Instituto de Auditores Internos de España

RiesgosClave

esfera consejeros

Risk in Focus 2024

VISIÓN DEL AUDITOR INTERNO

Ciberseguridad y talento, máximos riesgos

ÍNDICE

Sobre Esfera Consejeros: ..... 2 Pág.

De un vistazo: ..... 3 Pág.

Ciberseguridad y talento lideran el mapa de riesgos: ..... 4 Pág.

1. Incertidumbre macroeconómica y geopolítica 11 Pág.
2. Riesgo de terceros 15 Pág.
3. Talento: gestión y diversidad 18 Pág.
4. Riesgo climático, biodiversidad y sostenibilidad 21 Pág.
5. Ciberseguridad y protección de datos 24 Pág.

Referencias ..... 27 Pág.

Descarga el informe ..... 29 Pág.

Sobre Esfera Consejeros

Esfera Consejeros es una iniciativa dirigida a los consejeros miembros de la **Comisión de Auditoría**.

Es un servicio de análisis, síntesis y conocimiento. Siempre desde la perspectiva de **rigor, calidad** e **independencia** del Auditor Interno.

Nuestro objetivo es aportar el **conocimiento** y la **visión transversal** propia de los auditores internos y contribuir a que los consejeros puedan supervisar la compleja realidad empresarial y su entramado de riesgos.

El servicio se nutre de diferentes publicaciones, **RiesgosClave, EnFoco y EnRuta**, que abordarán con distinta profundidad y enfoque temas relevantes en la vida empresarial.

Un valor diferencial es **la mirada del Auditor Interno** respecto el tema analizado: ¿Cuáles son las preguntas clave que hay que hacerse? ¿Qué inquieta al Auditor Interno y dónde y cómo actúa para proporcionar aseguramiento y confort? Cuestiones todas ellas relevantes para la Comisión de Auditoría en sus labores de supervisión y control.

Confiamos en que **Esfera Consejeros** le sea de utilidad.

Septiembre 2023

- Si eres consejero de una empresa socia del Instituto y quieres darte de alta en Esfera Consejeros, solicítalo aquí.
- Si tienes dudas, escríbenos a esferaconsejeros@iai.es

De un vistazo

Policrisis, el gran riesgo empresarial. Lo decía el *World Economic Forum* en su último informe Global Risks Report y lo corrobora el estudio **Risk in Focus 2024**, que ofrece una panorámica europea sobre los principales riesgos empresariales desde la mirada del Auditor Interno. Los riesgos y las crisis se superponen y entrelazan conformando un escenario complejo de transitar. Presionadas por las difíciles condiciones económicas (desaceleración, tipos de interés altos, inflación…) y la volatilidad geopolítica, las organizaciones necesitan un enfoque inquebrantable en resiliencia y crecimiento para navegar en la policrisis y recuperarse rápidamente cuando la situación mejore. Ciberseguridad, talento y riesgo climático se perfilan como los tres riesgos permanentes de la policrisis. Los dos primeros lideran el ranking de riesgos para 2024 y los tres copan el top3 de las previsiones a tres años.

Riesgo de policrisis

Ciberseguridad y talento lideran el mapa de riesgos

Las empresas están sometidas a enorme presión con riesgos cada vez más complejos, entrelazados y de rápida transmisión global. Viven en modo crisis permanente que les obliga a una vigilancia constante y minuciosa. Ciberseguridad y la gestión de un talento escaso y difícil de retener se consolidan en en el top de riesgos.

La incertidumbre macroeconómica y geopolítica sigue dominando y condicionando el panorama empresarial que, una vez más, ve en la ciberseguridad un riesgo permanente a la vista de los crecientes -en número y complejidad- ciberataques.

Las dudas sobre el grado de desaceleración económica que va a generar la pronunciada y rápida subida de los tipos de interés por parte de los bancos centrales en prácticamente todo el mundo explican que el riesgo macroeconómico y geopolítico comparta con cambio regulatorio y compliance la tercera posición este año en el **Risk in Focus 2024**.

Risk in Focus: metodología

El informe *Risk in Focus*, que este año va por su octava edición, ha sido realizado por 16 Institutos de la Confederación Europea de Institutos de Auditores Internos (ECIIA): España, Austria, Bélgica, Bulgaria, Francia, Alemania, Grecia, Hungría, Italia, Luxemburgo, Países Bajos, Noruega, Polonia, Suecia, Suiza y Reino Unido & Irlanda. En la encuesta participaron 799 Directores de Auditoría Interna (DAIs) de compañías europeas de todos los sectores. Se llevaron a cabo 11 entrevistas en profundidad y 5 mesas redondas con un total de 46 participantes. El valor del informe radica en su visión desde Auditoría Interna, además de la perspectiva europea.

Las dificultades para atraer, retener y gestionar el talento siguen inquietando a las organizaciones: este riesgo se consolida en la segunda posición, puesto que también ocupa en las previsiones a tres años vista. En tercer lugar comparte puesto otro riesgo clásico: la carga regulatoria y el riesgo de compliance que lleva consigo tanta nueva normativa en múltiples frentes, especialmente en todas las cuestiones de sostenibilidad y criterios ESG.

Un riesgo que este año avanza dos puestos, de la séptima a la quinta posición, es el riesgo de continuidad de negocio, respuesta a crisis y resiliencia operativa. El motivo no es otro que la permanente agitación del entorno global. Recordemos que este riesgo estaba también en los puestos quinto y sexto los años anteriores y llegó a colocarse en la segunda posición en 2020, el año del estallido de la pandemia.

El análisis de los cinco principales riesgos a los que el departamento de Auditoría Interna dedica actualmente más tiempo y esfuerzo muestra esta priorización: ciberseguridad y protección de datos; gobierno corporativo y reporting; cambio regulatorio y compliance, continuidad de negocio y respuesta a crisis y, por último, en quinto lugar, riesgos financieros, liquidez e insolvencia. Cuando se les pregunta por los riesgos que prevén ser su prioridad a tres años vista, solo hay un cambio relevante: se cae de los cinco primeros puestos el riesgo financiero y entra con fuerza, en la cuarta posición, el riesgo climático.

Los cinco grandes bloques temáticos en los que se ha estructurado el informe Risk in Focus 2024 detallan estos desafíos y ofrecen consejos prácticos sobre cómo ayudar a las organizaciones a adaptarse.

Antes de entrar a fondo en cada uno de estos grandes bloques, resumimos algunos de sus aspectos más relevantes:

Incertidumbre macro y geopolítica

- Comparte el tercer puesto por las dudas sobre el crecimiento global, pero baja en las previsiones a tres años.
- Este riesgo es más intenso para las empresas europeas: China y EEUU lo viven de otra manera.
- Las organizaciones deben incorporar estrategias de crecimiento y resiliencia para afrontar con éxito el futuro.
- Hay que aprender a invertir de manera más inteligente tanto en innovación como en personas y clientes.
- Se implantan sistemas de control que son más ágiles, adaptables y que incorporan una monitorización en tiempo real.

Riesgo de terceros

- Se mantiene en el puesto octavo, pero podría dispararse si hay recesión económica.
- La desaceleración y el encarecimiento de la financiación puede aumentar las insolvencias.
- Las relaciones con los proveedores se han vuelto más complejas y pueden ser puerta de entrada de ciberataques.
- Conviene incorporar el impacto climático como variable del riesgo de terceros.
- Las empresas buscan alternativas e invierten en I+D para crear bienes y materiales de reemplazo.

El riesgo de talento se dispara

- Se consolida como segundo riesgo este año y repite posición en las previsiones a tres años.
- Con la salida de personal experimentado, se está creando un problema en los mandos intermedios, un segmento clave.
- Hay que revitalizar la cultura corporativa y las estrategias de capital humano.
- Se requiere un cambio cultural que no todas las empresas podrán abordar.
- Las empresas se enfrentan a un alza de los costes laborales en un momento de cambio de hábitos de clientes.

Riesgo climático, biodiversidad y sostenibilidad

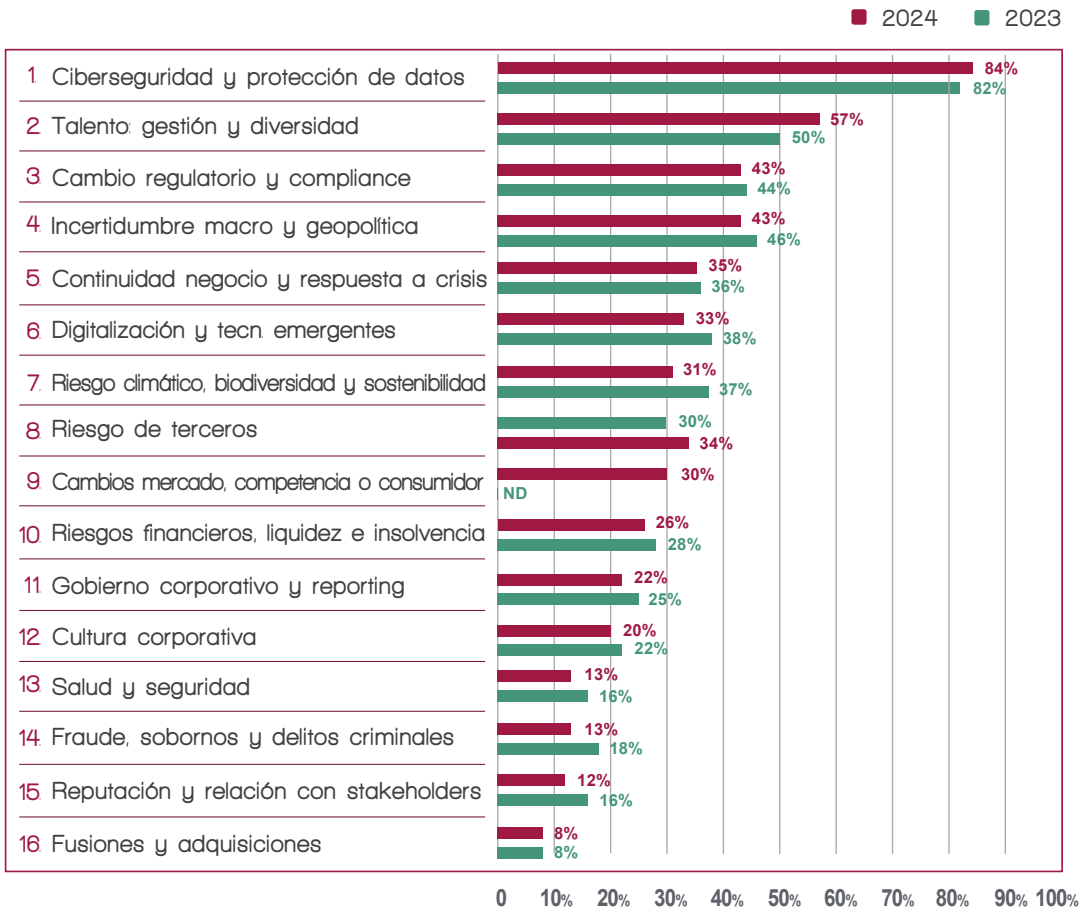
- Figura en el séptimo puesto, pero sube a la tercera posición en las previsiones a tres años.
- El riesgo climático va a absorber más atención y esfuerzo de 2024 en adelante.
- La carga regulatoria es muy elevada y va a requerir mucha labor de compliance.
- Cada empresa debe seleccionar sus objetivos sostenibles -la ONU promueve 17 ODS- y centrarse en los relevantes.
- La menor calidad de la información no financiera disponible quedará subsanada con las nuevas normativas y estándares.

Digitalización e Inteligencia Artificial

- Ciberseguridad se ha convertido en un riesgo permanente: lidera siempre el mapa de riesgos.
- La defensa cibernética está más madura ahora que antes de la pandemia, pero el mundo digital es más peligroso.
- La vigilancia constante y la innovación en el control de la ciberseguridad son imprescindibles.
- La Inteligencia Artificial puede ser el enemigo -en manos de los hackers- y el aliado que ayuda a detectar señales de alerta.
- Grandes avances en los sistemas de recuperación: es posible reconstruir desde cero con copias de seguridad dañadas.

Previsión de riesgos prioritarios actualmente

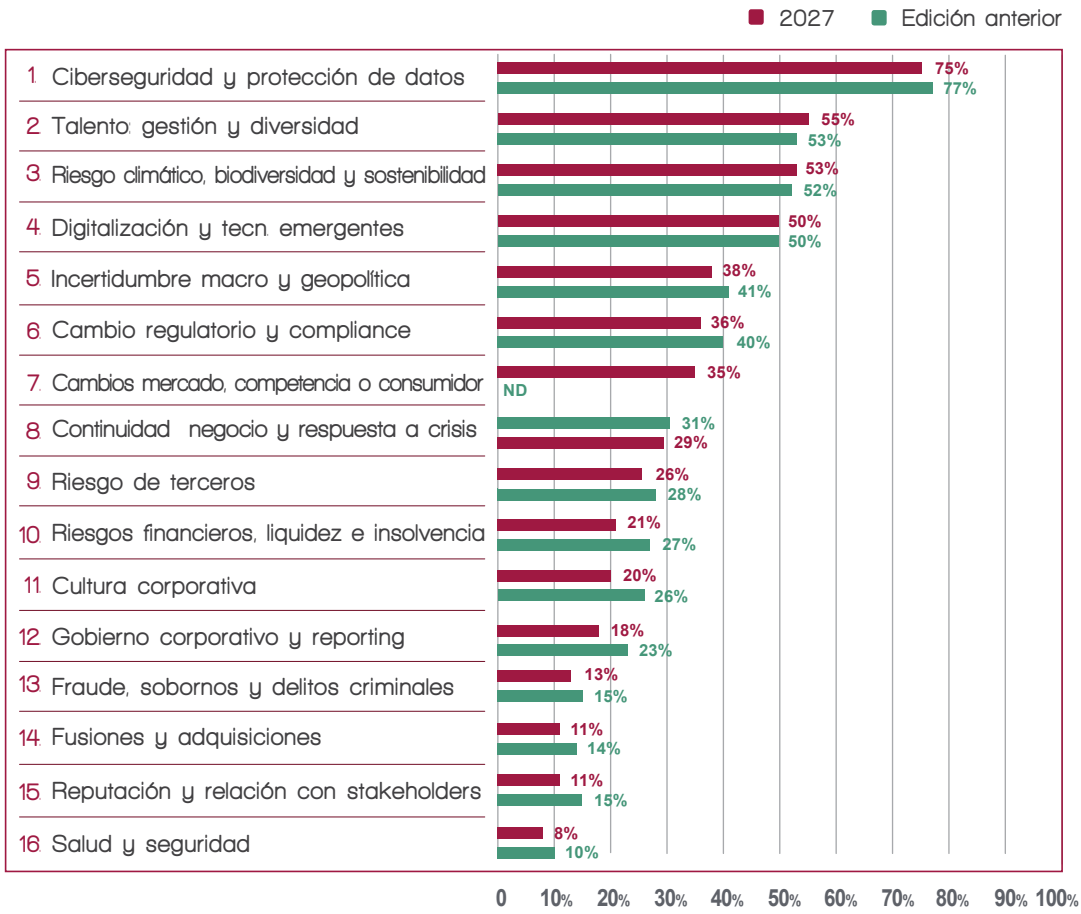
¿Cuáles son los 5 principales riesgos a los que se enfrenta tu empresa?



Fuente: *Risk in Focus 2024 y ediciones anteriores.*

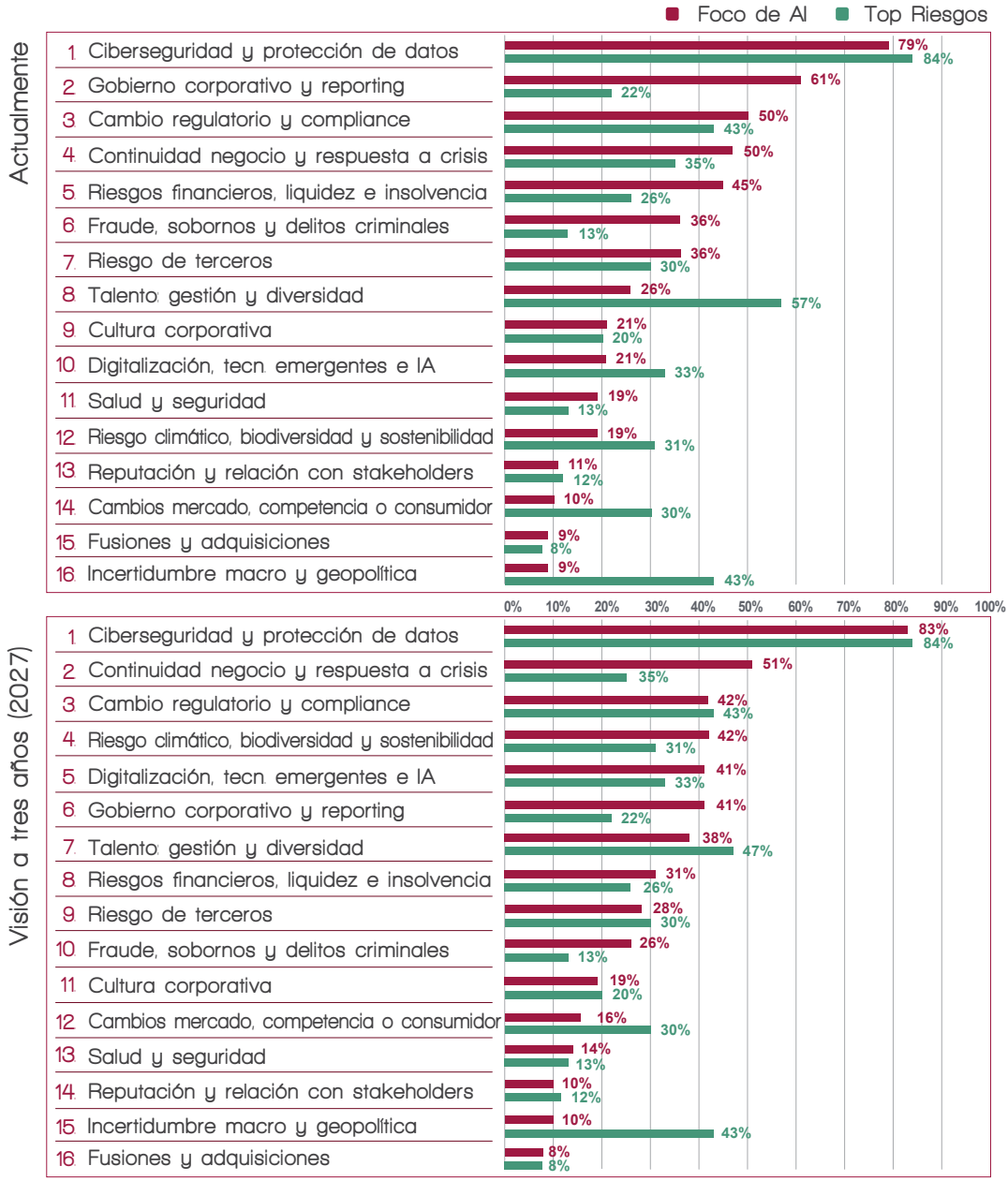
Previsión de riesgos prioritarios a tres años vista

¿Cuáles son los 5 principales riesgos a los que se enfrenta tu empresa en tres años?



Fuente: *Risk in Focus 2024 y ediciones anteriores.*

Riesgos a los que Auditoría Interna dedica más tiempo y esfuerzo



Fuente: *Risk in Focus 2024 y ediciones anteriores.*

Incertidumbre macroeconómica y geopolítica

Buscando crecimiento y resiliencia

El entorno es complejo y requiere de atención porque cualquier riesgo macroeconómico o geopolítico puede adquirir rápidamente dimensión global y afectar a toda la cadena de valor. Sucedió con la pandemia y la guerra de Ucrania. Y ahora, con la desaceleración.

Las organizaciones se enfocan en capear la tormenta económica, pero deben incorporar estrategias de crecimiento y resiliencia para afrontar con éxito el futuro.
El giro de la política monetaria mundial, con subidas pronunciadas de los tipos de interés después de dos décadas de laxitud, ha incrementado los costes financieros y aumentado el riesgo de insolvencia. A esto se han unido los colapsos financieros de Silicon Valley y Signature Bank, en EEUU, y de Credit Suisse, en Europa.

Aunque se espera que la inflación baje en 2024, también se prevé una desaceleración económica global más pronunciada, de ahí que el riesgo macroeconómico y geopolítico comparta con compliance la tercera posición del **Risk in Focus 2024.**

Cambios de mercado

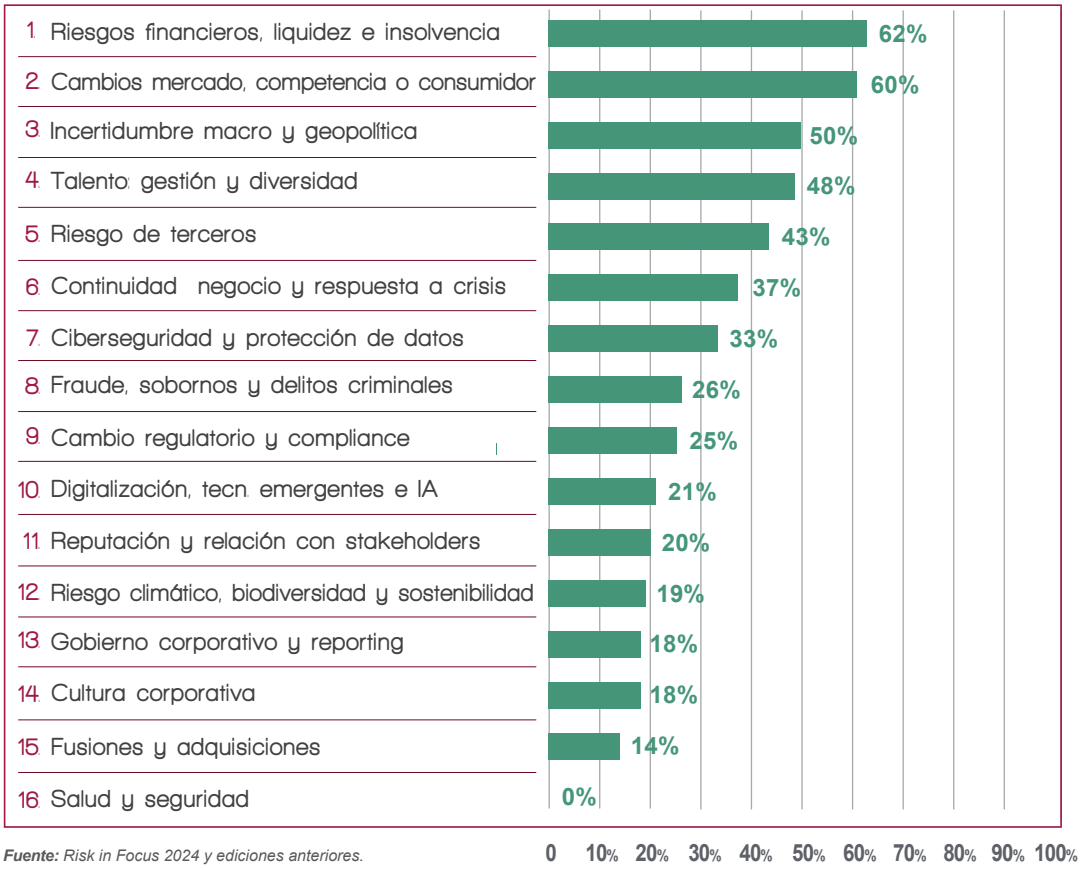
Ligado al riesgo del entorno aparece uno nuevo, cambios de mercado, competencia o cambios en los hábitos del consumidor que, aunque entra en el puesto noveno este año, salta al segundo lugar cuando se pregunta qué riesgos se verían más impulsados en caso de desaceleración o recesión económica. Los esfuerzos de resiliencia deben centrarse en capear esta amplia gama de presiones para garantizar que las empresas estén en condiciones de prosperar cuando mejore el entorno.

> *Es un riesgo importante para las empresas europeas porque las de EEUU y China no se enfrentan a la misma complejidad*

Para algunos expertos, el riesgo macro y geopolítico es más complejo para las empresas empresas europeas porque los competidores en EEUU y China no enfrentan la misma complejidad de riesgo macroeconómico político. Se argumenta que la innovación llega más de estos países que de Europa. Otro riesgo latente, aún no manifiesto en toda su intensidad, es el riesgo fiscal: los gobiernos europeos buscan ingresos para reconstruir sus finanzas después de la pandemia.

Aunque toca reducir costes para amortiguar la caída de los márgenes, las organizaciones no pueden dejar de invertir, pero sí deben aprender a invertir de manera más inteligente tanto en innovación como en personas y clientes, señala *Kees Roks,* DAI de Novartis.

Si hubiera una recesión o desaceleración económica, ¿qué 5 riesgos serían los más afectados?



Fuente: *Risk in Focus 2024 y ediciones anteriores.*

> *Es extremadamente importante que la empresa no se aísle demasiado en un mundo de riesgos interconectados.*

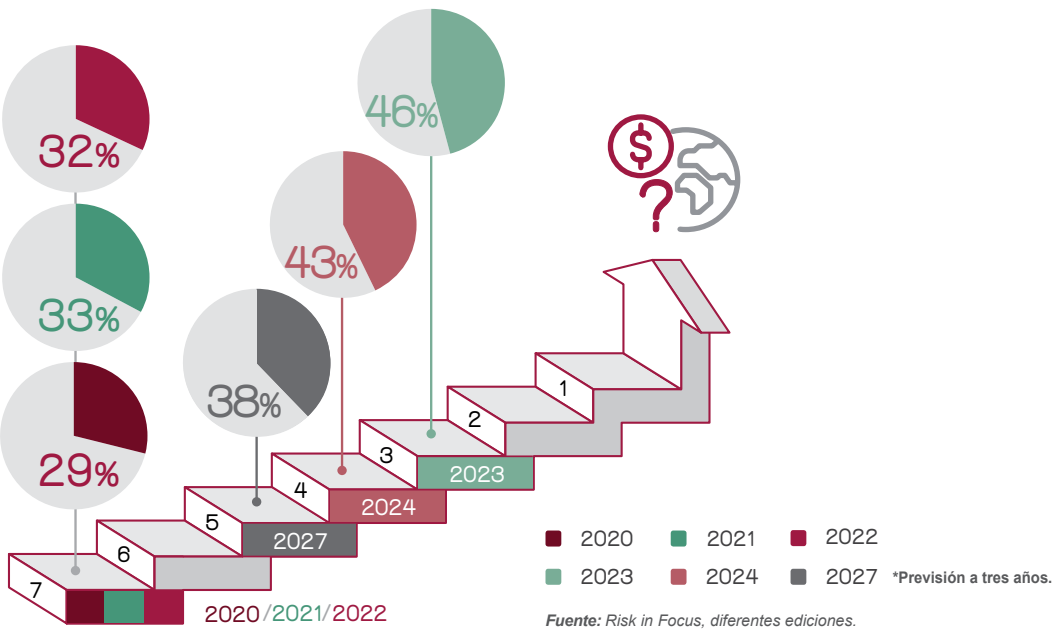
Las empresas están implementando sistemas de control que son más ágiles, adaptables y que incorporan una monitorización en tiempo real. También se están repatriando y descentralizando elementos de la cadena de suministro para hacerla más resistente y menos dependiente de proveedores específicos para materiales o productos clave.

"Es extremadamente importante que la empresa no se aísle demasiado en un mundo de riesgos interconectados", dice un DAI que defiende que *"Auditoría Interna participe en las discusiones sobre la estructura de gobierno de la organización para que se abran los silos y la gestión de riesgos tenga el enfoque correcto, incluso en la conexión entre amenazas"*. La función también debe ayudar a identificar riesgos geográficos específicos para reducir dependencias y preservar una perspectiva global del riesgo.

> *Encontramos el equilibrio sobre el riesgo geopolítico, pero el impacto macroeconómico sucede ahora mismo, mientras hablamos*

Evolución en los últimos cinco años del riesgo macroeconómico y geopolítico

Posición en el ranking y peso en porcentaje



Fuente: *Risk in Focus, diferentes ediciones.*

Cómo puede ayudar Auditoría Interna

1. Evaluar si la organización es resistente a cambios complejos e impredecibles y si los procesos de identificación, evaluación, control y gobierno de riesgos están diseñados para afrontar esos desafíos.

2. Evaluar la efectividad de los mecanismos que la organización necesita para estar al tanto de los cambios en el entorno macroeconómico y geopolítico, incluso si está adecuadamente informada sobre tendencias relevantes, sus interrelaciones y posibles impactos.

3. Evaluar si el proceso de inversión estratégica planificada en I+D es adecuado para ayudar a la organización a lograr sus objetivos estratégicos a largo plazo y seguir siendo competitiva a nivel mundial.

4. Evaluar si los supuestos realizados en las pruebas de estrés financiero, liquidez y otros procesos de riesgo económico se alinean con la realidad y si los ejercicios de planificación y simulación de escenarios económicos están atentos a posibles cambios futuros del mercado para preservar la robustez de la organización.

5. Evaluar si la organización y la infraestructura operativa del negocio -incluida la cadena de suministro- han adoptado estrategias ágiles y es adaptable y resiliente ante riesgos rápidos e impredecibles.

6. Asesorar a la empresa sobre la adaptación y mitigación de los riesgos asociados con la incertidumbre macroeconómica y geopolítica, incluida la revisión y el ajuste de las estrategias comerciales, planes financieros y prácticas operativas.

7. Evaluar los controles, políticas y procedimientos internos para garantizar el cumplimiento de las regulaciones y requisitos legales relacionados con la incertidumbre macroeconómica y geopolítica, como las sanciones internacionales y las normas contra el lavado de dinero.

Riesgo de terceros

Entre la disrupción y las insolvencias

La desaceleración económica unido al encarecimiento de la financiación podría disparar las insolvencias y el riesgo de terceros. Además, los ajustes de la cadena de suministro aún no han terminado y cualquier chispa puede avivar de nuevo este riesgo.

El riesgo de terceros se ha disparado tanto desde el punto de vista de proveedores, por las tensiones de la cadena de suministro, como del resto porque el viento sopla en contra debido a una desaceleración económica que, de ser acusada, aumentará el riesgo de insolvencia. Hay que abordar bien este riesgo *"crítico"*, tal y como lo han identificado los participantes de la encuesta **Risk in Focus 2024**. En el ranking se sitúa en octavo puesto, igual que los últimos años.

No se espera una gran recesión económica en Europa, aunque dependerá de algunas variables, entre ellas el hecho de que se haya logrado frenar ya la inflación y no surjan nuevos riesgos geopolíticos.

Tras la disrupción de las cadenas de suministro durante los años de pandemia, las relaciones con los proveedores se han vuelto más complejas y, fácilmente, pueden ser puerta de entrada de otros riesgos en la organización. Como no están *en casa sino lejos*, con frecuencia se subestima la escala y velocidad de transmisión de los riesgos que pueden generar.

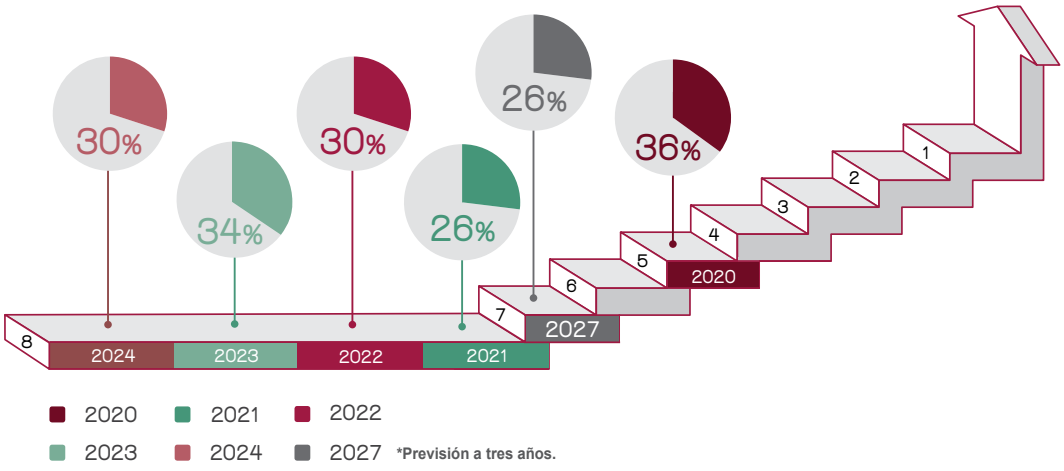
> *Necesito saber si mi proveedor está 100% comprometido a proporcionarme lo que necesito, de lo contrario podría quedarse fuera.*

> *No todos los contratos de proveedores tienen KPI sobre ESG y no siempre es posible imponerles los estándares propios.*

El riesgo de terceros será mayor en 2024, a medida que la desglobalización vaya avanzando y se adopten nuevas estrategias de la cadena de suministro para adaptarse a los cambios normativos: EEUU ha diseñado varias leyes para impulsar la repatriación de compañías y reducir su dependencia

Evolución en los últimos cuatro años del riesgo de terceros

Posición en el ranking y peso en porcentaje



Fuente: *Risk in Focus, diferentes ediciones.*

de China en tecnologías clave. Se espera una reacción de la UE para evitar la fuga de empresa a EEUU. Diferentes países europeos están haciendo regulaciones para preservar el respeto a los derechos humanos y otras cuestiones de sostenibilidad por parte de las cadenas de suministro. Pero en tiempos de inflación y estrechamiento de márgenes, puede ser más difícil imponer algo a proveedores. Otro aspecto relevante es que no siempre se tiene en cuenta el impacto climático en el riesgo de terceros.

De coste y calidad a seguridad

Antes, la mayoría de las organizaciones clasificaban a sus proveedores según coste, calidad y velocidad de entrega. Ahora, la clave es que no me falle para obtener los materiales y productos básicos que necesito.

El riesgo de terceros afecta tanto a la compañía que algunos DAIs empiezan a considerar a los proveedores como parte del universo de riesgos propios de la organización. Cada vez es más frecuente ayudar a los proveedores a diversificarse y establecer con ellos alianzas más estrechas, algo crítico cuando uno depende de una única fuente de suministro. La diversificación de la oferta también es importante. Las empresas buscan alternativas e invierten en I+D para crear bienes y materiales de reemplazo. Todo ello con el objetivo de dotarse de planes de continuidad comercial para la cadena de suministro. Esos planes tienen que identificar los riesgos interconectados que pueden afectar al mismo tiempo a la organización, cómo influyen entre sí, con qué velocidad se contagian y qué riesgos asociados despiertan.

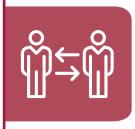
Cómo puede ayudar Auditoría Interna

1. Evaluar la diversificación de la cadena de suministro, considerado una combinación adecuada de proveedores globales y locales y si hay inversiones para encontrar materiales alternativos para recursos clave. Analizar si hay monitorización para detectar a tiempo problemas potenciales.

2. Asistir en la realización de la diligencia debida sobre posibles proveedores y socios. Evaluar estabilidad financiera, reputación, compliance y prácticas de gestión de riesgos y analizar si están alineados a la empresa.

3. Revisar contratos y acuerdos de la cadena de suministro: términos, asignación de riesgos, métricas de desempeño, resolución de disputas, protección de datos, confidencialidad y otros requisitos de cumplimiento.

4. Ayudar a desarrollar e implementar marcos efectivos de gestión de proveedores en todo su ciclo: selección, incorporación, monitorización y terminación.



5. Evaluar el rendimiento de terceros frente a criterios predefinidos. Garantizar el cumplimiento de los requisitos normativos y prepararse para la llegada de la Directiva de Diligencia Debida y la de Sostenibilidad Corporativa: realizar auditorías periódicas, evaluación de indicadores clave de rendimiento y seguimiento de obligaciones contractuales.

6. Identificación de áreas de mejora dentro de la cadena de suministro: relaciones de subcontratación, prácticas de gestión de riesgos de terceros, recomendaciones de mejora en los procesos, implementación de controles más sólidos y fomento de una cultura de concienciación sobre riesgos y responsabilidades.

7. Asistir en el desarrollo de planes sólidos de gestión de crisis e incidentes relacionados con interrupciones de la cadena de suministro: procedimientos para mitigar el impacto, revisiones posteriores al incidente e implementación de acciones correctivas.

Riesgo de talento

Nuevas estrategias de capital humano

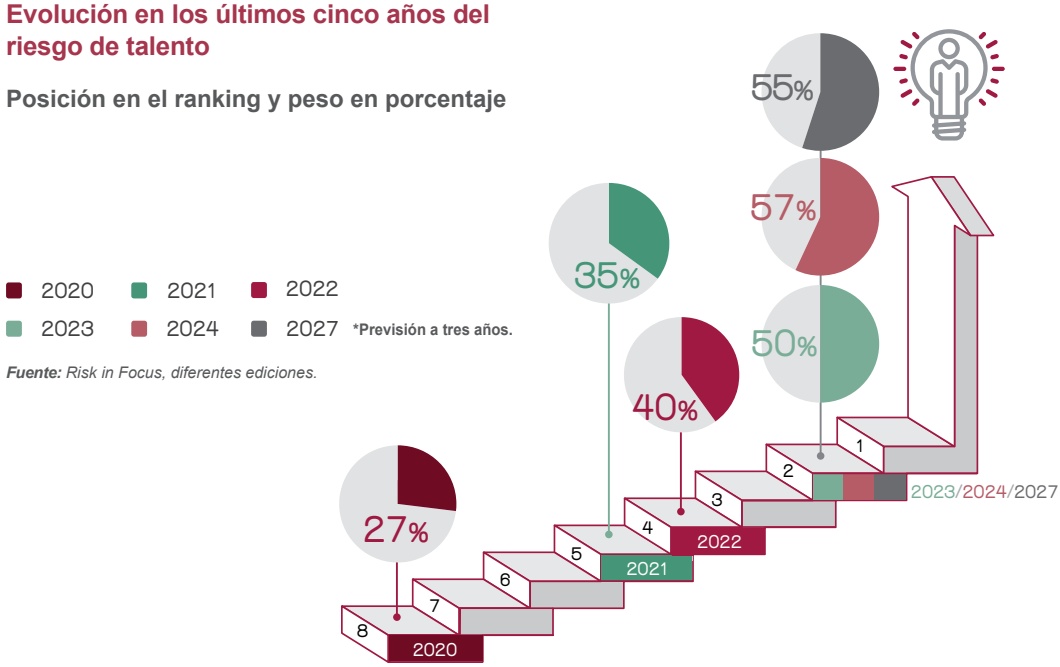
Es el segundo riesgo más relevante. Hay que revitalizar la cultura corporativa y las estrategias de capital humano porque se han quedado desactualizadas. Se requiere un cambio cultural que no todas las empresas podrán abordar.

El capital humano, la diversidad y la gestión del talento se consolida como segundo mayor riesgo para 2024 y a tres años vista. Las empresas luchan por atraer y retener al mejor talento. Ningún área de negocio es inmune. Sin las habilidades y el talento adecuado, las organizaciones ven peligrar sus objetivos estratégicos.

El difícil entorno económico ha alentado las demandas económicas y sociales de los empleados, que están paralizando con huelgas empresas y sectores. Las empresas se enfrentan a un alza de los costes laborales en un momento de cambio de comportamiento de los clientes.

Evolución en los últimos cinco años del riesgo de talento

Posición en el ranking y peso en porcentaje



Fuente: *Risk in Focus, diferentes ediciones.*

Cambio cultural

Muchas organizaciones se sienten fuera de juego. La cultura corporativa está desactualizada y no logra atraer talento. Es hora de revitalizar las estrategias de capital humano, incluyendo fórmulas como el trabajo flexible y dotándose de un sólido propósito social. Algunas firmas ofrecen salarios más altos para evitar la salida de talento. Eso puede solucionar el problema a corto plazo, pero no comunicar el propósito más amplio de la empresa y construir una cultura más diversa solo empeora las cosas. La pandemia dio paso a un cambio radical en las actitudes hacia la vida laboral que las empresas aún tienen que gestionar.

La diversidad, de género, raza y edad, ha crecido en las empresas, pero quedan gaps: todavía hay pocas mujeres en carreras STEAM y en puestos de alta dirección. Por regulación explícita, ellas tendrán en 2026 en Europa el 40% de los puestos del consejo de administración.

La retención también es un gran desafío. Muchas organizaciones han perdido empleados experimentados en los mandos intermedios, la gran columna vertebral de la mayoría de las empresas. ¿El problema? No hay rutas internas claras de carrera profesional o promoción y los jóvenes se marchan a otras firmas que comunican mejor las oportunidades.

La salud mental está adquiriendo también gran protagonismo en las empresas desde la pandemia. El trabajo en remoto conduce a aislamiento y, con frecuencia, deriva en ansiedad y estrés.

El consejo de administración debe ser consciente de estas realidades e ir más allá de los KPIs convencionales de recursos humanos. Debe impulsar la implementación de una transformación cultural que sea visible, real y esté alineada con los valores y las expectativas del talento. Auditoría Interna tiene que observar los procesos y evaluar si son adecuados para su propósito, haciendo auditorías más informales y flexibles si es necesario.

Los DAIs, que también están sufriendo problemas de captación y retención de talento, no pueden perder su propia batalla. Necesitan habilidades tecnológicas y perfiles especializados en información no financiera, por poner dos ejemplos que muestran que la función también requiere diversidad de nuevo talento, más allá de los financieros y contables tradicionales.

> 66
>
> *La cultura corporativa está desactualizada y no logra atraer talento. Es hora de revitalizar la estrategia de capital humano.*

Cómo puede ayudar Auditoría Interna

1. Evaluar si las estructuras de gobierno respaldan la información necesaria del consejo y permiten respuestas ágiles al riesgo de gestión del talento.

2. Revisar si los valores y objetivos de la organización se comunican dentro y fuera claramente y de una manera que se comprometa con el talento potencial y existente.

3. Analizar la planificación de la plantilla y las estrategias de gestión de la sucesión para puestos y roles clave. Ver si existen programas de desarrollo de la fuerza laboral para satisfacer las necesidades comerciales futuras y si estos se comunican claramente en toda la empresa.

4. Revisar los sistemas de gestión y evaluación del desempeño y su alineación con los programas de recompensas y reconocimiento. Evaluar las metodologías de establecimiento de objetivos y su correlación con compensación y desempeño.

5. Revisar las métricas de diversidad de la empresa, analizar la representación en diferentes niveles y departamentos y las mejores prácticas. Evaluar la eficacia de los programas e iniciativas de diversidad para atraer y retener talento.

6. Analizar la efectividad de los programas de capacitación y desarrollo de la organización y su impacto en el desempeño y el compromiso de los empleados.

7. Evaluar si las encuestas de compromiso de los empleados, las entrevistas de salida y otros mecanismos de retroalimentación evalúan efectivamente los niveles de satisfacción de los empleados y permiten identificar problemas potenciales que afecten a la moral de los empleados además de brindar recomendaciones de mejora.

Riesgo climático, biodiversidad y sostenibilidad

Absorberá mucha atención y esfuerzo

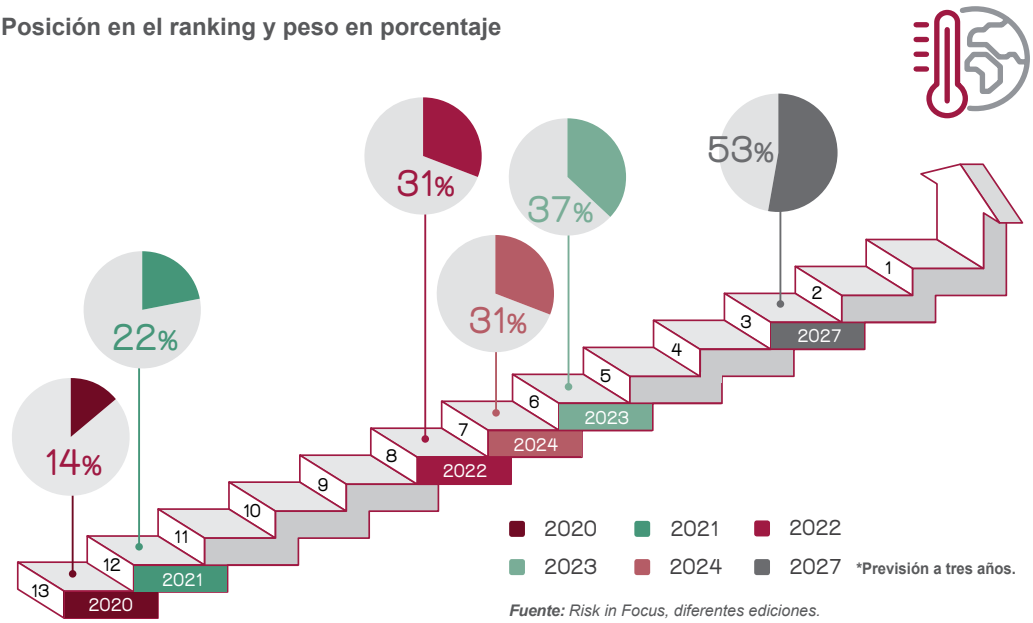
La proliferación de nuevas normativas y estándares elevará las tareas de cumplimiento normativo y elevará la calidad de la información no financiera. Cada empresa debe seleccionar sus objetivos sostenibles y centrarse en los más relevantes.

El cambio climático no da respiro. Ni a la naturaleza, ni a gestores o auditores. Están entrando en vigor nuevas regulaciones que añaden transparencia al reporting y a la clasificación (taxonomía) del riesgo climático. Desplazado este año al séptimo puesto por la desaceleración económica, sube nada menos que al tercero en las previsiones a tres años. El riesgo climático va a absorber más atención y esfuerzo de 2024 en adelante. También a los auditores: en tiempo y esfuerzo dedicado, el riesgo climático ocupa este año el puesto 12º y sube al 4ª a tres años vista.

Las temperaturas por encima de lo normal y el frío extremo están añadiendo dificultades a fábricas y plantas de energía. Estos riesgos

Evolución en los últimos cinco años del riesgo climático

Posición en el ranking y peso en porcentaje



Fuente: *Risk in Focus, diferentes ediciones.*

afectan a las operaciones y se extienden por toda la cadena de suministro. La incertidumbre regulatoria -hay aspectos importantes aún por precisar- está frenando la inversión en proyectos más ecológicos, pese a que ser verde vende y puede activar el impulso de pasarse y caer en el *greenwashing*.

El 2024 es el año de aprobación, entrada en vigor o aplicación efectiva de normas muy relevantes en materia de sostenibilidad como la Directiva de Informes de Sostenibilidad Corporativa (CRSD), los estándares europeos ESRS y los estándares internacionales del ISSB, entre otros. Compliance va a tener mucha carga de trabajo.

Propósito y estrategia

Auditoría Interna tiene un papel clave en la educación de sus organizaciones sobre la estrategia y los objetivos sostenibles y en la interpretación de reglas y regulaciones para que sean accesibles y manejables. Es fundamental contar con un marco de gestión de riesgos capaz de identificar y evaluar el riesgo climático y la sostenibilidad y establecer controles efectivos para gestionarlos e

> *El cambio climático podría afectar a nuestra capacidad para obtener productos naturales esenciales en el largo plazo.*

> *El tema y el dolor va a estar en el cumplimiento normativo. No en si podemos cambiar o no el medio ambiente.*

informar sobre ellos. Realizar auditorías de preparación y compartir los datos entre la primera y la segunda línea de aseguramiento ayudará a difundir las mejores prácticas.

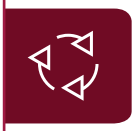
Las empresas deben seleccionar cuidadosamente sus objetivos sostenibles -la ONU promueve 17 ODS- y centrarse en los relevantes, aplicando métricas claras que pueden integrarse en el plan de negocio. La menor calidad de la información no financiera disponible quedará subsanada con las nuevas normativas y estándares. Hasta que eso llegue, hay más necesidad de que los auditores internos evalúen la validez de las afirmaciones y los datos de sostenibilidad. Fortalecer los procesos de gobierno interno para garantizar que se ajusten al propósito requiere mucho tiempo, pero es esencial para eliminar brechas, errores o duplicación en roles y responsabilidades.

Un error común es tratar de alinear el propósito de la organización con los ODS cuando no hay datos disponibles. Pero cuando no existen datos, hay que comenzar a construir desde cero. Asociarse con una ONG puede ser una gran ayuda para aprovechar su conocimiento y abordar el reporting, aún poco desarrollado, de los impactos sociales y de biodiversidad.

Cómo puede ayudar Auditoría Interna

1. Evaluar si los objetivos de sostenibilidad están alineados con la estrategia y tienen métricas claras.

2. Evaluar si los objetivos declarados interna y públicamente se construyen a partir de datos y análisis exhaustivos y están alineados con la regulación o dependen demasiado de metas y promesas vagas y corren el riesgo de ser calificados como *greenwashing*.



3. Evaluar la eficacia de la gestión de riesgos relacionados con el cambio climático, la pérdida de biodiversidad y la sostenibilidad ambiental, incluido el impacto en operaciones, cadena de suministro, reputación y cumplimiento normativo. Ver si los recursos asignados a los objetivos son adecuados para su logro.

4. Evaluar si la organización se adhiere a las reglamentaciones, normas y requisitos de informes ambientales actuales y está preparada para las futuras.

5. Evaluar si los mecanismos de monitorización rastrean adecuadamente el desempeño ambiental, incluida la evaluación del consumo de energía, las emisiones de gases de efecto invernadero, el uso del agua, la gestión de desechos y otras métricas. Promover una cultura de mejora continua, identificando e intercambiando mejores prácticas, soluciones innovadoras y oportunidades para aumentar la eficiencia en el uso de recursos.

6. Revisar la eficacia de sistemas y procesos relacionados con la sostenibilidad ambiental. Verificar si las consideraciones de sostenibilidad están incluidas en los procesos de toma de decisiones, en la gestión de la cadena de suministro, el diseño de productos y en las iniciativas de reducción de residuos.

7. Evaluar la interacción con las partes interesadas en temas de sostenibilidad y sus expectativas, facilitando el diálogo e identificando oportunidades de colaboración para abordar el cambio climático, la biodiversidad y las preocupaciones ambientales.

Ciberseguridad y protección de datos

Fortalecer el sistema nervioso digital

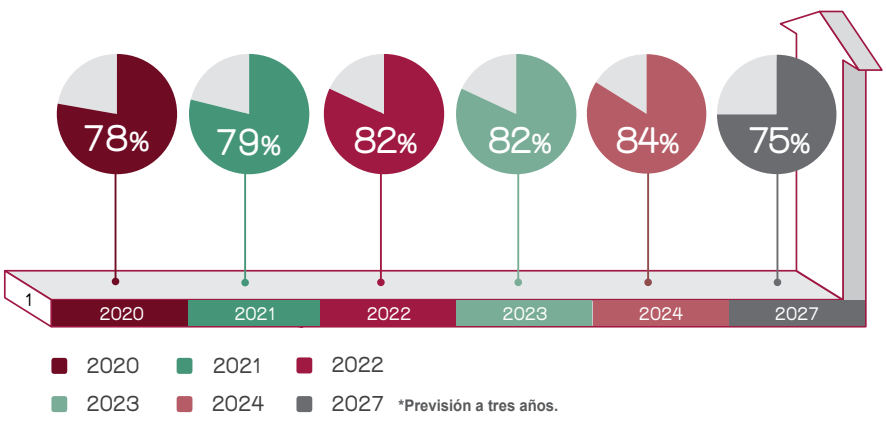
La defensa cibernética es más madura ahora que antes de la pandemia, pero el mundo digital es más peligroso y requiere permanecer vigilante. La monitorización constante y la innovación en el control de la ciberseguridad son imprescindibles.

Es el riesgo imbatible en la primera posición. Ahí ha estado los ochos años desde que lleva realizándose este informe y ahí figura también, a la cabeza, en las previsiones para los próximos tres años. Ciberseguridad es también el riesgo al que más tiempo y esfuerzo dedica Auditoría Interna actualmente y al que más tiempo dedicará a tres años vista.

Hay más conciencia sobre la amenaza de la ciberseguridad a todos los niveles gracias a la preparación y a las campañas ad hoc de las empresas e instituciones. La madurez de la defensa cibernética es ahora mayor que antes de la pandemia, pero también el mundo digital es más peligroso. La piratería se ha profesionalizado e industrializado para comercializarse fácilmente entre

Evolución en los últimos cinco años del riesgo de ciberseguridad

Posición en el ranking y peso en porcentaje



Fuente: *Risk in Focus, diferentes ediciones.*

> *El mayor desafío ahora es identificar en qué debemos invertir para abordar las exposiciones desconocidas.*

profesionales y aficionados. Los cibercriminales usan automatización y algoritmos avanzados en sus ataques y utilizan cada vez más a los proveedores de la cadena de suministro que detectan que tienen vulnerabilidades y son una puerta de entrada fácil. Paralelamente, crecen los ciberataques a nivel Estado: como objetivo y como autor indirecto, los llamados ataques patrocinados por estados, frecuentemente ligados a tensiones geopolíticas.

Además de aumentar en número y en complejidad los ciberataques, se ha incrementado el perímetro de ciberseguridad a vigilar, al incluir la cadena de suministro, digitalizar cada vez más partes y procesos del negocio y propagarse el uso de la Inteligencia Artificial Generativa entre las empresas. La vigilancia constante y la innovación en el control son imprescindibles.

La Inteligencia Artificial (IA) puede ser enemigo, en manos de los *hackers*, y aliado, si se utiliza para anticiparse a los ciberataques monitorizando potenciales amenazas que puedan estar gestándose en lo más oscuro de la dark web. Hoy en día hay múltiples técnicas y señales de alerta que hay que conocer, analizar e identificar. La IA permite monitorizar amenazas al escanear rápidamente patrones de actividad y detectar elementos poco o nada habituales.

También se ha avanzado en las soluciones de recuperación: hay sistemas avanzados que garantizan que las actividades críticas puedan reconstruirse desde cero incluso en el caso de que los piratas informáticos hayan dañado las copias de seguridad. En las organizaciones grandes, los esfuerzos se centran en asegurar la continuidad de negocio, la resiliencia operativa, la gestión de crisis y la respuesta a desastres.

Proteger la tecnología operativa de las amenazas es clave. Eso exige mirar la ciberseguridad desde un enfoque TI, prestando atención a cada detalle de la infraestructura digital para identificar vulnerabilidades y fortalecer los controles. Parece necesario elevar el perfil del CISO y que Auditoría Interna trabaje en estrecha colaboración con él para que los riesgos identificados por el CISO se cuantifiquen y comuniquen claramente.

> *Quien no identifique los riesgos para su infraestructura operativa con suficiente detalle, se verá afectado.*

Cómo puede ayudar Auditoría Interna

1. Evaluar posibles riesgos de ciberseguridad dentro de la organización y la eficacia de los controles existentes, incluida la identificación de vulnerabilidades y áreas de mejora.

2. Analizar si la organización cumple la normativa y estándares de ciberseguridad relevantes del momento y está preparada para las futuras.

3. Revisar la efectividad de los controles de ciberseguridad en primera y segunda línea y para los activos clave de la organización: controles de acceso, seguridad de red, planes de respuesta a incidentes, encriptación de datos y cualquier otra medida.

4. Hacer evaluaciones de vulnerabilidad para identificar debilidades y posibles puntos de entrada para ataques cibernéticos, incluidas pruebas de penetración, escaneo de vulnerabilidades y *hacking* ético.

5. Evaluar la efectividad de los procesos de monitorización: garantizar que las revisiones de los registros de seguridad, las configuraciones del sistema y otros indicadores de posibles infracciones de seguridad se controlen adecuadamente.

6. Revisar la eficacia del plan de respuesta a incidentes y sus capacidades para ejecución, incluido el uso de ejercicios simulados para brindar recomendaciones de mejora.

7. Evaluar los programas de capacitación y concientización sobre seguridad de la organización para descubrir si los empleados están adecuadamente capacitados para reconocer y responder a las amenazas de seguridad y brindar recomendaciones para mejorar la efectividad de las iniciativas de capacitación.

8. Analizar los controles y prácticas de seguridad cibernética para proveedores y socios para garantizar que cumplan con los estándares y políticas de seguridad de la organización.

Referencias

- **Instituto de Auditores Internos de España.**
  - **La Fábrica de pensamiento.** Auditoría de la Inteligencia Artificial aplicada a procesos. Febrero 2023.
  - **La Fábrica de pensamiento.** Auditoría Interna de la cultura corporativa. Abril 2023.
  - **Revista.** Sostenibilidad, de los cuentos a las cuentas. Julio 2023.
  - **Revista.** ChatGPT: abre nuevos riesgos para Auditoría Interna. Marzo 2023.
  - **Revista.** La guerra de Ucrania dispara el riesgo de terceros. Julio 2022.
  - **Revista.** Nueva era en la gestión del talento. Marzo 2022.

- **Esfera Consejeros.**
  - Riesgos ESG: puntos y preguntas clave.
  - Riesgo climático: ¿Estamos preparados?
  - Algoritmos para detectar (antes) el fraude.
  - La UE mapea el greenwashing para erradicarlo.
  - Ciberseguridad, un riesgo sistémico a vigilar.
  - Cómo supervisar la calidad de la información no financiera.
  - Serie Transformación digital.

- **Global IIA, ECIIA y otros institutos**
  - **ECIIA:** Risk in Focus 2024 edición europea en inglés.
  - **ECIIA.** GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation. 2019.
  - **Internal Audit Foundation.** Are we speaking the same language? identifies supply chain failings during the pandemic and after.
  - **IIA.** Auditing Culture Guide.
  - **IIA.** Global technology audit guides (GTAG). Ver Análisis técnicos (solo socios).
  - **IIA.** Understand the elements of combined assurance.
  - **Reino Unido.** CIIA 2023 report Navigating geopolitical risk,
  - **Reino Unido.** Chartered IIA warns boards to “get a grip” on unhealthy corporate cultures in the wake of a string of culture-related scandals.
  - **Reino Unido.** Harnessing internal audit against climate change.

- **Reino Unido.** Fraud is on the rise: step up to the challenge for analysis and practice advice.
- **Reino Unido.** Embracing data analytics.
- **Países Bajos.** A reference model for auditing organisational resilience.
- **Países Bajos.** Internal audit and supply chain risks.
- **Union Europea.**
  - Directiva Corporate Sustainability Reporting Directive (CSRD).
  - Gender Equality: The EU is breaking the glass ceiling thanks to new gender balance targets on company boards.
  - 2021 report on gender equality in the EU.
  - Minimum health and safety requirements for the protection of mental health in the workplace.
  - Reglamento General de Protección de datos: preguntas y respuestas. What is GDPR, the EU's new data protection law?
- **ONU.** The working Group. Sixth Assessment Report.
- **ISO.** ISO/IEC 27001 Information security management systems.
- **American Accounting Association.** Breaking the Barrier: On the Use of Joint Audits in the Internal Audit Profession.

Instituto de Auditores Internos de España.
Santa Cruz de Marcenado, 33 - 28015 Madrid
Tel.: 91 593 23 45 - Fax: 91 593 29 32
www.auditoresinternos.es

ISBN: 978-84-126682-3-0

Diseño y maquetación: Blondas de Papel S.L.

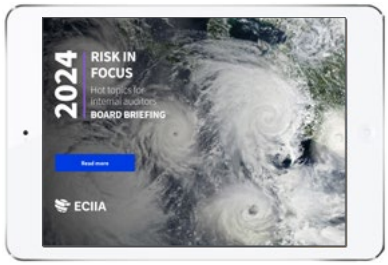
esfera consejeros

The Institute of Internal Auditors

European Confederation of Institutes of Internal Auditing

- Si eres consejero de una empresa socia del Instituto y quieres darte de alta en Esfera Consejeros, solicítalo aquí.
- Si tienes dudas, escríbenos a esferaconsejeros@iai.es

Risk in Focus 2024 es un Informe elaborado por Institutos de la Confederación Europea de Institutos de Auditores Internos (ECIIA) de 17 países, entre ellos el de España. El informe ofrece una perspectiva europea sobre los riesgos empresariales a corto y medio plazo desde la mirada del Auditor Interno.



Descarga PDF