

- El riesgo cibernético de los proveedores externos aumenta a medida que las cadenas de suministro se interconectan y aumenta la vulnerabilidad a los ciberataques.
- Los ciberdelincuentes atacan a las grandes empresas a través de pequeños proveedores que pueden carecer de los recursos necesarios para mantener una ciberseguridad robusta.
- La externalización de la ciberseguridad puede crear una falsa sensación de seguridad y no elimina la necesidad de:
 - Formación activa de los empleados
 - Planificación de la continuidad de la actividad
 - Mantenimiento de las mejores prácticas internas
 - Estrategias de Ciberseguridad basadas en defensa en profundidad



de los ejecutivos con sede en España coincidieron en que su empresa está planeando mejorar su ciberseguridad con sus proveedores externos tras los recientes ciberincidentes sistémicos.

El espejismo de la ciberseguridad

Los Estados-nación hacen uso de cibertécnicas como una forma de ciberguerra. Además, la inteligencia artificial aumenta la eficacia de los ciberdelincuentes.

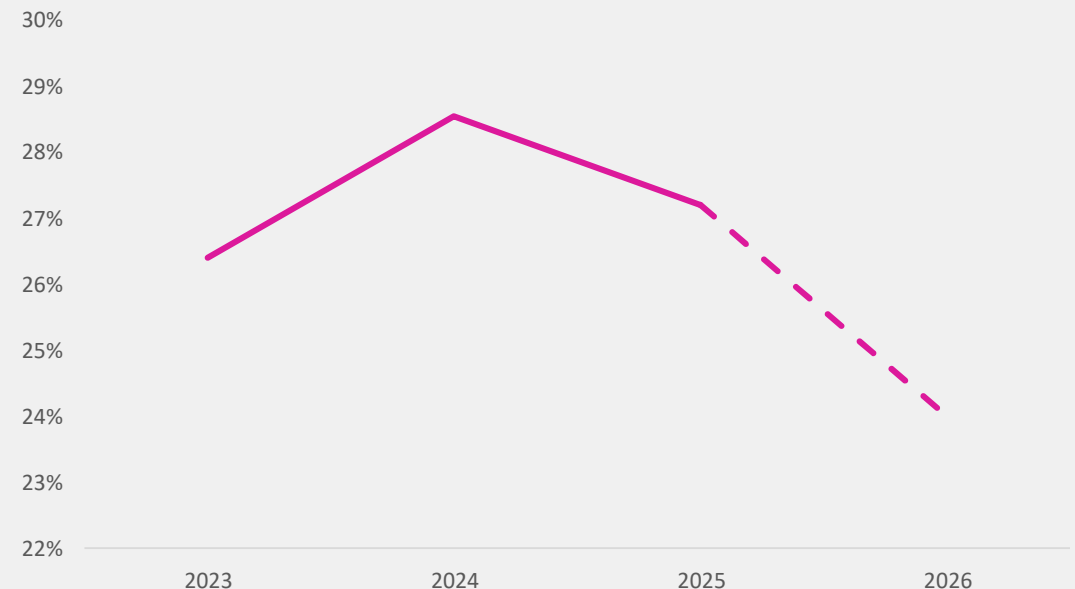
La intersección entre política y ciberseguridad

- Los ciberataques son ahora herramientas de la guerra híbrida, utilizadas para crear perturbaciones y ejercer presión política.
para crear trastornos y ejercer presión política.
- Los hacktivistas utilizan los ciberataques para maximizar el impacto de sus reclamaciones y programas. Estos ataques a menudo persisten en los sistemas y suponen una amenaza a largo plazo.

Evolución del ransomware

- El auge de los dispositivos Edge y del IoT está ofreciendo a los ciberdelincuentes nuevos puntos de entrada en los sistemas.
- La IA está ayudando a los ciberdelincuentes a automatizar los ataques, mejorar el phishing y crear deepfakes más convincentes.

Preocupación por el riesgo cibernético a lo largo del tiempo



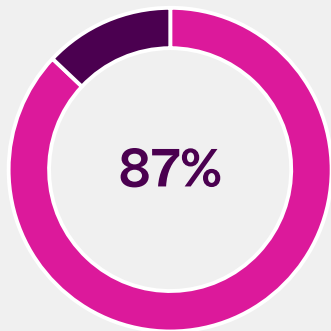
Porcentaje de directivos españoles que clasificaron el ciberriesgo (fallo de la empresa a la hora de garantizar la privacidad de los datos o amenaza delictiva externa, incluido el ransomware, o amenaza sistémica más amplia que genere una interrupción grave del negocio) como su principal riesgo cibernético y tecnológico a lo largo del tiempo. Las cifras de 2026 son una predicción del principal riesgo dentro de 12 meses.

Transformación tecnológica: del código a la comprensión

La IA obliga a las empresas a equilibrar sus beneficios con la necesidad de contar con sólidas salvaguardias contra los riesgos emergentes.

Riesgo y recompensa

- Aumenta el optimismo sobre la IA. Hoy en día, el riesgo de invertir poco en IA es mayor que el de invertir demasiado.
- La supervisión humana es esencial para mitigar riesgos como la infracción de los derechos de autor, la violación de la propiedad intelectual, los sesgos o la difamación.

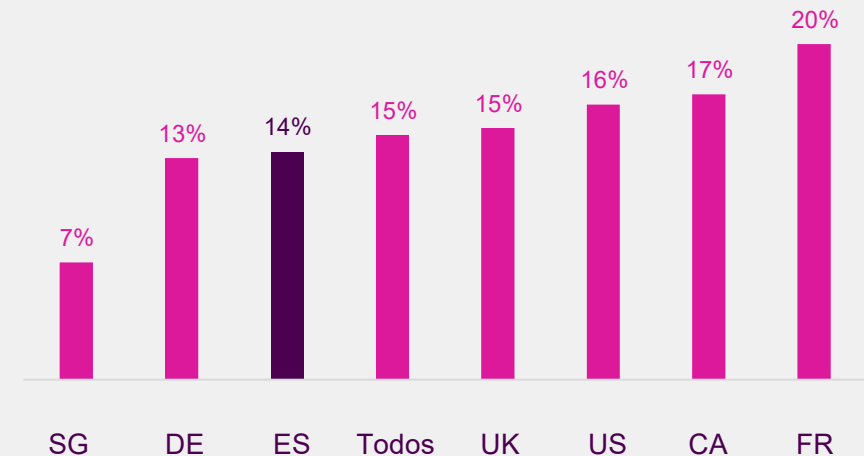


de los ejecutivos con sede en España coincidieron en que la IA tendrá un impacto positivo en las perspectivas económicas de sus empresas este año.

Tecnología obsoleta

- La IA suscita preocupación por la obsolescencia de la tecnología, la disrupción tecnológica y la pérdida de competitividad.

La preparación para la obsolescencia tecnológica varía según la región



El porcentaje de ejecutivos que no se siente preparado (respuestas "no muy bien" y "nada preparados" combinadas) para anticipar y responder al riesgo de obsolescencia tecnológica -la incapacidad de seguir el ritmo de los cambios en el desarrollo tecnológico y las oportunidades (por ejemplo, IA Generativa, IoT y automatización); incapacidad de actualizar los sistemas-. como su principal riesgo cibernético y tecnológico por región.

Protegidos o expuestos – Propiedad Intelectual y privacidad de los datos

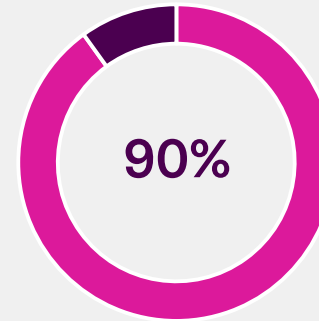
Proteger los datos y garantizar la seguridad de la propiedad intelectual es cada vez más importante.

Riesgos a la vuelta de la esquina

- Las normas en torno a la IA y los derechos de autor siguen sin estar claras, y el riesgo de robo de la propiedad intelectual existente es significativo.

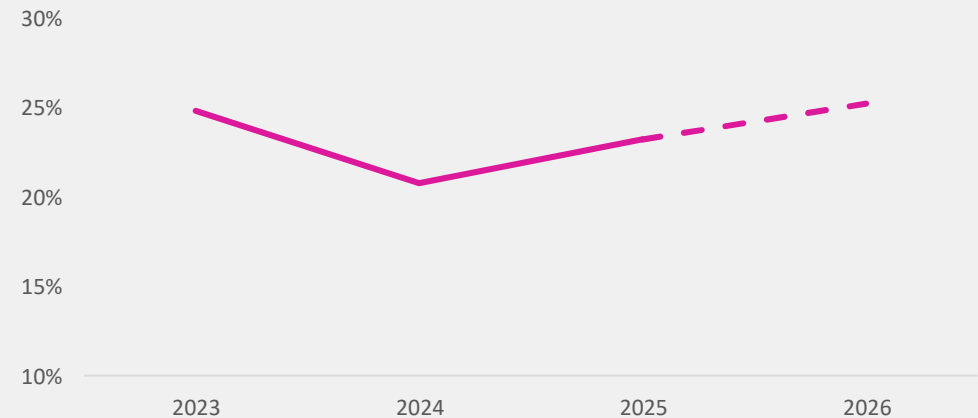
Laberinto normativo

- Las nuevas regulaciones nacionales para contrarrestar los riesgos en torno a la privacidad de los datos y la propiedad intelectual están creando una complejidad adicional para las empresas internacionales.
- A medida que perduran las tensiones geopolíticas, las organizaciones corren el riesgo de sufrir robos de propiedad intelectual y fuga de datos por parte de gobiernos hostiles.



de los ejecutivos con sede en España tiene un punto ciego en torno al riesgo de propiedad intelectual, con una percepción de preparación superior al 79% en 2024, a pesar de que la preocupación va en aumento.

Aumenta la preocupación por el riesgo de propiedad intelectual en España en 2025



Porcentaje de directivos españoles que considera el riesgo de propiedad intelectual -la incapacidad de reconocer y proteger el valor de los activos de propiedad intelectual, como el know-how, las patentes o los activos intangibles- como su principal riesgo cibernético y tecnológico a lo largo del tiempo. Las cifras de 2026 son una predicción de su principal preocupación de riesgo a 12 meses vista.

Construyendo resiliencia

Las estrategias de ciberseguridad nunca ha sido tan importantes como ahora.

Murallas dentro de murallas

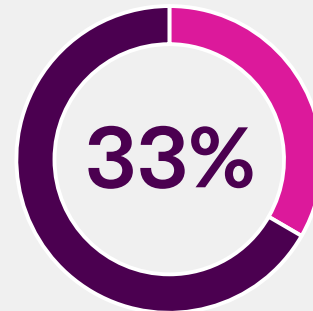
- Garantizar múltiples líneas o capas de defensa a modo de murallas para restringir el acceso a sistemas y datos es fundamental.
- Las organizaciones necesitan una estrategia de defensa en profundidad y a medida, que refleje su cadena de suministro y su perfil de riesgo únicos.

Amenaza de terceros

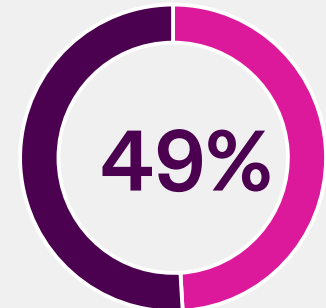
- Los contratos con los proveedores pueden limitar la responsabilidad, dejando que las empresas asuman las consecuencias legales y financieras de los ataques e interrupciones de terceros.

Mejorar las medidas preventivas

- Una buena estrategia de ciberseguridad incluye un enfoque preventivo, reactivo y adaptativo frente a la mitigación de los ciberriesgos.
- La inversión en ciberseguridad puede ayudar a que un incidente sea menos probable, ya que la mayoría de los ciberdelincuentes buscan el camino de menor resistencia.



de los ejecutivos españoles
tiene previsto explorar opciones
de seguros este año, incluida la
gestión de riesgos y crisis.

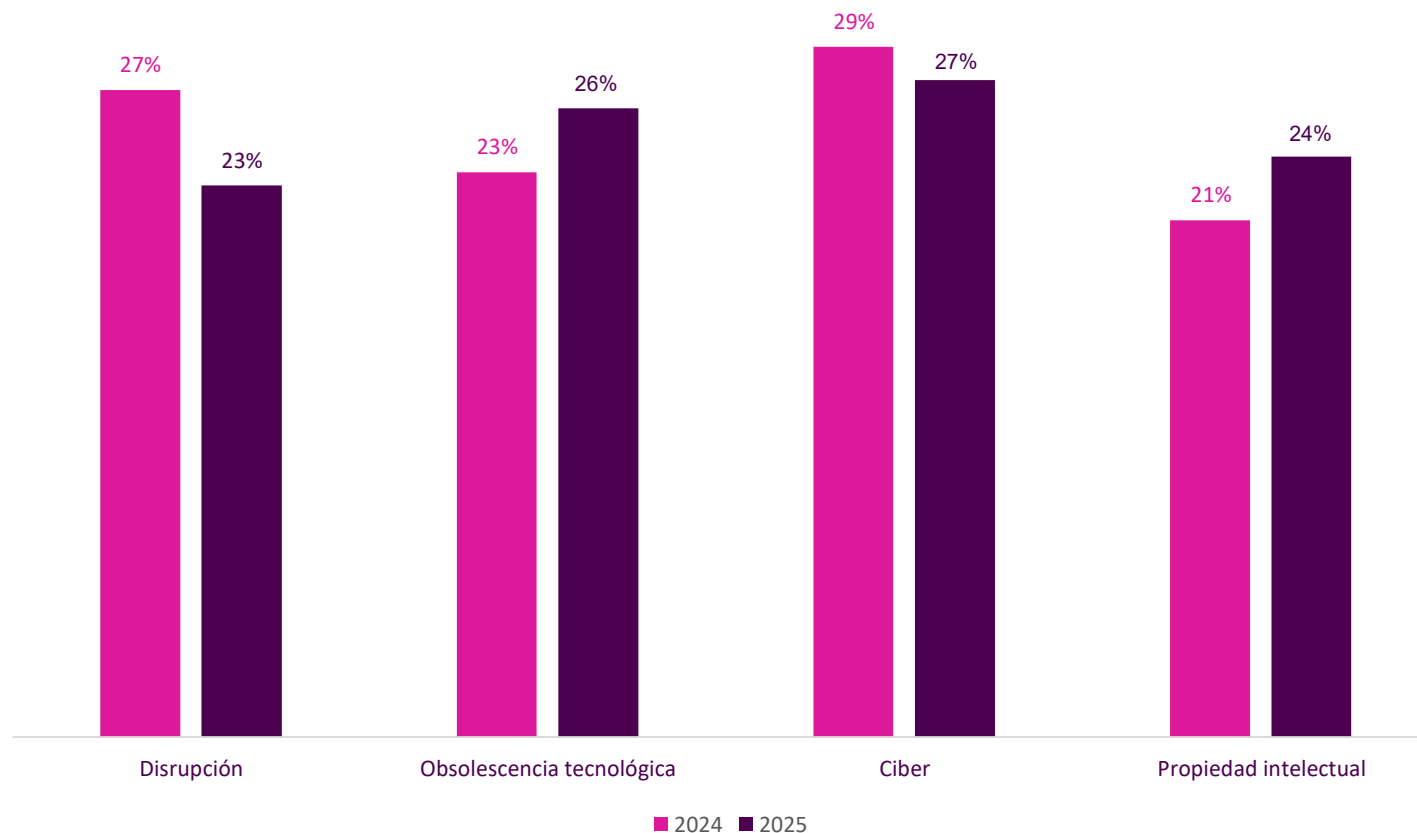


de los directivos españoles
afirma que su confianza en
el valor de los seguros
ha aumentado.

Los datos al detalle

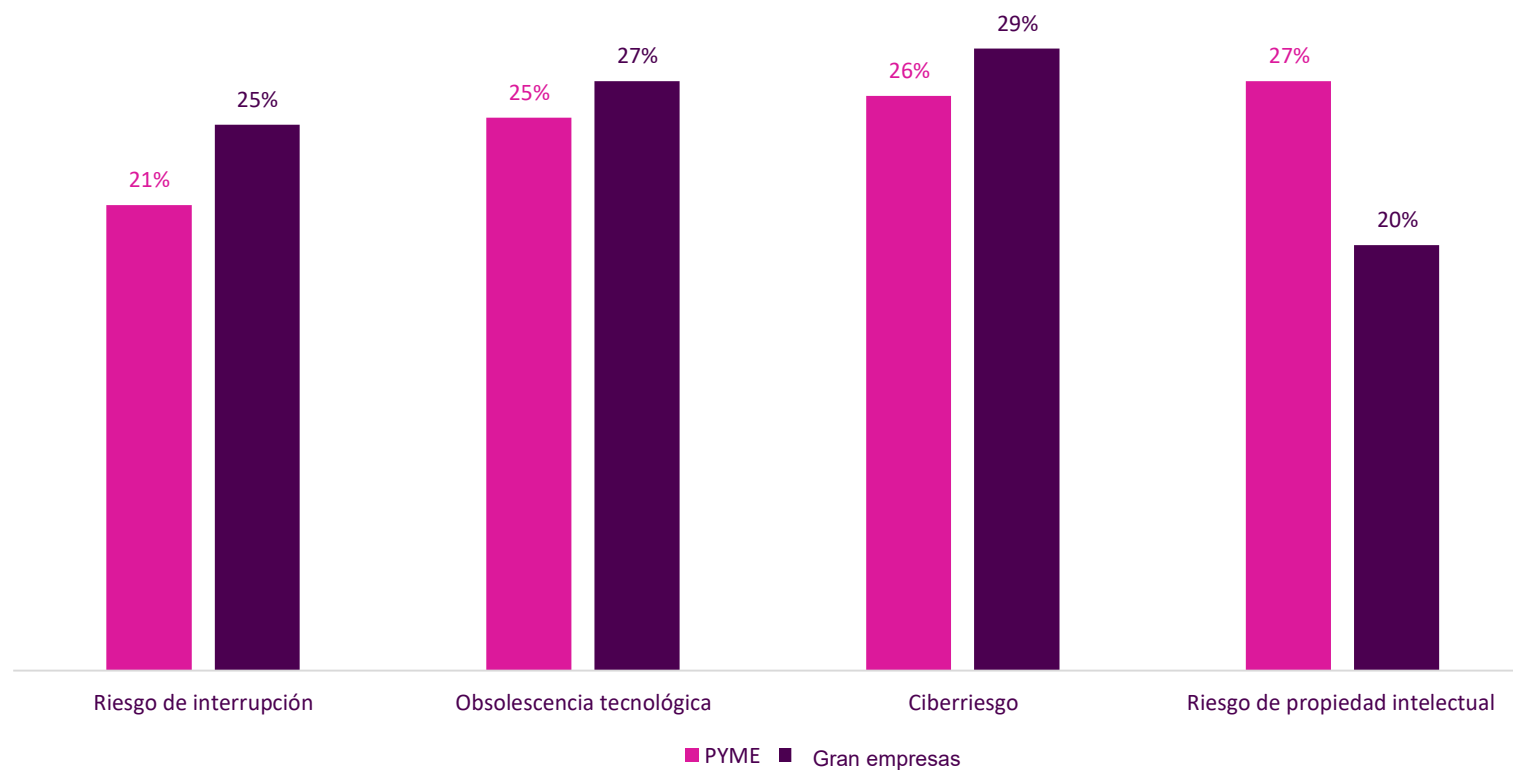


Clasificación del riesgo cibernético y tecnológico en España

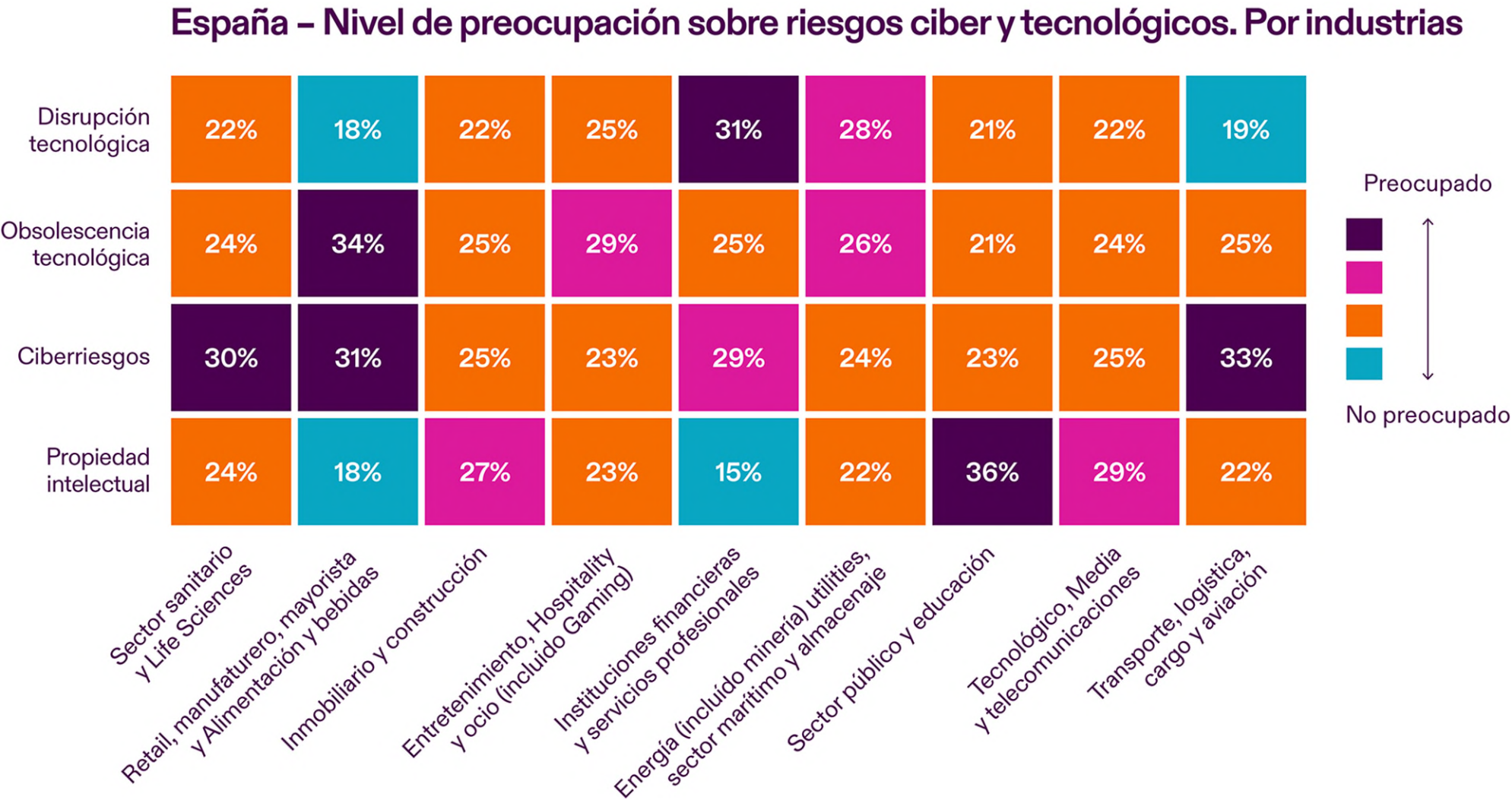


Riesgos cibernéticos y tecnológicos

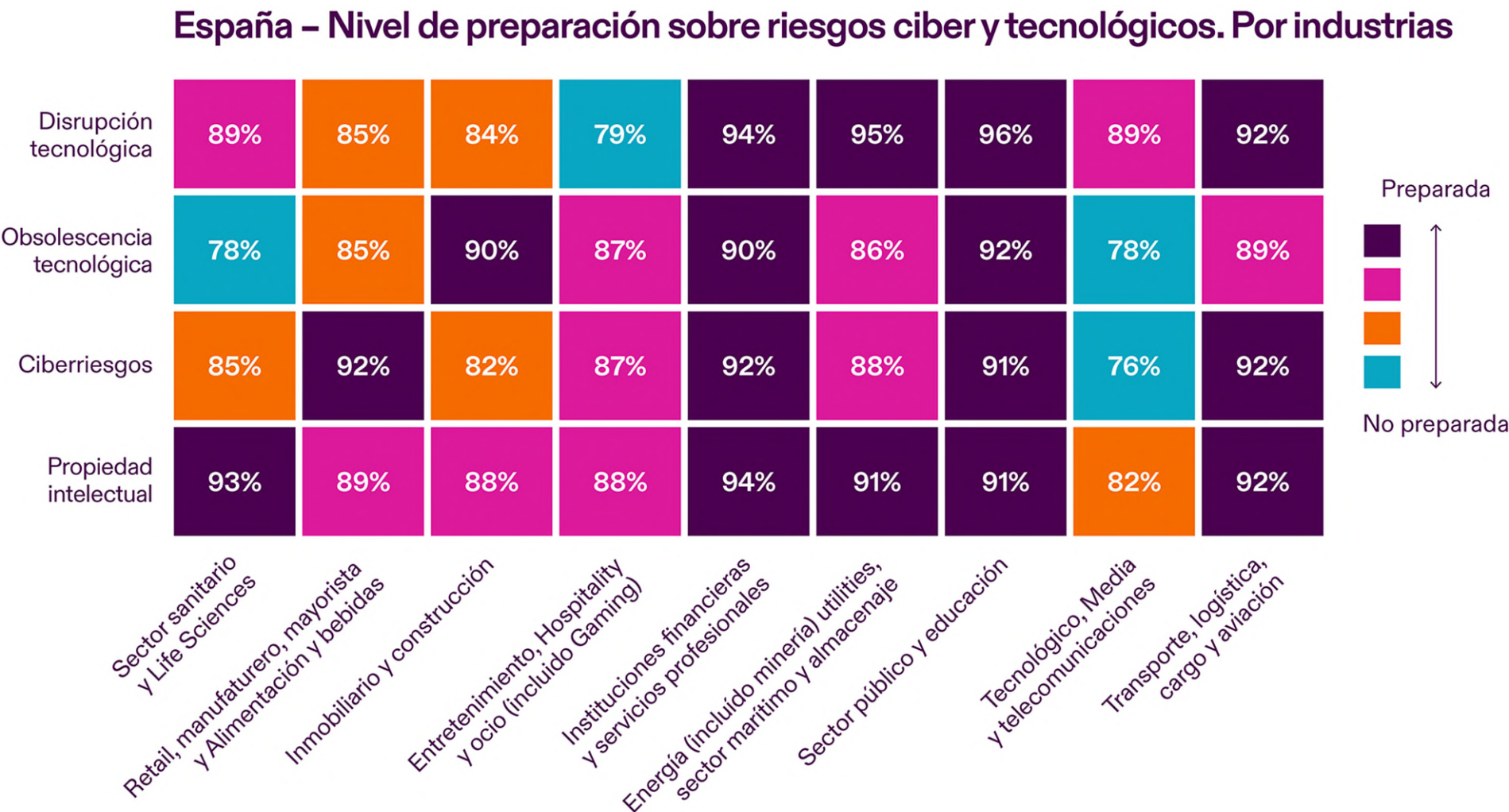
Pequeñas y medianas empresas con sede en España frente al riesgo de las gran empresas 2025



Mapa de riesgos por sectores



Mapa de resiliencia por sectores





Beazley plc (BEZ.L) es la sociedad matriz de empresas de seguros especializadas con operaciones en Europa, Estados Unidos, Canadá, América Latina y Asia. Beazley gestiona siete sindicatos de Lloyd's y, en 2024, suscribió un total de 6.104 millones de dólares en primas brutas mundialmente. Todos los sindicatos de Lloyd's están calificados A por A.M. Best.

Los suscriptores de Beazley en Estados Unidos se centran en suscribir productos de seguros especializados. La aseguradora europea de Beazley, Beazley Insurance dac, está regulada por el Banco Central de Irlanda y tiene calificación A de A.M. Best y A+ por Fitch.

Beazley es líder del mercado en muchas de sus líneas elegidas, entre las que se incluyen los seguros profesionales, responsabilidad civil, ciberriesgos, daños materiales, marítimo, reaseguro, accidentes y vida, riesgos políticos y contingencia.

Para más información, visite: beazley.com

La información contenida en este documento tiene por objeto la gestión general de riesgos. Se pone a su disposición con el entendimiento de que Beazley no presta servicios o asesoramiento jurídicos. No debe interpretarse ni utilizarse como asesoramiento jurídico; y no pretende sustituir la consulta con un abogado. Aunque razonablemente se ha tenido cuidado en la preparación de la información expuesta en este documento, Beazley no se responsabiliza de los errores que pueda contener ni de las pérdidas supuestamente sufridas atribuibles a esta información.

