

esfera
consejeros

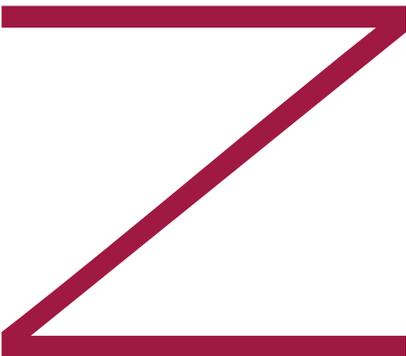
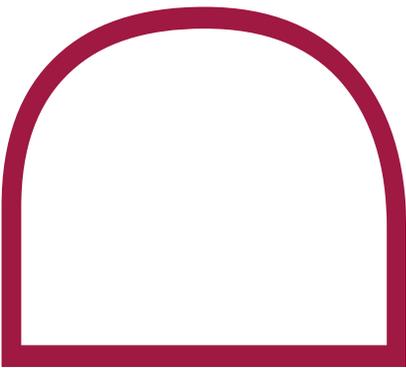
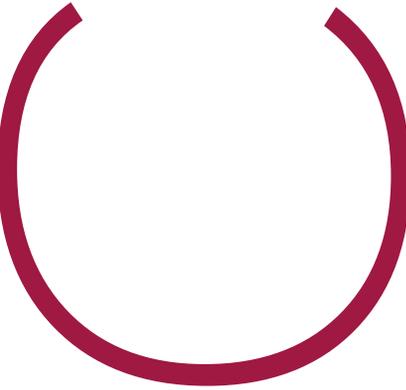
Risk in Focus

2023

VISIÓN DEL
AUDITOR INTERNO

El riesgo de
talento se dispara





1. Incertidumbre marco y geopolítica	13 Pág
2. Riesgo climático	16 Pág
3. El riesgo de talento se dispara	19 Pág.
4. Ciberseguridad y protección de datos	22 Pág
5. Digitalización y tecnologías emergentes	25 Pág.

28

30

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 2022

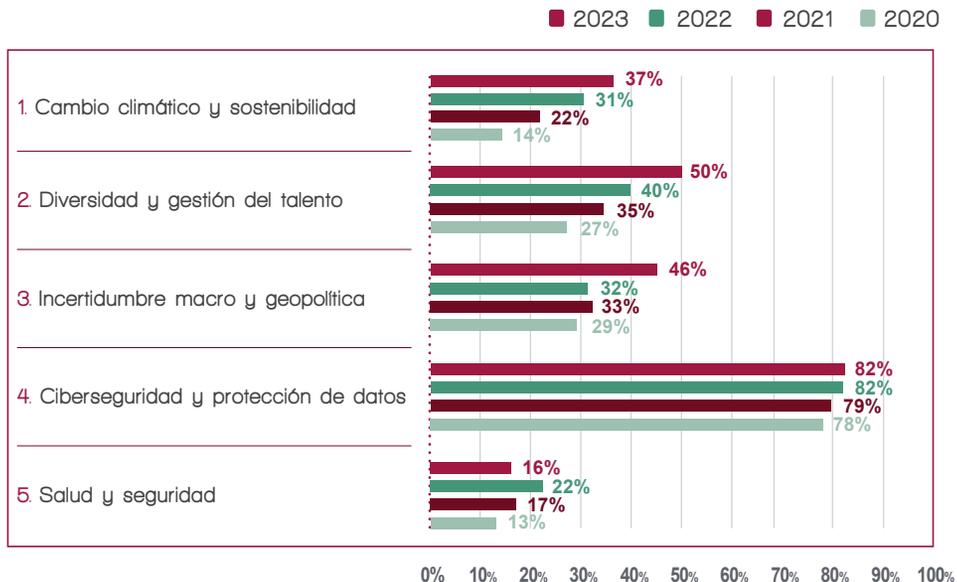
- Si eres consejero de una empresa socia del Instituto y quieres darte de alta en Esfera Consejeros, [solicítalo aquí](#).
- Si tienes dudas, escríbenos a esferaconsejeros@iaies



De un vistazo

El riesgo de talento se dispara. El año pasado se pudieron ver los primeros síntomas de lo que ya se ha convertido en una realidad: el riesgo de talento se ha disparado en el nuevo marco empresarial, colocándose incluso por encima del más que evidente riesgo geopolítico ocasionado por la guerra de Ucrania. Así lo refleja el informe *Risk in Focus 2023*, que ofrece una panorámica europea sobre los principales riesgos empresariales desde la mirada del Auditor Interno.

Los riesgos que más han subido en cuatro años



Fuente: Risk in Focus 2023 y ediciones anteriores.

Adaptarse a un estado de crisis permanente

Las empresas están sometidas a enorme presión. Los riesgos son cada vez más complejos y vienen entrelazados, conformando un estado de crisis permanente de difícil gestión. A los riesgos clásicos como ciberseguridad, financieros o de terceros, se suman otros como el riesgo de talento, de cultura corporativa y de cambio climático.

Se esperaba que 2022 fuera un año de vuelta gradual a la normalidad. Y nada más lejos de la realidad: la guerra en Ucrania ha disparado complejos riesgos, sometiendo a las organizaciones a un nivel de presión sin precedentes.

Desde 2021, los precios se han disparado, las cadenas de suministro operan con muchas dificultades, hay escasez de ciertos productos básicos, el descontento social crece, los bancos centrales han empezado a endurecer su política monetaria... Todo ello hace pensar que el mundo se encamina hacia una recesión, lo que traería más presión política y social.

Los Directores de Auditoría Interna (DAIs) esperan que las crisis impregnen progresivamente todas las áreas empresariales los próximos años porque, en un mundo interconectado, los riesgos también cruzan rápidamente sus propias categorías y los perímetros departamentales. Un ejemplo es la guerra de Ucrania, que ha disparado los riesgos de compliance, ciberseguridad, macroeconómico y geopolítico, de insolvencia y de continuidad de negocio... Sus efectos serán más profundos y



Risk in Focus: metodología

El informe *Risk in Focus*, que este año va por su séptima edición, ha sido realizado por Institutos de la Confederación Europea de Institutos de Auditores Internos (ECIIA de 15 países europeos): España, Austria, Bélgica, Bulgaria, Eslovenia, Francia, Alemania, Grecia, Italia, Luxemburgo, Países Bajos, Suecia, Suiza y Reino Unido e Irlanda. En la encuesta participaron 834 Directores de Auditoría Interna (DAIs) y se llevaron a cabo cuatro mesas redondas en las que participaron 39 DAIs y entrevistas en profundidad a 9 expertos, presidentes de Comisiones de Auditoría y CEOs. El valor del informe radica en su visión desde Auditoría Interna, además de la perspectiva europea.

generalizados a medida que siga subiendo la inflación y la escasez de oferta. Y esto tiene serias implicaciones para las organizaciones, tanto en las funciones de riesgos como de aseguramiento.

Muchas compañías no están preparadas para afrontar un estado de crisis tan permanente. Aún están estructuradas sobre la visión de que las amenazas pueden abordarse una a una. Pero no.

Ahora más que nunca, los auditores internos deben estar a la altura de estos desafíos inmediatos, sin perder de vista los objetivos estratégicos a largo plazo. El cambio climático podría convertirse rápidamente en el próximo gran riesgo para el que muchas empresas no se han preparado adecuadamente. Y a medida

que los esfuerzos de digitalización se vuelven más importantes, ¿cómo pueden las empresas continuar encontrando y asignando la inversión y las habilidades necesarias para completar un cambio operativo y tecnológico tan amplio? Los auditores internos deben ayudar a sus organizaciones a resolver estos problemas¹.

Los cinco grandes bloques temáticos en los que se ha estructurado el informe **Risk in Focus 2023** 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 en puntos algunos de sus aspectos más relevantes:

¹ Risk in Focus 2022.

Incertidumbre geopolítica

- El riesgo macroeconómico y geopolítico ha saltado de un plumazo del séptimo puesto al tercero.
- La guerra ha disparado la incertidumbre, la ciberseguridad, el riesgo de continuidad de negocio y el de terceros.
- Los riesgos ya no se quedan localizados en una región o área, sino que adquieren dimensión global.
- La planificación del plan de continuidad de negocio también se plantea a escala global y no por regiones.
- Los auditores internos deben mantener actualizadas las evaluaciones de riesgo y reforzar la gobernanza de datos.

Riesgo climático y sostenibilidad

- El clima podría convertirse en la próxima gran crisis para la que las organizaciones no están preparadas.
- Ahora es el sexto de los riesgos prioritarios, pero las previsiones apuntan al tercer puesto en tres años.
- Auditoría Interna se está implicando en el aseguramiento del proceso hacia el objetivo de cero emisiones netas.
- La única forma de combatir el riesgo de maquillaje o *greenwashing* es con buena gobernanza.
- La presión de los accionistas seguirá impulsando la elaboración de informes más precisos.

El riesgo de talento se dispara

- Ha escalado de la cuarta a la segunda posición en el mapa de riesgos empresariales.
- El capital humano es una ventaja competitiva en un mundo escaso de profesionales técnicos.
- La salida de empleados seniors puede crear problemas en las empresas: abre brechas difíciles de llenar.
- Hay que retocar la cultura corporativa, empezando por las políticas de flexibilidad y el propósito.
- La inflación y el descontento social va a añadir más presión a la retención y captación de talento.

Ciberseguridad y protección de datos

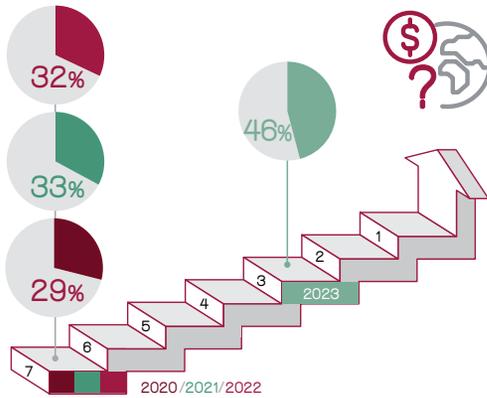
- El riesgo de ciberseguridad sigue imbatible en la primera posición desde hace años.
- Una brecha puede afectar al servicio, la confianza, la reputación, las finanzas... y puede parar el negocio.
- Con la profesionalización del cibercrimen, las empresas deben mantener actualizadas sus estrategias de ciberseguridad.
- Los proveedores son una puerta de entrada a las empresas: suelen tener sistemas de seguridad menos maduros.
- En ciberseguridad, hay que aplicar una visión holística, implicando a IT, compliance y otras áreas.

Digitalización e Inteligencia Artificial

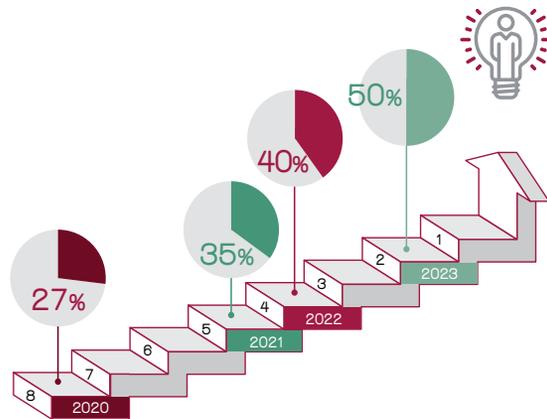
- No basta con considerar la digitalización desde un punto de vista técnico, hay que familiarizarse primero con la cultura de innovación.
- Auditoría Interna puede ayudar a evaluar y fomentar una cultura de innovación.
- Tener datos separados en diferentes sistemas es una práctica habitual en las empresas no nativas digitales.
- Auditoría Interna tiene una visión holística y puede enfrentarse de manera práctica a la fragmentación de datos.
- En los procesos de RPA, tienden a inflarse los beneficios y subestimarse los costes.

Los riesgos que más han subido en cuatro años

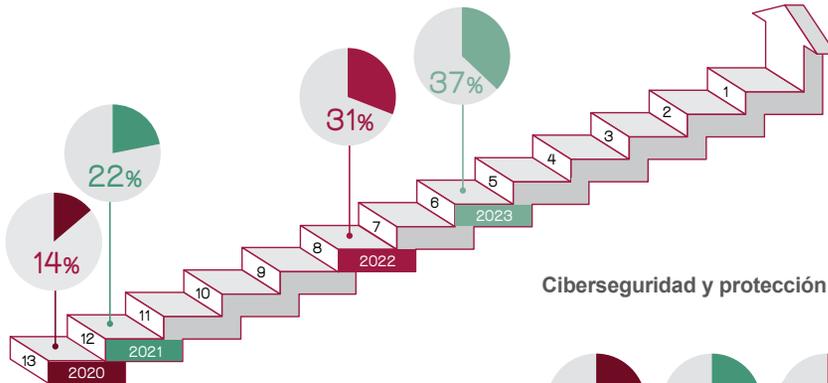
Riesgo macroeconómico y geopolítico



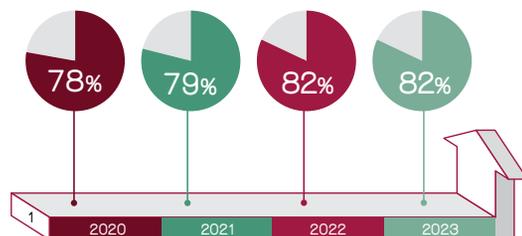
Diversidad y gestión de talento



Riesgo climático y sostenibilidad



Ciberseguridad y protección de datos

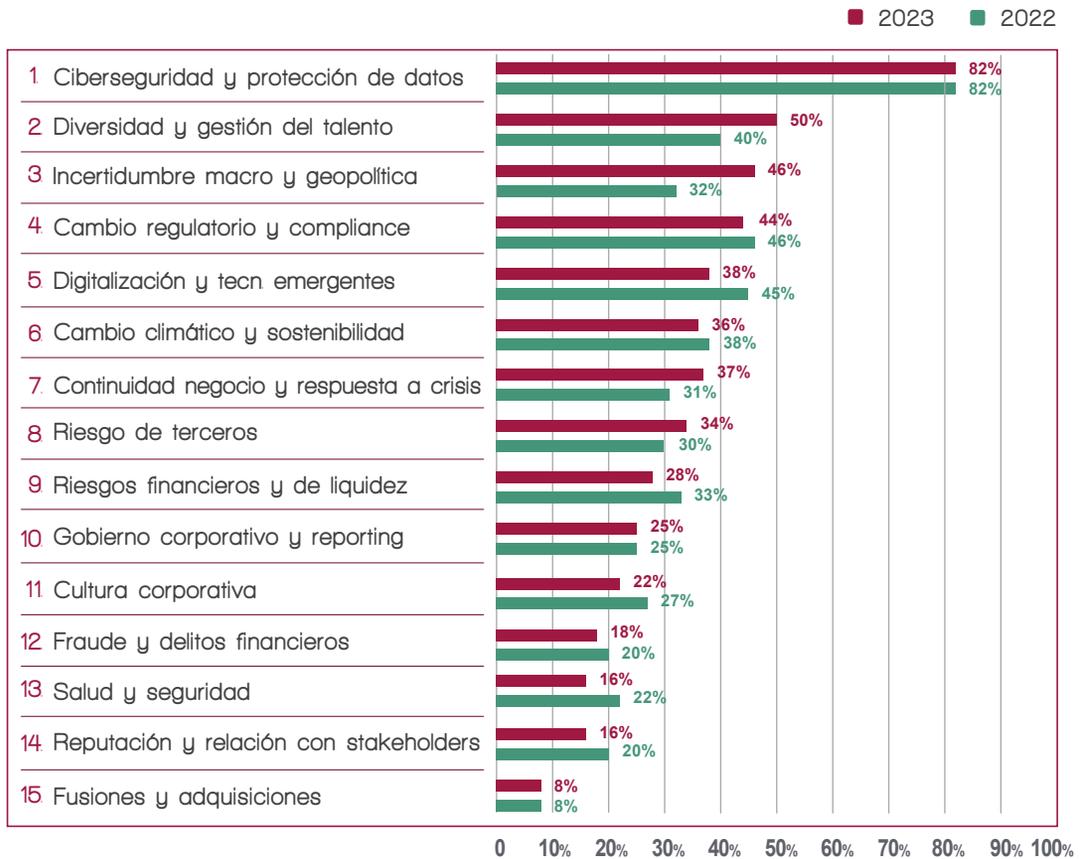


■ 2020 ■ 2021
■ 2022 ■ 2023

Fuente: Risk in Focus, diferentes ediciones.

Previsión de riesgos prioritarios actualmente

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



Fuente: Risk in Focus 2023. Ordenado por los datos de la edición actual (2023) y comparados con la edición anterior (2022).

Previsión de riesgos prioritarios a tres años vista

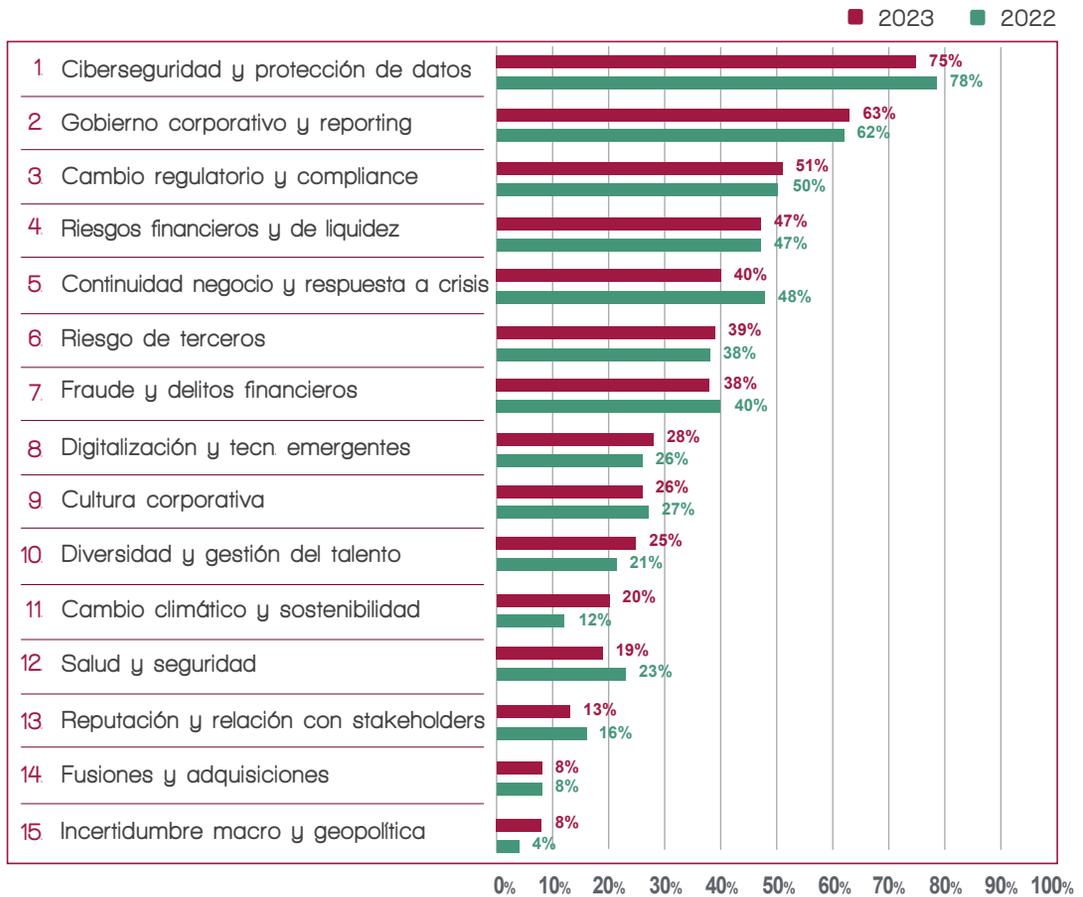
¿Cuáles son los 5 principales riesgos a los que se enfrentará tu empresa en tres años?



Fuente: Risk in Focus 2023. Previsiones de los riesgos prioritarios a tres años vista, 2026.

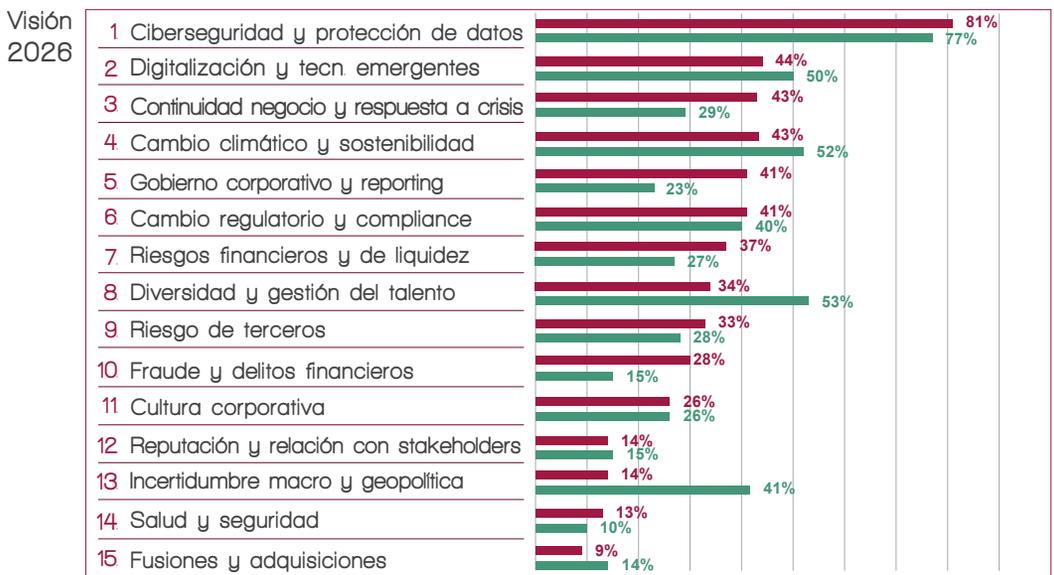
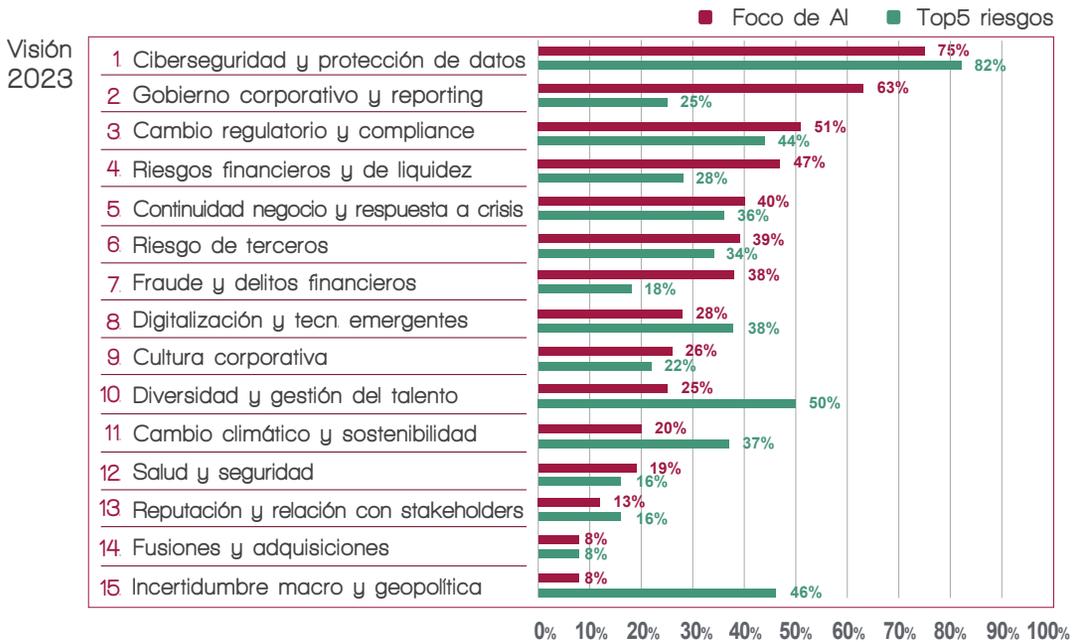
Riesgos a los que Auditoría Interna dedica más tiempo y esfuerzo

Actualmente



Fuente: Risk in Focus 2023. Los datos de 2023 corresponden a esta edición y los de 2022, a la edición anterior.

Auditoría Interna, enfocada a los riesgos prioritarios



Fuente: Risk in Focus 2023. Foco de AI corresponde a los riesgos a los que Auditoría Interna presta más esfuerzo y tiempo. Top riesgos equivale a los riesgos señalados como prioritarios.

Incertidumbre macroeconómica y geopolítica



Las crisis se están volviendo sistémicas. Arrancan en un punto, pero la cadena de consecuencias se expande de un área a otra y rápidamente adquiere una dimensión global. Sucedió con la pandemia antes y ahora con la guerra.

La guerra en Ucrania ha disparado el riesgo macroeconómico y geopolítico. Preguntados por los impactos del conflicto, los Directores de Auditoría Interna (DAIs) apuntan la incertidumbre económica y política, la ciberseguridad y la continuidad de negocio. También ha subido el riesgo de terceros, como analizamos en la revista del Instituto².

Y la reacción de los mercados y de los bancos centrales para contener la inflación ha aumentado el riesgo de liquidez y de insolvencia. Y queda más por llegar ahora que Europa se encamina a una etapa de mayor inflación y menor crecimiento³. El Banco Central Europeo (BCE) ya ha puesto fin a 8 años de tipos de interés negativos⁴.

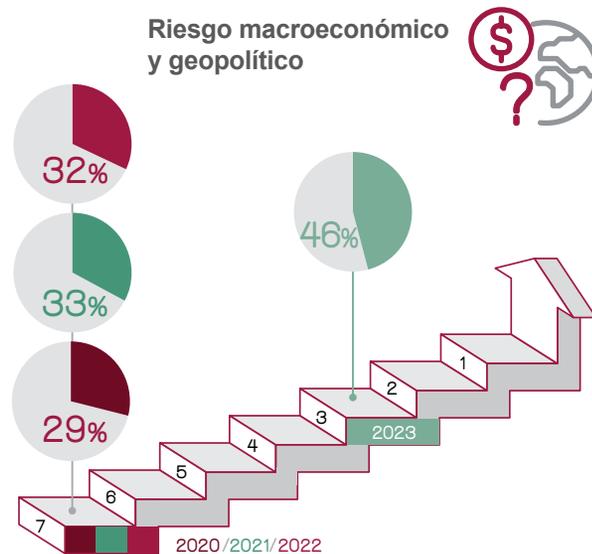
66

La pandemia primero y la guerra, después, han provocado un cambio en la naturaleza de los riesgos emergentes

■ 2020 ■ 2021
■ 2022 ■ 2023

Fuente: Risk in Focus, diferentes ediciones.

Riesgo macroeconómico y geopolítico



² Instituto de Auditores Internos de España. Revista. La guerra de Ucrania dispara el riesgo de terceros. Julio 2022.

³ Comisión Europea. Spring 2022 Economic Forecast: Russian invasion tests EU economic resilience. Mayo 2022

⁴ El País. El BCE acelera y sube los tipos hasta el 0,5% para aplacar la inflación. Julio 2022

Guerra y sanciones

Las sanciones a Rusia y Bielorrusia han obligado a los auditores internos a estar muy pendientes de los cambios regulatorios y su cumplimiento. Es crítico que trabajen con la Primera y la Segunda Línea para mantener actualizadas las evaluaciones de riesgo y reforzar la gobernanza de datos.

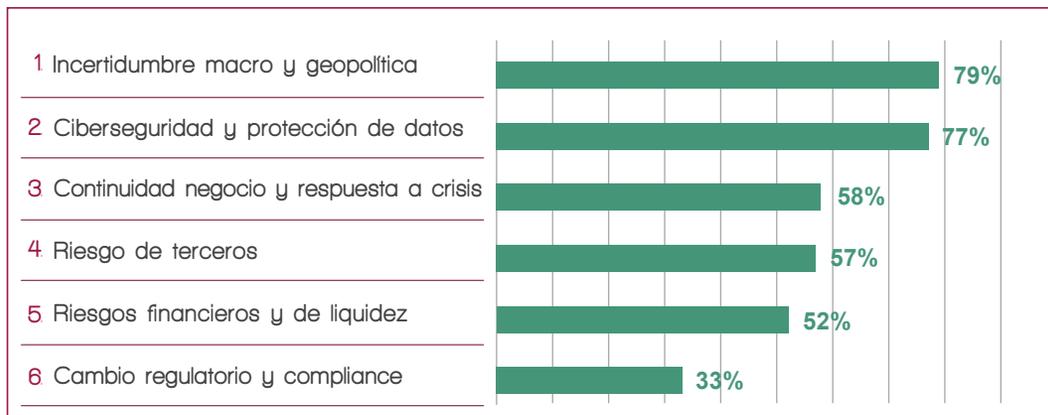
“Sanciones de esta escala y complejidad son una pesadilla”, dice Angela Foyle, socia y responsable de delitos financieros de BDO. Como se originan en diferentes jurisdicciones y se aplican tanto a organizaciones como a individuos, el simple hecho de mantener actualizadas las evaluaciones de riesgos es un auténtico desafío. Las empresas deben mapear las restricciones impuestas por todos los países en su empresa global, incluidas la financiación.

Seguir el rastro del dinero cuando los activos pueden estar en manos de familiares de los sancionados es difícil, lento y costoso.

“La pandemia primero y la guerra, después, han provocado un cambio en la naturaleza de los riesgos emergentes. Ya no permanecen acotados, sino que atraviesan todas las áreas de negocio y están fuera de control”, dice Greg Schlegel, fundador del *Supply Chain Risk Consortium* y profesor de gestión de riesgos en Villanova University. Los eventos de baja probabilidad y alto impacto, como los desastres naturales, la agitación política, la inflación, las pandemias y las guerras, pueden resultar más comunes de lo que la gente piensa y pueden llevarse por delante a las organizaciones.

El impacto de la guerra de Ucrania

¿Qué riesgos desatados por la guerra de Ucrania han impactado más en la organización?



Fuente: Risk in Focus 2023.

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Crisis sistémicas

“Hace más de tres años que estamos en estado de emergencia, incluido el episodio de la guerra de Ucrania. Las crisis se están volviendo sistémicas”, dice Stanislas Martin, Director de Riesgos de EDF. Cuando no es la pandemia, es la guerra, los fenómenos extremos ocasionados por el clima, la escasez energética, la escasez de ciertos alimentos básicos... Todo se convierte rápidamente en una crisis global. Infunden urgencia y mayor sensación de amenaza a todas las áreas de la organización, pero su escala e impacto potencial puede ser tan elevado y complejo que las empresas no pueden resolver estas crisis rápidamente. No tienen el control sobre sus causas.

Tradicionalmente, un equipo de gestión de crisis ayudaba al área corporativa afectada y el equipo de crisis iba rotando según la naturaleza del evento. Pero esta estructura se ha roto: está más allá del alcance de un director de gestión de crisis hacer frente a un estado de emergencia permanente. En muchos sectores, toda la empresa forma parte del equipo de crisis, estén o no preparados para ello, porque una amenaza puede saltar de un área a otra en días, semanas o meses, creando una cadena de subcrisis de diferentes intensidades. *“El nivel acumulado de fatiga y agotamiento de los empleados es un gran problema”,* añade el directivo de EDF.

66

Hace tres años que estamos en estado de emergencia; las crisis se están volviendo sistémicas

Reevaluación del riesgo global

Los problemas han dejado de estar acotados. *“La situación es similar a lo que pasó con la pandemia cuando todos pensaban que sería un problema localizado como el SAR. Pocos se habían preguntado qué sucedería si se rompiera nuestra cadena de suministro global a China y, menos todavía, se habían preparado para esa eventualidad”,* señala Ken Marnoch, vicepresidente de Auditoría Interna de Royal Dutch Shell. La petrolera ha reconsiderado la vieja relación entre crisis y gestión de riesgos y conceptos como el peor escenario posible ahora forman parte del día a día de la gestión de riesgos y del negocio.

La planificación del plan de continuidad de negocio también se plantea a escala global y no por regiones.

66

Los ecosistemas empresariales, con una tupida red de proveedores y partners, hace que las compañías estén más expuestas

Riesgo climático

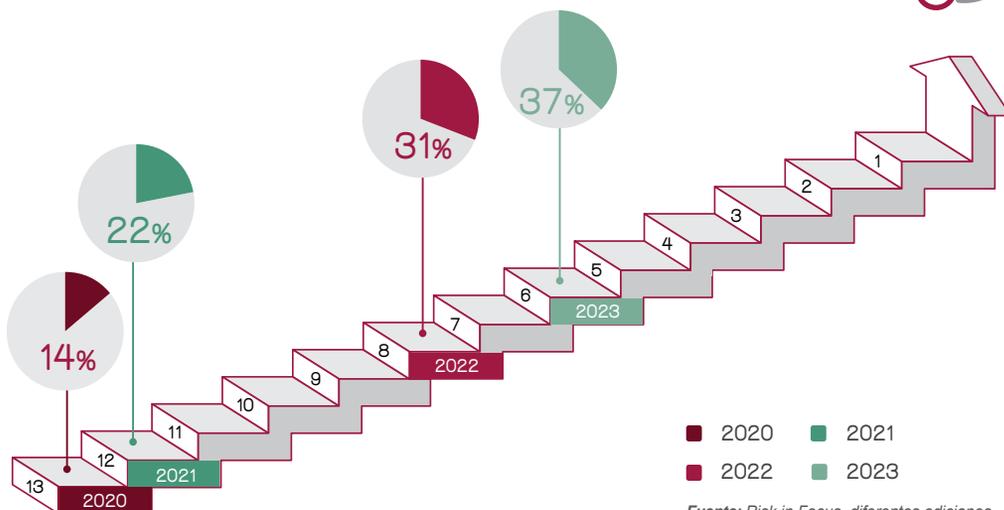


Podría ser la próxima gran crisis para la que las organizaciones no están preparadas. Pese a que el riesgo climático lleva una carrera meteórica y se convierte en el tercer riesgo prioritario en las previsiones a tres años.

El riesgo climático gana peso en la agenda de los auditores internos. Ya están entrando en detalles y comenzando a implementar temas ambientales en cada auditoría. No en vano, se trata del sexto riesgo más importante al que se enfrentan, dos puestos más que en la anterior edición del Risk in Focus. Y las previsiones a tres años apuntan el ascenso del riesgo climático al tercer puesto. Recordemos que en 2020 estaba en la décimo tercera posición.

El clima podría convertirse en la próxima gran crisis para la que las organizaciones no están preparadas⁵. Los auditores internos no le dan aún la prioridad que merece: es el riesgo undécimo en cuando a dedicación de tiempo y recursos. Pero esto está llamado a cambiar⁶.

Riesgo climático y sostenibilidad



⁵ Esfera Consejeros. Riesgo climático: ¿Estamos preparados? 2020.

⁶ Instituto de Auditores Internos de Países Bajos. Climate change and environmental Risk. 2021.

La transición energética y el objetivo de lograr cero emisiones netas va a tener un impacto relevante en muchos sectores. Para Shell, *“la transición energética a las energías renovables tiene una dinámica muy similar a la pandemia y el conflicto en Ucrania”*, dice Ken Marnoch, vicepresidente de Auditoría Interna de Royal Dutch Shell.

Objetivo cero emisiones

En algunas compañías, Auditoría Interna se ha implicado directamente en la supervisión del objetivo cero emisiones netas para 2050, participando desde el principio en el diseño de los controles apropiados y en los reportes de carbono, aportando así seguridad a la Comisión de Auditoría sobre cómo se está desarrollando ese viaje de transición hacia una economía baja en carbono.

El papel de Auditoría Interna en ese proceso de descarbonización es difícil de precisar debido a los diferentes niveles de madurez de las compañías. Más claro es su papel en ayudar a crear conciencia de las iniciativas ambientales, involucrando a los que realmente creen en la agenda climática para que asuman roles y ayuden a crear objetivos de abajo arriba. Esas personas pueden convertirse en sus aliados para implantar las recomendaciones de Auditoría Interna.

Evitar el greenwashing

Pasar de la teoría a la práctica plantea cuestiones delicadas. ¿Cómo se integra la sostenibilidad en el modelo de gobierno para que funcione de forma efectiva y no se convierta en un ejercicio de marcar casillas sobre requisitos regulatorios? *“Existe el riesgo de que haya muchas empresas que sean buenas para comunicar sobre el riesgo ambiental, pero malas para gestionarlo”*, dice un DAI de una empresa de TI. El riesgo de maquillaje o greenwashing se origina en los bajos niveles de madurez de los estándares de información no financiera. Como ocurrió en la crisis financiera 2007/2008, llevará tiempo desarrollar KPIs más rigurosos y comparables.

66

Para abordar los riesgos ESG, Auditoría Interna debe tener un asiento en la mesa y ser escuchada

ESG: empezar por la G

Para los DAIs que participaron en este informe, el enfoque adecuado hacia los riesgos ESG es comenzar por la “G” de Gobernanza^{7,8}. De hecho, el gobierno corporativo y el reporting son la prioridad para los auditores internos en términos de dedicación. *“Se podría decir que la gobernanza es la madre de todas las preocupaciones y todas las soluciones”*, dice un directivo. *“La buena gobernanza proporcionará la transparencia que necesita para protegerse del greenwashing. Y también brinda seguridad a los stakeholders sobre si está en el camino correcto”*⁹.

Para los bancos, la dimensión sostenible es mucho más amplia. *“Las políticas y filosofías de los bancos sobre la financiación de la transición, es decir, con quién hará o no negocios, es fundamental”*, dice John Devine, presidente de la Comisión de Auditoría de Abrdn.

Independientemente de los nuevos desarrollos específicos, cada organización debe tener una estrategia clara que comunicar al mercado. *“Los auditores internos deben asegurarse de que los procesos de control que sustentan estas comunicaciones resuenen en la estrategia central y no estén equivocadas”*, añade. La presión de los accionistas seguirá impulsando la elaboración de informes más precisos.

Las organizaciones que desean abordar el riesgo climático y los riesgos ESG deben otorgar a Auditoría Interna la importancia que necesita para hacer su trabajo: *“debe tener un asiento en la mesa, poder hablar con el director ejecutivo, la Comisión de Auditoría, incluir cuestiones en la agenda y asegurarse de que la voz de Auditoría se escuche y se escuche”*, añade Devine.

“

La gobernanza es la madre de todas las preocupaciones y de todas las soluciones y aportará transparencia para protegerse del greenwashing

“

Existe el riesgo de que haya muchas empresas buenas a la hora de comunicar el riesgo ambiental, pero malas en gestionarlo

⁷ Instituto de Auditores Internos de España. La fábrica de pensamiento. Auditoría Interna y los aspectos ESG. 2021.

⁸ Esfera Consejeros. Riesgos ESG: puntos y preguntas clave. 2022

⁹ Accounting for Sustainability. New proposals for european sustainability reporting standards. Mayo 2022

El riesgo de talento se dispara

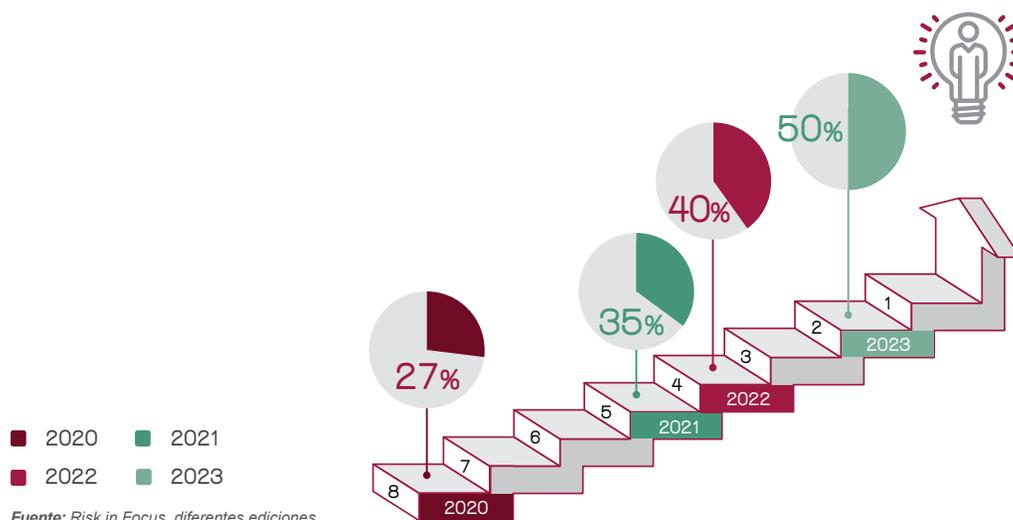


Es el segundo riesgo más relevante. El talento es escaso y exigente en sus demandas de propósito social y flexibilidad. Se requiere un cambio cultural que no todas las empresas podrán abordar.

Desde que llegó la pandemia, las personas son una prioridad. Por cuestiones de salud el capital humano representa una ventaja competitiva ante las dificultades crecientes para captar y retener el talento en un mundo escaso de profesionales con experiencia técnica. La inflación y el descontento social va a añadir más presión: con el aumento de los costes, a las empresas les resultará más difícil retener a las personas clave.

Todo ello explica la meteórica subida del riesgo de talento, que figura en segunda posición en este Risk in Focus 2023. “No poder seguir el ritmo a las expectativas sobre los problemas sociales y el impacto en la cultura organizacional es un gran riesgo, pero las empresas no se están adaptando y necesitan acelerar”, señala. La flexibilidad y el teletrabajo forman parte de esas expectativas¹⁰.

Diversidad y gestión de talento



¹⁰ Microsoft. Great Expectations: Making Hybrid Work Work. 2022

Rotación y evasión

Preocupa la llamada Gran Evasión, empleados que abandonan y evidencian que estamos en una nueva era en la gestión del talento que es clave descifrar, como abordamos en la revista del Instituto¹¹ y recogimos en Esfera Consejeros¹². “Nos preocupa la cantidad de personas con experiencia que abandonan la plantilla, mientras que los más jóvenes permanecen más tiempo en la educación”, señaló Kate Shoemith¹³, directora ejecutiva adjunta de la Confederación de Empleadores de Reclutamiento en el Reino Unido.

Esta combinación de escasez y pérdida de talento abre brechas difíciles de llenar en proyectos clave como la digitalización. “Si tu tecnología no es lo suficientemente buena como para acomodar a 5.000 personas que teletrabajan, estás sentado sobre una

bomba”, dice John Devine, presidente de la Comisión de Auditoría de la gestora Abrdn. “Si está buscando crear un entorno diverso para fomentar el talento, debes enfocarte en que sean capaces y aptos para el puesto. Y eso se verá reflejado en la atención al cliente. Ahora llamo a una empresa, escucho que por el Covid debo esperar 40 minutos para ser atendido y, claro, cuelgo”, añade.

El problema es que muchas empresas quieren volver al mundo prepandemia. Y eso no es posible. Los auditores internos pueden ayudar a las empresas a distinguir entre tendencias cíclicas y cambios más profundos y permanentes. La nueva normalidad implicará retocar, recortar y organizar la cultura corporativa.

66

No poder seguir el ritmo de todas las expectativas en torno a los temas sociales y el impacto en la cultura corporativa es un riesgo enorme

¹¹ Instituto de Auditores Internos de España. Revista. Nueva era en la gestión del talento. Marzo 2022.

¹² Esfera Consejeros. La Gran Evasión (de talento) y sus consecuencias (Febrero 2022), Gestión del talento, el gran desafío empresarial (Marzo 2022).

¹³ ECIA. Risk overview 2022: Human capital, diversity, and talent management. Marzo 2022.

El valor del propósito

¿Cómo puedo crear una organización con corazón? Es la pregunta clave. Los jóvenes buscan empresas cuyo propósito social está alineado con sus propias metas y creencias. Cuando se logra esta sintonía, los resultados son más de dos a cinco veces más, según McKinsey¹⁴. El auge de las empresas sociales refleja ese cambio de prioridades. Pero muchas organizaciones no logran conectar sus valores y propósito con los cambios de la sociedad.

66

El personal quiere estar orgulloso de la gestión y la conducta ética de la organización.

Hoja de ruta para el cambio cultural

No es un proceso rápido, requiere de tiempo. Un primer paso puede ser que Auditoría Interna revise las pautas culturales existentes y utilice los resultados como catalizador para definir la cultura corporativa, con su propia hoja de ruta. Los auditores internos tendrán que enfocarse menos en los números y más en los aspectos cualitativos. Buscar puntos de vista fuera del negocio es clave. Clientes y proveedores tienen a menudo una visión clara de la cultura predominante y pueden aportar gran valor.

La hoja de ruta debe mostrar cómo se integran los comportamientos culturales deseados en los procesos de una organización y si están alineados, con roles y responsabilidades claras, y articulados en todo el negocio. Y, por supuesto, con ejemplo y liderazgo desde arriba. “*El personal quiere estar orgulloso de la gestión y la conducta ética de la organización*”, comentaba un DAI.

Cuando se comprende y objetiva el comportamiento deseado, se pueden incluir en los programas de selección -incluso en la descripción del puesto ofertado-, formación y gestión del talento.

66

El gran desafío es cómo crear una organización con corazón.

¹⁴ McKinsey. *Help your employees find purpose—or watch them leave.* Abril 2021.

Ciberseguridad y protección de datos



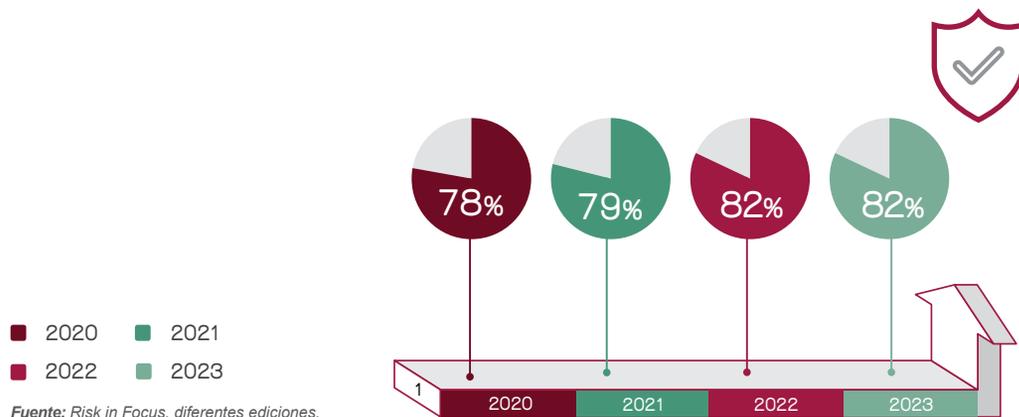
La ciberseguridad es un riesgo permanente, de dimensiones crecientes. La guerra de Ucrania ha disparado los ciberataques tanto a empresas como a infraestructuras críticas para el funcionamiento de la sociedad.

Desde hace años es el riesgo número uno. También para los auditores internos. La guerra de Ucrania ha disparado los ciberataques, sobre todo tipo *ransomware*, que exigen el pago de un rescate para recuperar datos robados.

“Una brecha de datos puede afectar a la calidad del servicio, la confianza, la reputación y nuestras finanzas. Si nuestros clientes pierden dinero, tenemos que compensarlos... Pero lo que más asusta es que no podamos mantener nuestro negocio funcionando”, dice un DAI.

Con la profesionalización del cibercrimen, las empresas deben mantener actualizadas sus estrategias de ciberseguridad¹⁵. Los auditores internos deben participar de ello e impulsar una mayor comprensión y sensibilidad por parte del consejo y sus comisiones delegadas¹⁶. El consejo debe ser muy consciente de las pérdidas económicas que un ciberataque puede ocasionar.

Ciberseguridad y protección de datos



¹⁵ Esfera Consejeros. Ciberseguridad, un riesgo sistémico a vigilar. 2021

¹⁶ ECIIA. GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation. 2019

Ecosistemas empresariales

Los proveedores son una puerta de entrada fácil a las organizaciones: suelen tener sistemas de seguridad menos maduros. Pero sufrir un ciberataque vía un proveedor no exonera de responsabilidad a la organización propietaria de los datos, al menos en la banca. Y eso pasará a otros sectores. Esta inquietud se ha extendido a los proveedores de servicios en la nube¹⁷, aunque ahí las organizaciones no tienen mucho poder de negociación para acordar o imponer controles. Pero el riesgo de terceros es muy relevante y requiere la atención de los auditores internos.

“El negocio necesita alguna metodología para evaluar la salud financiera de los proveedores externos porque el mundo es un lugar muy incierto, especialmente con las presiones inflacionarias y el riesgo de suministro de energía”, dice Greg Schlegel, fundador del Supply Chain Risk Consortium y profesor de gestión de riesgos en Villanova University. Los servidores, esté o no en la nube, siempre necesitarán energía para estar operativos. Que los servidores de Amazon sufran un apagón eléctrico origina graves problemas como ya ha sucedido.

66

La amenaza que más nos asusta es que no podamos mantener el negocio funcionando

66

Es crítico que las organizaciones se aseguren de que tienen personas en diferentes áreas del negocio lidiando con la ciberseguridad

¹⁷ Esfera Consejeros. Supervisión de tecnologías emergentes. 2020

¹⁸ WSWS. Power outage in Amazon's cloud service disrupts technology throughout the United States. 2021; Consejodigital. Un apagón en un data center de Amazon muestra que los datos en la nube no siempre están seguros.

Fusión de delitos

Las taxonomías del cibercrimen también están evolucionando, desde ciberataques que utilizan correos electrónicos para suplantar la identidad y defraudar (phishing), al ciberataque puro de robo de datos para pedir un rescate a cambio. Ahora todo tiende a mezclarse: las tecnologías permiten ataques más sofisticados que combinan varios elementos y delitos en una sola infracción.

“Tradicionalmente, el fraude no se consideró delito económico como el lavado de dinero, el soborno o la corrupción, pero los gobiernos ya los ven como delitos económicos interrelacionados”, dice Ángela Foyle, socia de BDO. Esto exige aplicar una visión holística a la ciberseguridad, implicando a IT, compliance y otras áreas. “Es crítico que las organizaciones se aseguren de que tienen personas en diferentes áreas del negocio lidiando con la ciberseguridad y la protección de datos”, añade Foyle. A su juicio, “los auditores internos deben asegurarse de que esas líneas existen y de que los controles que garantizan una comunicación rápida y clara están correctamente implementados y funcionan”. Lo ideal es que haya algún auditor interno con formación en ciberseguridad y TI. La función debe incluir en los controles alertas y formación para concienciar a la plantilla y que esta adopte prácticas más seguras.

Hay que aplicar los marcos de riesgos con políticas y procedimientos, incluidos ISO 27100, NEST y COBIT, sabiendo que, sin embargo, no es suficiente. *“Podemos tener políticas y*

estándares excelentes de TI, pero el error más simple es que a menudo las personas no las implementan”, dice un DAI. Auditoría Interna puede mitigar las amenazas analizando si las políticas están adecuadamente implementadas, si los parches de software se aplican de manera oportuna y si existen procedimientos de respaldo adecuados. En organizaciones más maduras, su implicación será mayor y más compleja, participando incluso en simulaciones o hacking ético.

Los seguros ante ciberataques son cada día más habituales. Pero ponerle precio a la prima no es fácil. Muchas organizaciones utilizan un proceso de gestión de riesgos para mapear y cuantificar el ciber riesgo, pero al principio solo se avanza a base de prueba y error. Auditoría interna puede ayudar a afinar estos cálculos.

66

Podemos tener políticas y estándares excelentes de TI, pero el error más simple es que a menudo las personas no las implementan.

Digitalización y tecnologías emergentes

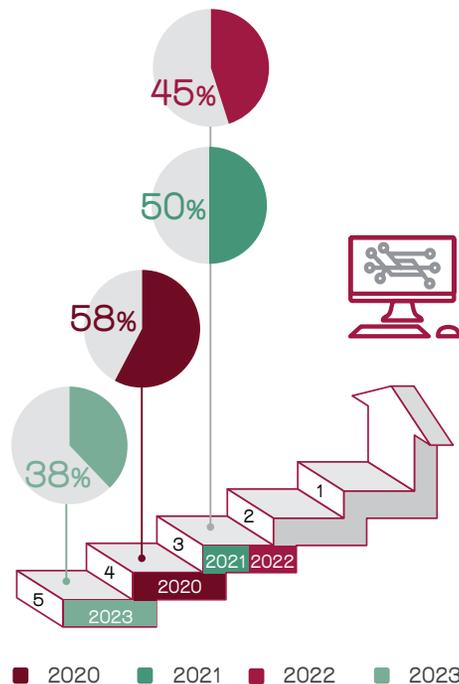


Se está poniendo el foco en la Inteligencia Artificial, pero también es importante asegurarse de que las organizaciones tienen los conceptos básicos correctos para la digitalización que, además, debe estar alineada con la estrategia.

“Más que considerar la digitalización desde un punto de vista técnico, las organizaciones deben familiarizarse primero con la cultura de la innovación para tener éxito. Esta debe fomentar transparencia, flexibilidad, igualdad, colaboración y tener enfoque al cliente”, dice el DAI. Y todo ello, respaldado por una visión estratégica clara, el talento adecuado y la capacidad de ver desde arriba todos los proyectos para asegurarse de que van en la dirección correcta. Una cultura de prueba y error que permita explorar y avanzar.

Auditoría Interna puede ayudar a evaluar y fomentar una cultura de la innovación, sin perder de vista que las metodologías ágiles tienen un alto potencial para originar brechas de datos. Desde un punto de vista práctico, los auditores deberían ayudar a medir cuánto valor financiero crea la innovación. Por ejemplo, calculando las ganancias comerciales en áreas que se están digitalizando o midiendo el aumento de la propiedad intelectual.

Digitalización y tecnologías emergentes



Valoración de datos

Salvo las nativas digitales, las empresas tienen sistemas TI heredados que no están bien integrados y los datos figuran en sistemas separados. *“La fragmentación de los datos es una barrera para la digitalización en cualquier gran organización que no se haya construido sobre una plataforma digital nueva”*, dice Shehryar Humayun, de auditoría interna de Lloyds Banking Group. A su juicio, poner valor monetario a los datos es clave para cambiar de enfoque.

La automatización de procesos (RPA) es una innovación relevante, aunque la experiencia muestra que tienden a inflarse los beneficios y a subestimarse los costes. Es imprescindible desarrollar un marco de gobierno para toda la empresa. Los auditores internos deben tener métricas claras y comprensibles para todas las tecnologías¹⁹.

66

Auditoría Interna puede ayudar evaluando si los esfuerzos de innovación están alineados con los objetivos estratégicos

Cuando la causa raíz son los datos, el riesgo puede manifestarse en muchas formas: riesgo de reputación, de compliance, riesgos operativos, financieros... Clasificar los datos de origen puede mitigar los riesgos. El equipo de Auditoría Interna de Lloyds tiene una sección de analítica avanzada de datos y otra que realiza auditorías temáticas sobre riesgo de datos específicos: privacidad, ética, retención, metadatos, etc. Auditoría Interna tiene una visión holística de la organización y puede enfrentarse de manera práctica a esta realidad de datos fragmentados, además de asegurarse que el riesgo de datos se aborda desde una perspectiva estratégica.

66

La fragmentación de los datos es una barrera clave para la digitalización en cualquier gran organización

¹⁹ Esfera Consejeros: Supervisión de tecnologías emergentes. 2021

Auditar la Inteligencia Artificial

Los más avanzados auditan la Inteligencia Artificial (IA) en la empresa y han comenzado a aplicarla en sus procesos de auditoría, para aprender de los errores y detectar dónde surgen los primeros desafíos.

Auditar la IA exige a los auditados estar preparados para compartir conocimiento con Auditoría Interna y entrar en detalles complejos como los modelos implementados. La certificación de los modelos de IA no tardará en llegar tras el reglamento europeo de IA de 2021²⁰. Se espera que las organizaciones tengan que registrar sus sistemas ante las autoridades y realizar verificaciones periódicas de compliance. Las empresas necesitan proteger los datos, usarlos de manera ética y garantizar que los algoritmos no tienen sesgos de cualquier tipo que puedan dar lugar a riesgos reputacionales, legales o de gestión de talento.

66

No tiene sentido tratar de reinventar la rueda si se pueden personalizar las herramientas de Inteligencia Artificial ya entrenadas por auditores internos.

Análisis predictivo

El análisis predictivo aún resulta complejo y difícil. Con la IA, conviene arrancar con pruebas piloto y seguir avanzando. La independencia de Auditoría Interna no se ve trastocada si se utilizan datos de otros departamentos, pero se deben aplicar parámetros propios a estos datos. *“No tiene sentido tratar de reinventar la rueda si se pueden personalizar las herramientas de Inteligencia Artificial emergentes que ya han sido entrenadas por auditores internos”*, dice Rajesh Singh, Director de Auditoría Interna de la *World Intellectual Property Organisation*. *La Inteligencia Artificial*, bien gestionada, es muy útil, siempre y cuando no se pierda el norte. *“Poner toda nuestra energía en la automatización de sistemas muy sofisticados está bien, pero ¿corremos el peligro de no percibir riesgos de áreas grises que no son tan visibles para la IA?”*

²⁰ Comisión Europea. A European approach to artificial intelligence. 2021

Referencias

- **Instituto de Auditores Internos de España.**
 - La fábrica de pensamiento. Auditoría Interna y los aspectos ESG. 2021.
 - Revista. La guerra de Ucrania dispara el riesgo de terceros. Julio 2022.
 - Revista. Nueva era en la gestión del talento. Marzo 2022.
- **Esfera Consejeros.**
 - Risk in Focus 2022. Edición Consejeros.
 - Riesgos ESG: puntos y preguntas clave.
 - Riesgo climático: ¿Estamos preparados?
 - Ciberseguridad, un riesgo sistémico a vigilar.
 - Cómo supervisar la calidad de la información no financiera.
 - Supervisión de tecnologías emergentes.
- **ECIIA**
 - ECIIA: Risk in Focus 2022 edición europea en inglés.
 - Risk overview 2022: Human capital, diversity, and talent management. Marzo 2022.
 - GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation. 2019.
- **Instituto de Auditores Internos de Países Bajos.** Climate change and environmental Risk. 2021.
- **Accounting for Sustainability.** New proposals for european sustainability reporting standards. Mayo 2022.
- **Microsoft.** Great Expectations: Making Hybrid Work Work. 2022.
- **Mckinsey.** Help your employees find purpose—or watch them leave. Abril 2021.
- **Comisión Europea.** Spring 2022 Economic Forecast: Russian invasion tests EU economic resilience. Mayo 2022.
- **El País.** El BCE acelera y sube los tipos hasta el 0,5% para aplacar la inflación. Julio 2022.
- **Ypulse.** Why The Great Resignation is Happening in Western Europe Too.
- **WSWS.** Power outage in Amazon's cloud service disrupts technology throughout the United States. 2021.



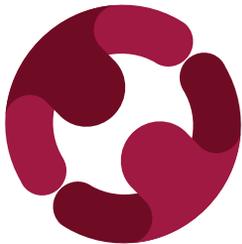
- **Consejerodigital.** Un apagón en un data center de Amazon muestra que los datos en la nube no siempre están seguros.
- **Reglamento General de Protección de datos:** preguntas y respuestas. What is GDPR, the EU's new data protection law?



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

Propiedad del Instituto de Auditores Internos de España. Se permite la reproducción total o parcial y la comunicación pública de la obra, siempre que no sea con finalidades comerciales, y siempre que se reconozca la autoría de la obra original. No se permite la creación de obras derivadas.

Diseño y maquetación: Blondas de Papel S.L.



esfera
consejeros



- 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@iaies



Risk in Focus 2023 es un Informe elaborado por 14 Institutos de la Confederación Europea de Institutos de Auditores Internos (ECIIA), 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