¿Puede la complejidad ser un riesgo para la ciberseguridad de una empresa?

EY 2023 Global Cybersecurity Leadership Insights Study

Resumen en español

EY INSIGHTS

Contenidos

Introducción

Mientras el número de ciberamenazas y los costes asociados aumentan, los responsables de ciberseguridad de las empresas parecen tener problemas con la eficacia de la seguridad de sus entornos digitales, según el estudio *EY 2023 Global Cybersecurity Leadership Insights*.

La encuesta realizada a **500 responsables de ciberseguridad de todo el mundo**, entre los que se encuentra una muestra de empresas españolas, revela que sólo uno de cada cinco considera que el enfoque de su organización es eficaz frente a las amenazas actuales y futuras. La mitad de los encuestados también se muestran escépticos sobre la eficacia de la formación que imparten a sus trabajadores y sólo el 36% está satisfecho con los niveles de adopción de las mejores prácticas por parte de sus empleados.

En 2022, las empresas consultadas recibieron una **media de 44 incidentes relacionados con su ciberseguridad**. Al mismo tiempo, los encuestados revelan un aumento de los costes asociados a la inversión en ciberseguridad: el coste medio anual se sitúa en 35 millones de dólares, mientras que el coste medio de una brecha de seguridad para las organizaciones ha aumentado un 12% hasta los 2,5 millones de dólares en 2023.

A pesar de los altos niveles de gasto, los tiempos de detección y respuesta siguen siendo lentos. Más de tres cuartas partes de los encuestados (76%) afirman que sus organizaciones tardan una media de seis meses o más en detectar y responder a un incidente.

Principales resultados

Las organizaciones se enfrentan a un entorno muy cambiante a la hora de gestionar las ciberamenazas de hoy y de prevenir las del futuro.

Al preguntar a los CISO y otros directores ejecutivos, sólo uno de cada cinco considera que su ciberseguridad es eficaz en la actualidad y está bien posicionada de cara a las amenazas del futuro.

Las organizaciones sufren ataques constantes y su respuesta no está a la altura:

~75%
De incremento de los ciberataques en los últimos 5 años*

44
Incidentes de media en el último año

76%
De las empresas tarda 6 meses o más en detectar y actuar frente a un problema

*Universidad de Maryland - CISSM Cyber Attacks Database

Para identificar las empresas con mejores prácticas de ciberseguridad, hemos evaluado las organizaciones en función de una serie de métricas de ciberseguridad. A partir de los resultados, hemos identificado dos tipos de organizaciones:

Empresas seguras
Aquellas con la ciberseguridad más desarrollada y eficiente (42% del total)

Empresas vulnerables
Las organizaciones con una ciberseguridad menos eficiente (58%)

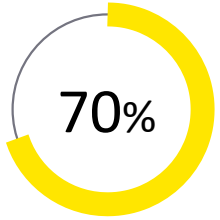
Empresas seguras		Empresas vulnerables
5 meses	Tiempo medio de detección y respuesta a un ciberataque	11 meses
32	Promedio de ciberataques en 2022	52
51%	% de satisfacción con su estrategia de ciberseguridad	36%
53%	% de acuerdo con que su organización está preparada para el futuro	41%

1 Incorporar tecnologías emergentes en la gestión de la ciberseguridad

Seguridad a través de la simplificación

La mayoría de las 'Empresas seguras' (70%) se consideran pioneros en la adopción de tecnologías emergentes en lugar de esperar a que la tecnología esté probada y comprobada, una cifra que desciende al 60% en las 'Empresas vulnerables'.

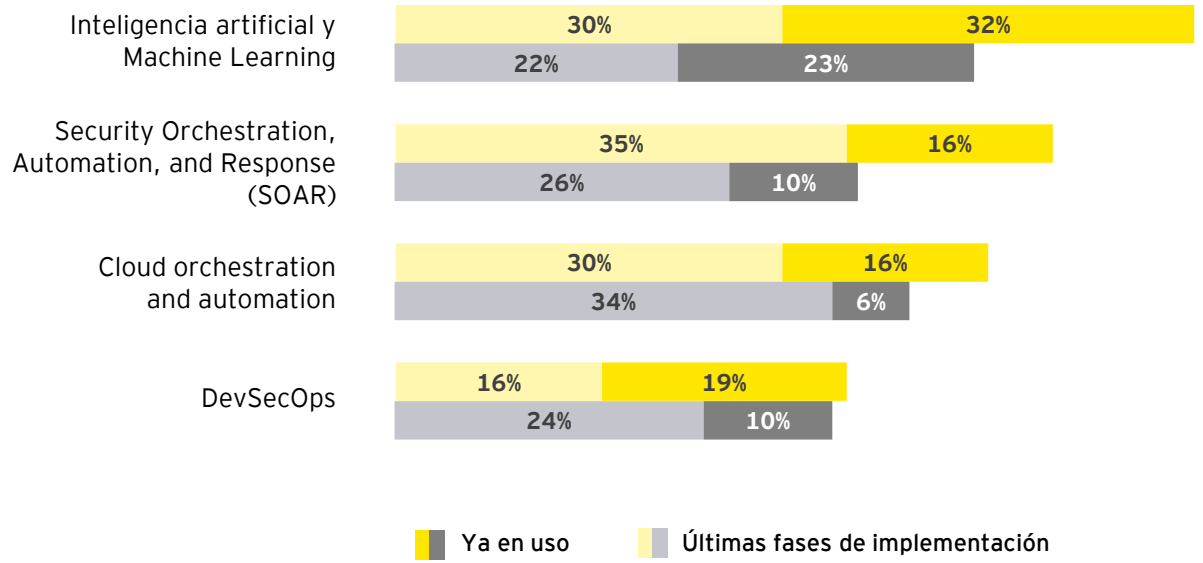
Las empresas más avanzadas utilizan soluciones para simplificar su entorno mediante la adopción de tecnologías centradas en la automatización y la simplificación, como IA o ML, SOAR, DevSecOps y orquestación y automatización de la nube.



Empresas seguras que se consideran pioneras en la adopción de tecnologías emergentes. En el caso de las en el caso de las vulnerables es del 60%.

Tecnologías emergentes de simplificación y automatización

Estado de implementación de tecnologías en Empresas seguras vs. Empresas vulnerables



2 Proteger toda la superficie de ataque

Acompañar con ciberseguridad la adopción de nuevas tecnologías

El incremento y adopción de nuevas tecnologías aumenta la superficie de ataque, lo cual supone un riesgo según la mayoría de los encuestados.

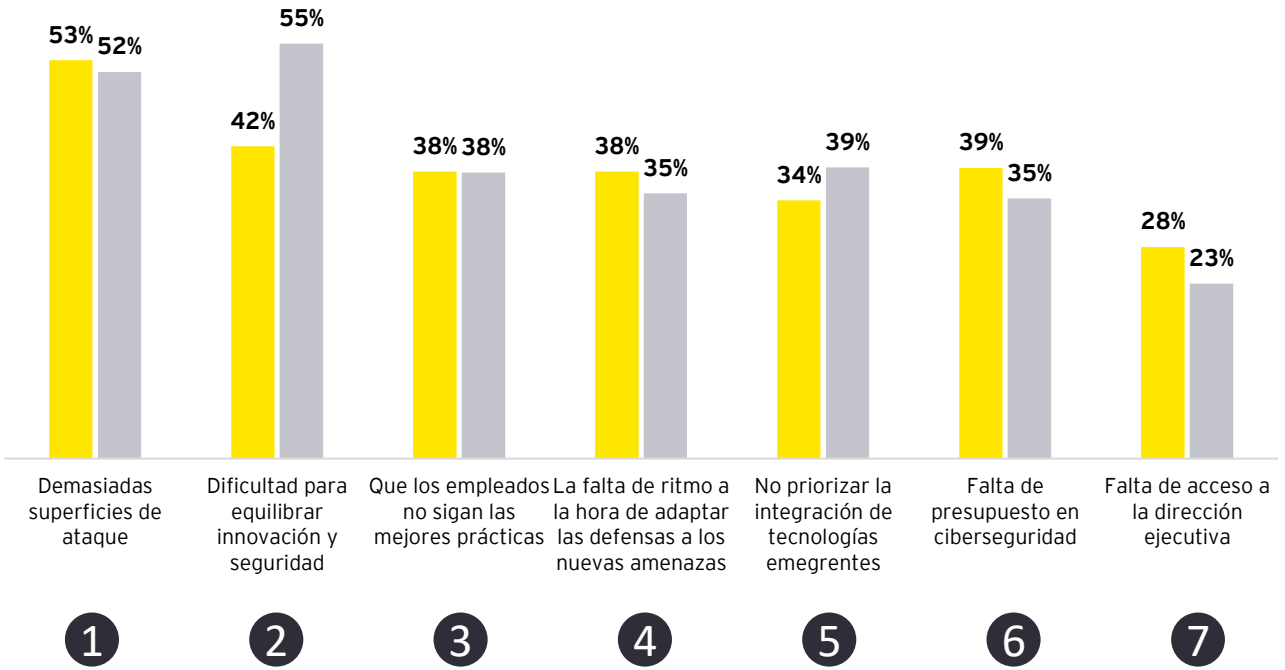
El **presupuesto**, que históricamente ha sido citado en la encuesta como el principal obstáculo, en esta ocasión de sitúa en el puesto 6 de 7 en la clasificación general, el mismo porcentaje que en la muestra española.

La dificultad para equilibrar el ritmo de la innovación y el de la seguridad se posiciona como el segundo desafío más nombrado, tanto en la media global como en la española, donde ocupa el primer lugar.

Esto se ve agravado por el riesgo que plantean la **implementación de la tecnología *cloud*** a gran escala y el Internet de las cosas: más de 7 de cada 10 consideran que son los dos principales riesgos tecnológicos en los próximos cinco años.

Principales desafíos internos para la ciberseguridad de las organizaciones

Percepción de las mayores situaciones de riesgo según las Empresas seguras vs. Empresas vulnerables



Protección de toda la superficie de ataque

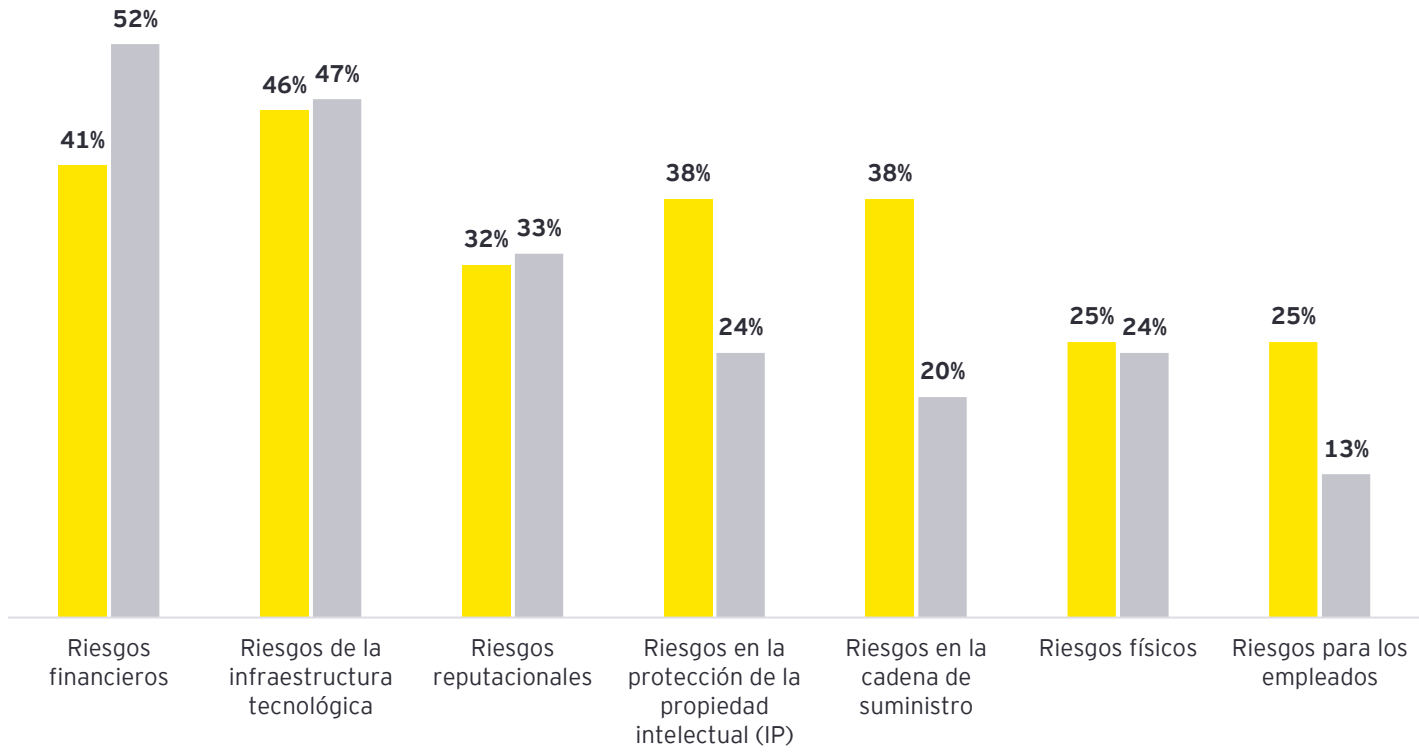
Todas las organizaciones están vinculadas operacional y digitalmente a las empresas que participan en su **cadena de suministro**. Sin embargo, a pesar del peligro, son pocos los que declaran estar muy preocupados por los ciberriesgos de la cadena de suministro y existe una brecha entre la percepción de las Empresas seguras y las vulnerables en este sentido (38% frente al 20% de las Empresas Vulnerables).

Tanto las Empresas seguras como Empresas vulnerables tienen su máxima preocupación en los **riesgos financieros**, los relacionados con la **infraestructura tecnológica** y los **reputacionales**.

Cabe señalar que las 'Empresas vulnerables' tienen una mayor inclinación por centrarse en los **riesgos financieros** que las 'Empresas seguras', registrando una diferencia considerable de 11 puntos porcentuales.

Preocupación por los riesgos relacionados con la ciberseguridad en las organizaciones

Proporción de quienes se muestran "muy preocupados" en las Empresas seguras vs. Empresas vulnerables



3 Hablar el mismo idioma que el resto de la empresa

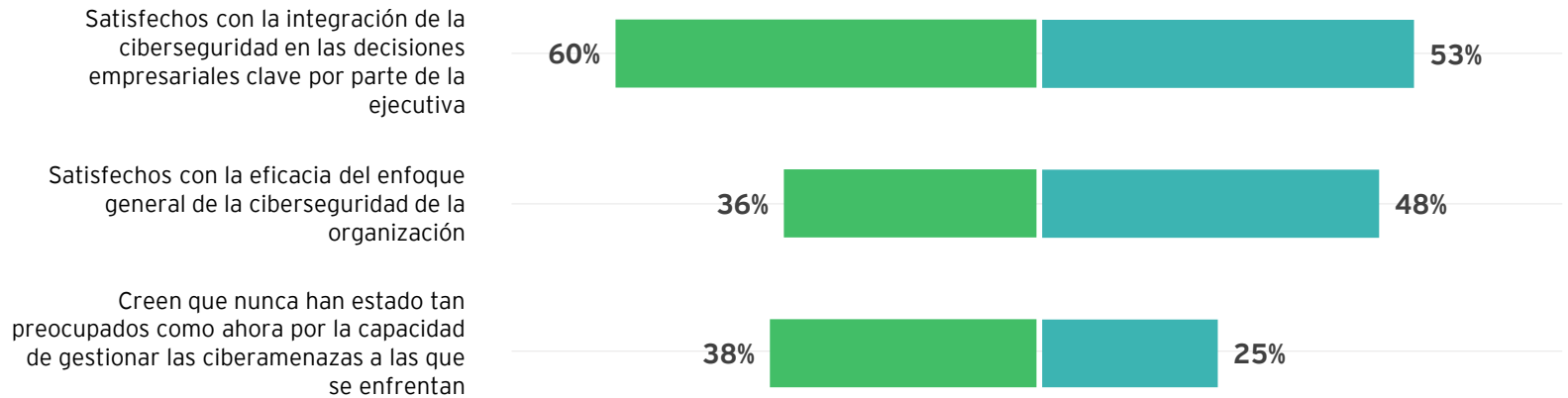
Aplicar la ciberseguridad en todos los niveles de la organización

Los resultados de la encuesta revelan que sigue habiendo una **desconexión entre los CISO y el resto de la dirección ejecutiva** (C-suite). Los CISO están menos satisfechos con el enfoque de ciberseguridad de su organización (36% frente a 48%). Entre las 'Empresas vulnerables', esta brecha es aún más pronunciada.

Cerrar estas brechas es clave: las organizaciones que tienen las operaciones de ciberseguridad integradas en las prioridades y estrategias empresariales básicas tienen menos probabilidades de sufrir incidentes de seguridad.

Brechas entre los CISO y otros directores ejecutivos

Percepción de distintos supuestos en la ciberseguridad de la empresa de los CISO vs. otros directores ejecutivos



Hablar el mismo idioma que el resto de la empresa

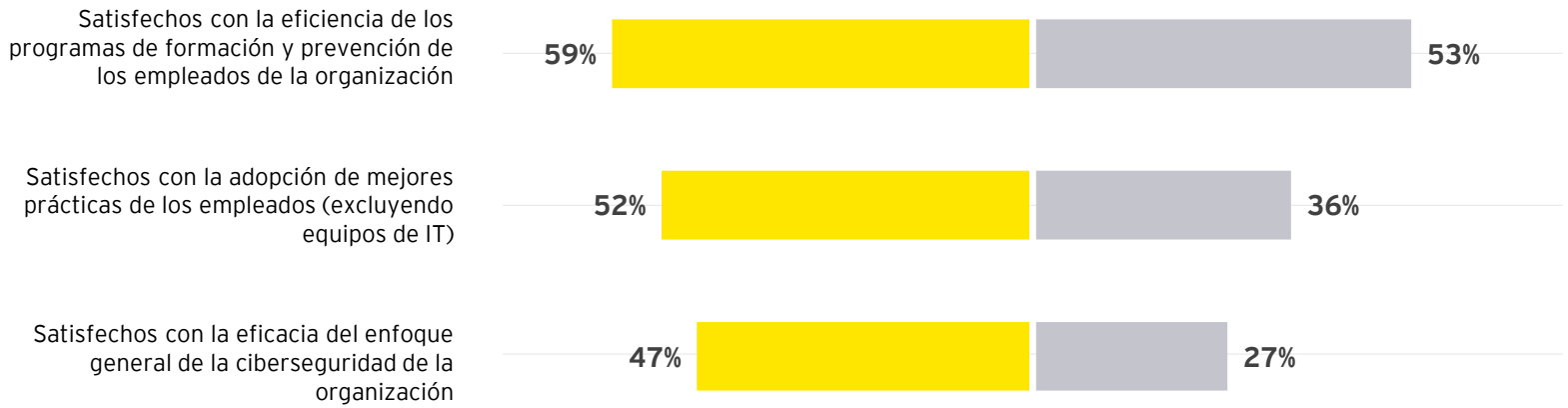
Casi 4 de cada 10 responsables de ciberseguridad señalan en la encuesta la **falta de cumplimento** de las mejores prácticas de ciberseguridad entre el personal no informático como uno de los mayores retos internos .

Entre las Empresas seguras, sólo la mitad están satisfechos con la **eficacia de sus programas de formación** en materia de ciberseguridad (52%), mientras que entre las Empresas vulnerables sólo el 36%.

El 47% de las 'Empresas seguras' están satisfechas con el cumplimiento de las mejores prácticas por parte de sus plantillas frente al 27% de las 'Empresas vulnerables'.

Diferencias en el papel de los empleados

Diferencia de satisfacción con distintas situaciones en la ciberseguridad de la empresa entre las Empresas seguras vs. las Empresas vulnerables



4 Transformar la ciberseguridad en un creador de valor

La ciberseguridad bien planteada contribuye a la generación de valor

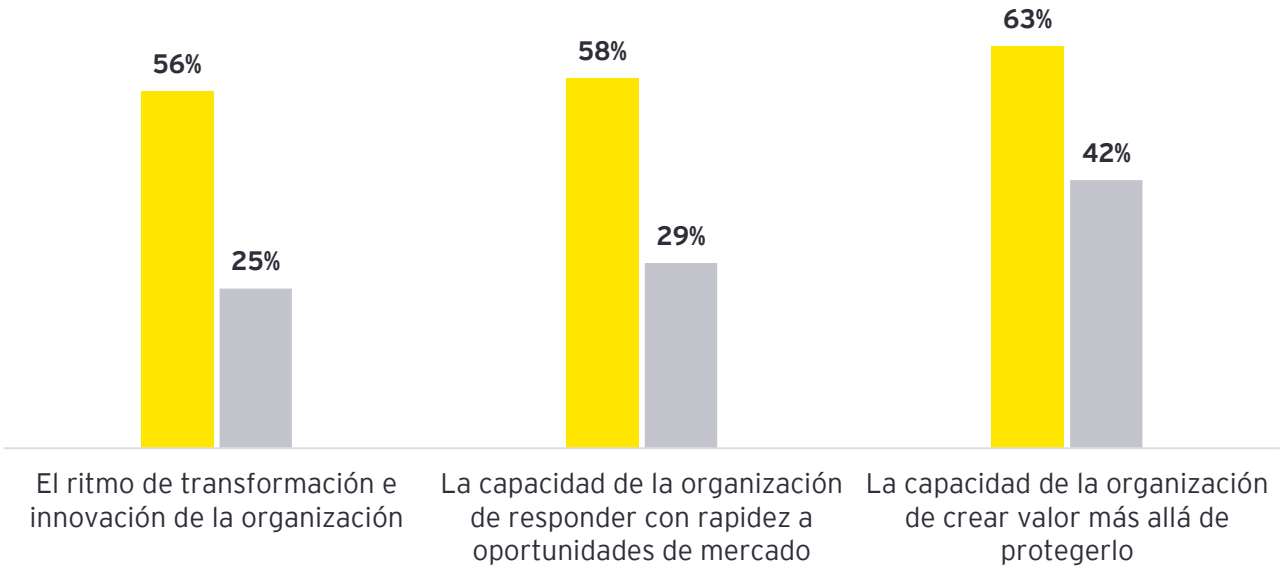
Las 'Empresas seguras' trabajan para crear valor, no sólo para defenderlo. Su estrategia de ciberseguridad busca tener una repercusión positiva en su capacidad para transformarse a un ritmo adecuado, responder a las oportunidades del mercado y centrarse en la creación de valor.

La creación de valor puede adoptar muchas formas, entre ellas:

- Alcanzar una mayor confianza por parte de clientes y proveedores, que se sentirán más seguros al realizar transacciones con ellos.
- Aprovechar plenamente las ventajas de los ecosistemas de colaboración y asociaciones sin incurrir en riesgos.

Percepción de creación de valor a partir de la ciberseguridad

Impacto positivo de la estrategia de ciber seguridad en la creación de valor de las Empresas seguras vs. Empresas vulnerables



Acciones para crear una ciberestrategia centrada en el valor

Los responsables de ciberseguridad se enfrentan a las amenazas actuales y a futuro. De hecho, las organizaciones experimentan resultados muy diferentes en función de su estrategia. Las empresas pueden reforzar su ciberseguridad haciendo hincapié en la simplicidad, el pensamiento transversal y la integración de las consideraciones relacionadas con la ciberseguridad en toda la organización. Los puntos de acción clave que se desprenden tras consultar a los responsables de ciberseguridad de empresas de todo el mundo son los siguientes:

01

Simplificar el conjunto de tecnologías en uso para **reducir el riesgo y mejorar la detección**.

La automatización y orquestación sirven para facilitar la organización del entorno tecnológico, lo que permite detectar señales más rápidamente y responder con mayor eficacia.

02

La homogeneización y la automatización dentro de las **cadenas de suministro** pueden mejorar el seguimiento y la supervisión continua del rendimiento sin añadir una burocracia excesiva.

Los equipos de seguridad deben participar desde el principio en la **selección de proveedores.**

03

Los CISO más eficaces utilizan un **lenguaje que pueda comprender y asimilar toda la empresa.**

Por ejemplo, pueden trasladar información en términos de reducción de riesgos, impacto empresarial y creación de valor.

04

El error humano sigue siendo una de las principales causas de las vulneraciones de la ciberseguridad.

Las organizaciones más avanzadas **combinan la formación constante y adaptada con la automatización** y las herramientas de prevención para que sus empleados apliquen las medidas de ciberseguridad en todos sus ámbitos de trabajo.

05

La ciberseguridad debe integrarse en el tejido de la organización, no considerarse un limitador.

Una estrategia de ciberseguridad adecuada tiene la capacidad de impulsar el valor, infundir la confianza necesaria para innovar y abrir nuevas oportunidades de ingresos y de mercado.

EY | Building a better working world

En EY trabajamos para construir un mundo que funcione mejor, ayudando a crear valor a largo plazo para los clientes, las personas, la sociedad y generar confianza en los mercados de capital.

Gracias al conocimiento y la tecnología, los equipos de EY, en más de 150 países, generan confianza y ayudan a las compañías a crecer, transformarse y operar.

EY es líder mundial en servicios de auditoría, fiscalidad, estrategia, asesoramiento en transacciones y servicios de consultoría. Nuestros profesionales hacen las mejores preguntas para encontrar nuevas respuestas a los desafíos a los que nos enfrentamos en el entorno actual.

ey.com/es_es

EY INSIGHTS

Área de estudios responsable de la generación y difusión de contenidos de EY España

EY Insights tiene como objetivo generar y compartir conocimiento útil para el conjunto de la sociedad. A partir de un enfoque basado en la generación de valor a largo plazo, nuestra meta es impulsar la participación de EY en debates relevantes para la sociedad, generar puntos de encuentro y divulgar contenidos que ayuden a empresas, administraciones y ciudadanos a afrontar los desafíos del presente y del futuro.

Más información

eyinsights.spain@es.ey.com