ECONOMIST IMPACT

Reajuste del riesgo: pasar de la reacción a la anticipación

Patrocinado por

IRON MOUNTAIN®

Contenido

Acerca de la investigación y agradecimientos

«Reajuste del riesgo: pasar de la reacción a la anticipación» es un programa de investigación realizado por *Economist Impact* y patrocinado por Iron Mountain que analiza los factores internos y externos cruciales que configuran el enfoque de riesgo de una organización y el papel que desempeñan los ejecutivos, la tecnología y la estructura institucional en la gestión del riesgo. *Economist Impact* usó datos de entrevistas a expertos y de una encuesta llevada a cabo con 656 ejecutivos de sectores clave de Alemania, Australia, Brasil, Canadá, Estados Unidos, Francia, Hong Kong, India, México, Nueva Zelanda, Reino Unido y Singapur.

Queremos dar las gracias a los siguientes expertos por su tiempo y sus conocimientos:

- Simeon Fishman, vicepresidente ejecutivo y CRO de *The Clearing House*
- Sophie Heading, responsable de riesgos globales del Foro Económico Mundial
- Dr. Witold J. Henisz, vicedecano y director docente de la Iniciativa Ambiental, Social y Gobernanza (*Environment, Social, and Governance Initiative*) de la Wharton School

El documento informativo fue elaborado por un equipo de investigadores, editores y diseñadores de *Economist Impact*:

- Mónica Ballesteros — directora del proyecto
- Durukhshan Esmati — jefa de proyecto
- Kathleen Harrington — analista
- Alasdair Ross — escritor
- Amanda Simms — editora
- EMC Design Ltd — diseñador/a

Economist Impact es el único responsable del contenido de este informe. Las conclusiones y opiniones aquí expresadas no reflejan necesariamente los puntos de vista de nuestro patrocinador, socios ni expertos entrevistados.

Prólogo de Iron Mountain

En los últimos tres años, muchas organizaciones han experimentado transformaciones significativas en respuesta a las amenazas emergentes y a los disruptores globales. Esta evolución nos ha obligado a todos a ser más resilientes, dejando atrás las medidas reactivas y adoptando una anticipación proactiva. Al desarrollar resiliencia frente a posibles amenazas futuras, en lugar de limitarse a responder a las ya conocidas, las organizaciones son capaces de adaptarse a riesgos imprevistos y aprovechar las oportunidades emergentes.

Durante más de 70 años, Iron Mountain ha ayudado a clientes de todo el mundo a mitigar los riesgos para su marca, reputación y situación financiera, así como para su capacidad de prestar un servicio eficaz a clientes, pacientes o ciudadanos. Teniendo esto en cuenta, nos complace patrocinar el estudio más reciente de Economist Impact, que explora las cambiantes percepciones de la gestión del riesgo organizativo.

Como descubrirá en este informe, más del 90 % de las organizaciones están haciendo más hincapié en la gestión de riesgos debido a las recientes perturbaciones mundiales y económicas. En cuanto a los riesgos emergentes, el informe destaca la preocupación constante por la ciberseguridad. Otro es la proliferación de tecnologías emergentes, como la inteligencia artificial generativa, por ejemplo, que crea nuevos riesgos y amplía al mismo tiempo la capacidad de los gestores de riesgos para detectar estas amenazas. Aunque la protección de los activos físicos sigue siendo crucial para nuestra organización, reconocemos que ahora todo el mundo es más vulnerable a las ciberamenazas, y hemos avanzado con el mercado para proteger los datos de los clientes en un espacio digital.

Las conclusiones del informe también muestran que los ejecutivos prestan más atención a los riesgos medioambientales que en años anteriores. En lo que respecta a la sostenibilidad, nuestro camino hacia la neutralidad de carbono se centra en reducir el consumo de energía, electrificar nuestros sistemas y vehículos, instalar sistemas de energías renovables y adquirir energía verde para reducir la exposición a la subida de los precios de los combustibles fósiles y las normativas locales sobre emisiones. Al perseguir nuestros propios objetivos medioambientales, sociales y de gobernanza y ayudar a nuestros clientes a alcanzar los suyos, no solo mitigamos los riesgos asociados a la evolución de la normativa, el cambio climático y la desigualdad social, sino que también desbloqueamos nuevas oportunidades.

Nos alientan los resultados de la encuesta, que muestran que los ejecutivos gestionan los riesgos de forma más proactiva y aumentan la resiliencia. Esto mismo es el núcleo de nuestra misión. Los datos de este informe nos ayudan a prepararnos mejor y a preparar mejor a nuestros clientes para el futuro.

Larry Jarvis
Vicepresidente ejecutivo sénior, director de Seguridad de la Información
Iron Mountain

Resumen ejecutivo

La gestión de riesgos está cada vez más integrada en la estructura organizativa y está representada en los niveles superiores. Los gestores de riesgos recopilan datos sobre amenazas potenciales y coordinan la respuesta de la organización. Sin embargo, a medida que esas amenazas evolucionan a un ritmo acelerado, es fundamental que la disciplina avance hacia la anticipación de los riesgos que aún no están en el radar de la organización. Todo ello en lugar de limitarse a responder a los acontecimientos a medida que suceden.

Economist Impact, patrocinado por Iron Mountain, realizó una investigación primaria para comprender cómo perciben los ejecutivos los factores internos y externos cruciales que configuran el enfoque de una organización y el papel que desempeñan los ejecutivos, la tecnología y la estructura institucional en la gestión del riesgo. *Economist Impact* usó datos de entrevistas a expertos y de una encuesta llevada a cabo con 656 ejecutivos de sectores clave (servicios financieros, sanidad y ciencias de la vida, energía y sector público) de Alemania, Australia, Brasil, Canadá, Estados Unidos, Francia, Hong Kong, India, México, Nueva Zelanda, Reino Unido y Singapur.

Los gestores de riesgos están profundizando en cómo los riesgos se propagan en cascada a través de la organización. Por ejemplo, cómo un cierre o una brecha de seguridad en un proveedor potencial podría afectar las operaciones, ingresos y reputación de la organización. La sensibilización sobre el riesgo contingente está aumentando, pero aún hay aspectos para mejorar.

Una gestión de riesgos holística y anticipatoria que responda a las amenazas emergentes debe dirigirse desde la cúpula de la organización, con una respuesta al riesgo sistemáticamente coordinada que cada miembro del personal asuma y acepte como propia. Más allá de la organización, la sensibilización sobre los riesgos debe extenderse a socios, proveedores y distribuidores.

Las tecnologías digitales emergentes, como el *machine learning* y la inteligencia artificial (IA), prometen ampliar las herramientas del gestor de riesgos, detectando patrones en los datos que los analistas humanos podrían pasar por alto. Sin embargo, los atacantes también tienen acceso a estas tecnologías, que podrían usar para encontrar vulnerabilidades o lanzar ataques de *phishing* más persuasivos. Hay que vigilar de cerca estas tecnologías emergentes a medida que se aclaran sus verdaderas implicaciones.

Analizamos cuatro ámbitos en los que la evolución de las prácticas está transformando el panorama de la gestión de riesgos:

Evolución del lugar de trabajo: el personal de una organización es a la vez tu mayor activo y tu mayor vulnerabilidad, lo que se refleja en los esfuerzos y recursos que las organizaciones dedican a atraer, retener y formar a los mismos. La digitalización ha acercado al personal a los procesos críticos, aumentando el riesgo y acelerando el ritmo en el que se manifiesta. Mientras tanto, el aumento del teletrabajo ha hecho que las fronteras digitales de la organización sean más permeables. Atraer y retener al personal también se está convirtiendo en un reto a medida que toda una generación adopta un enfoque del trabajo basado, mayormente, en los valores. Nuestra encuesta sugiere que los gestores de riesgos se mantienen al tanto de estas nuevas tendencias; el 96 % de los encuestados indica que su organización ha desarrollado nuevas políticas y procedimientos de gestión de la plantilla que incluyen, por ejemplo, el trabajo híbrido.

Ciberseguridad y gobernanza de datos: la informática no solo ha respaldado una nueva ola de ganancias en términos de productividad, sino que también ha creado nuevas fuentes de riesgo. La información fluye con más rapidez y amplitud que nunca y, lo que es más importante, con más rapidez que la reacción humana. Con el riesgo contingente, también en aumento por la aparición de organizaciones gigantes, dispersas y multinacionales, proteger la presencia digital de una entidad frente a daños accidentales o malintencionados se ha convertido en una cuestión de supervivencia. El lanzamiento de modelos abiertos de IA generativa ha hecho que aparezca de repente en el horizonte y en la sala de juntas un riesgo muy esperado, pero las repercusiones de esta tecnología naciente siguen siendo difíciles de prever. Los directivos pueden responder mejor a este entorno cambiante, centrándose rigurosamente en tres grandes áreas de riesgo de la informaciím: gobernanza, seguridad y privacidad.

Sostenibilidad: el cambio climático amenaza nuestro futuro, pero sus efectos ya están entre nosotros. Los fenómenos meteorológicos extremos son cada vez más intensos y frecuentes, mientras que la biodiversidad está sometida a una amenaza creciente. También se producen impactos catastróficos en el comercio y las infraestructuras, por lo que las organizaciones se centran en mantener cadenas de suministro diversas y flexibles. Al tiempo que se enfocan en la resiliencia, también reciben presión de las partes interesadas para que ayuden a resolver los problemas subyacentes: agotamiento de los recursos, degradación del medioambiente y emisiones peligrosas. No tomar medidas sobre estas cuestiones podría tener graves repercusiones. Así lo reconoce la mayoría de los encuestados, ya que un 80 % destaca la importancia de los indicadores de riesgo para la reputación.

Eficiencia operativa: mientras las organizaciones se enfrentan a una creciente oleada de riesgos que surgen externamente, los gestores de riesgos deben seguir centrándose en las amenazas más cercanas, ya sean de origen humano, de procesos o de requisitos normativos. Las organizaciones han caído en la trampa de percibir la función de riesgos como un centro de costos que pone trabas a la obtención de lucros. Los gestores de riesgos han mejorado su capacidad para proporcionar a la administración indicadores que equilibren los costos de mantener unas prácticas de riesgo sólidas con las pérdidas potenciales derivadas de un descuido. La forma en que se manifiesta el riesgo operativo varía enormemente entre organizaciones y sectores, pero nuestra encuesta sugiere que los gestores de riesgos de todos ellos reconocen la importancia de invertir en este ámbito.

A pesar de que la disciplina de la gestión de riesgos está evolucionando en sintonía con los cambios del panorama de amenazas, hay desafíos considerables que deben enfrentarse. Entre ellos, se encuentran:

Medición: aunque los costos de implantar un sistema de gestión de riesgos están claros, no ocurre lo mismo con la medición de sus beneficios. Parte del papel de la función es garantizar que las amenazas potenciales no se materialicen, pero evaluar el costo de algo que no ha sucedido es problemático. Y si bien la inversión es inmediata, los beneficios pueden acumularse a lo largo de los años, lo que aumenta el reto de la medición. La clave está en establecer parámetros que vinculen los riesgos a objetivos organizativos mensurables.

Recursos: las organizaciones tienden a financiar la función de riesgos para reflejar el panorama del pasado en lugar de equiparla para prepararse para el futuro. En un momento en el que surgen nuevos riesgos y los antiguos evolucionan, esto suele dejar la gestión baja en fondos, con falta personal y, potencialmente, poco cualificado.

Coordinación: una función de riesgos con visión de futuro, eficiente y resiliente requiere una sensibilización y coordinación únicas en toda la estructura corporativa, más que en las funciones tradicionales aisladas. También, requiere tanto un liderazgo descendente como una colaboración y ejecución ascendentes, y debe ir más allá de la organización para incluir a los socios, proveedores y otras partes interesadas.

Introducción

No hay certezas en el funcionamiento de las organizaciones. La posibilidad de que algo vaya mal dentro de cada organización y en cada punto de su cadena de valor está siempre presente. Desde la recesión de mercados clave hasta la interrupción de suministros críticos, pasando por las acciones malintencionadas de un empleado descontento, los riesgos difíciles de prever o evitar suponen un obstáculo para los resultados y objetivos de las organizaciones. Los daños pueden variar desde una molestia menor hasta la quiebra y penas de cárcel en casos extremos.

Enfrentar estas amenazas es una disciplina sofisticada y de evolución rápida. Se complica por el hecho de que los riesgos cambian con el tiempo en intensidad, naturaleza y ámbito. Durante e inmediatamente después de la crisis financiera de 2008-2009, el riesgo de quedarse sin crédito era una preocupación latente. Durante la pandemia de la COVID-19, la atención se centró en la continuidad de las actividades, ya que los confinamientos forzosos obligaron a las organizaciones a cerrar sus puertas. Cuando los tanques rusos entraron en Ucrania en 2022, las restricciones en el suministro mundial de alimentos y combustible dispararon los precios y perturbaron las cadenas de suministro.

El auge de formas de tecnología cada vez más avanzadas y fácilmente accesibles, combinado con el hecho de que el teletrabajo está cada vez más extendido y arraigado, ha introducido un nuevo nivel de riesgo. Los límites geográficos de las organizaciones se han ampliado, pasando de oficinas centralizadas y construidas para tal fin a los áticos, estudios y jardines residencias privadas, a menudo a muchos kilómetros de la sede central y con frecuencia en un país diferente. Proteger los procesos y los datos confidenciales en un entorno tan disperso es doblemente difícil, ya que convierte a cada empleado en un punto potencial de filtración o sabotaje.

Economist Impact, patrocinado por Iron Mountain, ejecutó una investigación primaria para comprender cómo perciben los ejecutivos los factores internos y externos cruciales que configuran el enfoque de una organización y el papel que desempeñan los ejecutivos, la tecnología y la estructura institucional en la gestión del riesgo. *Economist Impact* usó datos de entrevistas a expertos y de una encuesta llevada a cabo con 656 ejecutivos de sectores clave de Alemania, Australia, Brasil, Canadá, Estados Unidos, Francia, Hong Kong, India, México, Nueva Zelanda, Reino Unido y Singapur.

Gestión de riesgos — tendencias y percepciones

La gestión de riesgos evolucionó como disciplina para hacer frente a la transformación de las amenazas. Se ha ido introduciendo gradualmente en la estructura de una organización, involucrando a más personas y recursos (aunque, al parecer, nunca los suficientes) a un nivel mayor. La responsabilidad del riesgo suele recaer en el consejo de administración, con gestores de riesgos (CRO) dependen directamente del Director Financiero (CFO) o del Presidente Ejecutivo (CEO). Al mismo tiempo, los gestores de riesgos se ven menos como jefes de una división separada y más como coordinadores de actividades repartidas por toda la organización. La responsabilidad del riesgo y de informar sobre él a los niveles superiores de la cadena suelen recaer en los jefes de sección, mientras que la función de riesgos proporciona orientación, recoge datos y recomienda medidas correctivas a la alta dirección.

El camino desde que el riesgo era un elemento apenas reconocido hasta la actual arquitectura de riesgos en toda la empresa ha sido largo. La concienciación del riesgo como una preocupación organizativa existencial surgió en la segunda mitad del siglo pasado, pero los primeros directores de riesgos no se nombraron hasta la década de 1980. Esta función no se consideró una respuesta dominante al riesgo hasta los primeros años de este siglo. Hoy en día, la gestión de riesgos se reconoce como una competencia clave de la alta dirección. Cuatro de cada cinco organizaciones representadas en nuestra encuesta afirman haber invertido en equipos de gestión de riesgos para toda la empresa como parte de su enfoque táctico de la disciplina.

Nuestra investigación sugiere que aún queda por hacer, aunque los altos directivos de riesgos son cada vez más sofisticados en la comprensión de la disciplina. Por ejemplo, se está pasando de reaccionar a los riesgos cuando surgen a anticiparse a ellos y crear capacidad de resiliencia en la organización antes de que se produzcan daños. La identificación del riesgo ha aumentado en importancia para más del 90 % de los encuestados desde 2020, al igual que la creación de modelos predictivos de riesgos para casi el mismo número. El enfoque en la anticipación se extiende a la reformulación de la organización con ese fin. Ahora, el 28 % afirma buscar una mayor capacidad para identificar y anticiparse a las amenazas, mientras que el 41 % declara anticiparse a los riesgos mediante la vigilancia de las amenazas emergentes y la identificación de anomalías en los procesos. Este cambio de enfoque no es sorprendente, dada la sucesión de conmociones que han sorprendido a los directivos de las organizaciones en las últimas décadas.

Además, las organizaciones también se enfrentan a la interconexión del riesgo. Un acontecimiento adverso en una parte de la organización, o del

mundo, puede afectar a todo el funcionamiento de múltiples maneras. El cierre de un proveedor clave a causa de una catástrofe natural puede provocar retrasos en la producción y un aumento de los costos al tener que buscar suministros alternativos. Aunado a ello, puede llevar a pérdidas de ingresos al retrasarse o no completarse los pedidos y un golpe para la marca y la reputación de la organización al circular la noticia de la interrupción. A partir de un único riesgo externo, toda la organización se ve arrastrada a la gestión de crisis. Anticiparse a estas amenazas contingentes es un elemento clave de la gestión moderna de riesgos.

Una vez más, las organizaciones están progresando, pero hay margen de mejora. Sophie Heading, responsable de riesgos globales en el Foro Económico Mundial, explica que «se aprecia mejor la conectividad entre riesgos, pero aún está evolucionando. Con un poco de imaginación, la repercusión de los acontecimientos en un lado del mundo puede servir para prever un riesgo potencial en otro. La falta de esta visión puede hacer que la organización sea susceptible a los riesgos derivados de estos acontecimientos».

Simeon Fishman, vicepresidente ejecutivo y director de riesgos de *The Clearing House*, cree que cada vez se presta más atención a los riesgos emergentes, es decir, riesgos que están menos definidos y son menos aparentes. «Ahora es más crítico para las organizaciones conseguir una mayor visibilidad en el horizonte e intentar comprender mejor estos riesgos» — explica. «Una de las áreas cruciales del riesgo emergente es el tecnológico, que evoluciona continuamente. Por ejemplo, solo unos pocos proveedores ofrecen servicios en la nube, que tiene el potencial de dar lugar a una concentración de información en ellas. Una organización centrada en la tecnología, a través del software que usan o desarrollan, puede poner, sin querer, todos sus esfuerzos en una sola posibilidad».

En esta transición de una gestión de riesgos reactiva a una proactiva, los directivos cuentan con la ayuda de un conjunto emergente de herramientas digitales, como reflejan las respuestas a nuestra encuesta, en la que el 43 % de los ejecutivos afirmó utilizar tecnologías cognitivas e IA para gestionar el riesgo. Sin embargo, aunque el cambio es el pan de cada día de los gestores de riesgos, llevarlo a cabo al ritmo que estamos observando los cambios en la IA es muy desafiador. Está claro que el *machine learning* ofrece una nueva forma de interrogar los datos que entran y salen de una gran organización, ayudando a los analistas humanos a detectar patrones que ellos no verían. No obstante, también puede convertirse en un vector de ciberataques, ya que los hackers y estafadores usan la tecnología para potenciar su programación. Lo cierto es que aún es demasiado pronto para saber cómo evolucionará esta tecnología y cuál será su impacto neto en la gestión de riesgos.

La tecnología solo puede llevarte hasta cierto punto si no cuentas con el diseño, la arquitectura de riesgos o la información adecuados en tus sistemas. También es fundamental comprender cómo están conectados los procesos empresariales y la información. Una vez establecidos el diseño y la información, se pueden aprovechar las herramientas de análisis e interrogación de la misma para lograr una mayor comprensión del riesgo en una organización.

Simeon Fishman, vicepresidente ejecutivo y director de riesgos de *The Clearing House*.

La necesidad de anticipar los riesgos y sus repercusiones en toda la organización en una época de rápidos cambios tecnológicos subraya la importancia de adoptar un enfoque holístico de la gestión de riesgos. Confiar en reaccionar a las amenazas, una vez que se materialicen, deja a las organizaciones desprevenidas y con dificultades para ponerse al día. Centrarse por separado en cada área de las operaciones expone a la organización a riesgos contingentes. La respuesta no consiste simplemente en recurrir a tecnologías innovadoras. Adoptar ciegamente la innovación deja a las organizaciones expuestas a amenazas nuevas e imprevistas. La Sra. Heading advierte de que «la tecnología permite gestionar los riesgos, pero tiene que conjugarse con el elemento humano».

El enfoque holístico de la gestión de riesgos requiere un liderazgo desde arriba y una coordinación en toda la estructura organizativa para poner toda la información disponible en conocimiento de quienes están mejor situados para interpretarla y actuar. El Dr. Witold J. Henisz, vicedecano y director docente de la facultad *Environment, Social and Governance Initiative* (Iniciativa Ambiental, Social y de Gobernanza) de la Wharton School, coincide con esta afirmación. Él añade que «hacer que los datos sean comprensibles, transparentes y fáciles de entender es extremamente importante cuando se reúne a personas con diferentes conocimientos de datos y antecedentes funcionales».

Como sugiere la etiqueta «holística», la gestión de riesgos se está convirtiendo en responsabilidad de toda la organización (y de sus proveedores, socios y distribuidores). Los gestores de riesgos aplican y coordinan el sistema, pero, a diferencia del director de marketing o del director de operaciones, no es una competencia reservada exclusivamente a ellos. La gestión de riesgos ha pasado de ser un cargo incrustado en algún lugar del organigrama a convertirse en un elemento integral de la cultura organizativa, junto con su marca, su declaración de misión o su enfoque del desarrollo y la retención del capital humano. Incluye compromisos en toda la organización, como una declaración de tolerancia al riesgo, una característica cada vez más común de las

organizaciones modernas que define el nivel de riesgo aceptable y su actitud general a la hora de asumir riesgos.

La coordinación entre las distintas unidades de la organización, su cadena de suministro ampliada y las principales partes interesadas son el centro de este enfoque. Muchos gestores de riesgos de alto nivel son defensores de este enfoque en sus organizaciones, como muestra nuestra encuesta. Entre los encuestados, el 77 % está de acuerdo en que la gestión de riesgos debe tener en cuenta todas las partes de la organización, mientras que el 46 % afirma haber invertido en equipos de gestión de riesgos para toda la empresa. Otro 36 % considera prioritario integrar la gestión de riesgos en la estrategia global de la organización y en la toma de decisiones.

Esto requiere «cambios estructurales que varían de acuerdo al tipo y el tamaño de la organización», según Fishman. «La comunicación desde la alta dirección y el CEO a todos los niveles inferiores se vuelve más crítica para garantizar que la gestión de riesgos forme parte del ADN de toda la organización y no sólo sea una función creada que asuma la responsabilidad especial de impulsar la gestión de riesgos».

No obstante, los ejecutivos siguen sin alcanzar la situación ideal. El 57 % señala que su organización necesita mejorar la colaboración interfuncional. Sólo el 4 % de los ejecutivos encuestados declaró tener un comité de gestión de riesgos directamente responsable de impulsar tal gestión, mientras que el 27 % afirmó que su CEO/presidente/socio es directamente responsable. Más del 60 % de los encuestados cree que su organización necesita mejorar el compromiso de los empleados y el intercambio de información entre funciones, equipos y socios externos.

Gestión de riesgos en los cuatro pilares

Por su naturaleza, el riesgo es difuso. Incluso cuando las fuentes están claras (algo poco frecuente), la ruta que sigue el riesgo (por dónde entra en la organización y cómo viaja a través de ella) es difícil de predecir. En esta sección, examinaremos cuatro manifestaciones distintas del riesgo organizativo, realizaremos un seguimiento de sus efectos y exploraremos cómo los abordan los directivos. Los cuatro pilares son:

- Evolución del lugar de trabajo
- Ciberseguridad y gobernanza de datos
- Sostenibilidad
- Eficacia operativa

Evolución del lugar de trabajo

Una organización es poco más que el grupo de personas que reúne para llevar a cabo su misión. Sus diversos talentos se combinan para convertir los insumos en resultados de mayor valor. Con toda razón, muchas empresas valoran mucho sus recursos humanos e invierten dinero y esfuerzo en atraerlos, formarlos y retenerlos. Sin embargo, junto con sus habilidades y energía, los humanos vienen acompañados de imprevisibilidad y tendencia a cometer errores. Los riesgos relacionados con las personas son algunos de los más difíciles de gestionar por tres razones. En primer lugar, median en todos los procesos que una organización ejecuta con o sin tecnología, por lo que los riesgos que plantean se manifiestan en todas partes. En segundo lugar, están sujetos a los impulsos humanos, lo que lleva a un rendimiento impredecible en comparación con el de una máquina. Por último, la relación entre las organizaciones y su personal está evolucionando y el trabajo a distancia es cada vez más habitual; por ello, lo que prevalece hoy puede ser diferente de lo que será mañana.

Las personas siempre han sido la mayor fortaleza y la mayor vulnerabilidad de las organizaciones, pero los últimos sucesos han agravado los riesgos. La transformación digital de las últimas décadas ha impulsado la productividad en general. No obstante, también ha acercado a los empleados a procesos de misión crítica y datos valiosos. Debido a esta proximidad, el personal descuidado o malintencionado puede causar más daños que nunca. Recientemente, la pandemia de la COVID-19 obligó a una profunda y repentina transformación de muchos entornos laborales, dejando a las organizaciones sin personal en un momento crucial y apresurándose a establecer sistemas de trabajo en línea. Esto también planteó a las organizaciones un nuevo desafío de gestión, como explica Fishman. «Es posible que no tengamos el mismo conocimiento de las funciones y responsabilidades de todo el mundo — conocer los comportamientos de cada uno y algunas vulnerabilidades de riesgo es más difícil con el trabajo a distancia», afirma.

A medida que la pandemia va remitiendo, las organizaciones se dan cuenta de que la actitud de sus empleados hacia el trabajo ha cambiado, quizá de forma permanente. Al personal actual no suele entusiasmarle la idea de volver a la oficina, mientras que los posibles nuevos empleados esperan que el teletrabajo sea la norma. Las organizaciones también han experimentado una escasez de mano de obra, en parte por las repercusiones sanitarias a largo plazo provocadas por la pandemia, pero también por una tendencia apodada «la gran renuncia», provocada por una confluencia de factores como la protesta contra los lugares de trabajo tóxicos.

En el futuro, los cambios generacionales en las actitudes y expectativas de los empleados, incluida una creciente priorización de valores como la diversidad, la sostenibilidad y la justicia social, harán más difícil atraer y retener al personal. El salario en sí no será suficiente. Esto amenazará con crear un desajuste entre las cualificaciones necesarias en un entorno tecnológico en rápida evolución y la disponibilidad y la voluntad de los candidatos en el mercado. Las organizaciones pueden verse operando con un déficit de competencias, lo que perjudica la productividad y aumenta el riesgo de que se produzcan errores y actos malintencionados.

Reajuste del riesgo: pasar de la reacción a la anticipación

Como en otros ámbitos del riesgo, no todas las organizaciones están al día de los avances, aunque muchas sí. Las más innovadoras están trasladando oficinas para adaptarse a la nueva realidad, más descentralizada. Los resultados de nuestra encuesta muestran que el 94 % de las organizaciones ha diversificado su enfoque de la oficina física y el lugar de trabajo; por su parte, la pandemia ha impulsado al 45 % de ellas a hacerlo en los últimos tres años. En un mismo orden de ideas, el 96 % de los encuestados indicó que su organización ha desarrollado nuevas políticas y procedimientos de gestión de la plantilla, incluido el trabajo híbrido. Las empresas también están evaluando las necesidades de talento para un mundo laboral cambiante, lo que incluye la función de riesgos. Las principales organizaciones están «estudiando el modelo de dotación de personal dentro de su negocio para asegurarse de que cuentan con gestores de riesgos tecnológicamente competentes», afirma Fishman. «El papel de los expertos en materia tecnológica de riesgo y recuperación es fundamental, como los expertos en la nube y la IA».

Las empresas también están recopilando más datos sobre cuestiones relacionadas con la mano de obra y desarrollando procesos más sistemáticos para gestionar la contratación y la retención. Nuestra encuesta corrobora esta afirmación, ya que la mitad de los encuestados afirman estar aprovechando más datos para ello, con un número ligeramente superior declarando que desarrollaron una reserva de talento.

Ciberseguridad y gobernanza de datos

El entusiasmo de las organizaciones por las tecnologías de la información ha transformado sus operaciones. De los viejos tiempos de instalaciones centralizadas con ejércitos de trabajadores supervisados por directivos austeros en estrictas jerarquías, las organizaciones han pasado a ser más flexibles, ágiles y mucho más productivas, gracias, en gran medida, a la digitalización. Las computadoras, la automatización e Internet han alterado profundamente los modelos de trabajo y futuros avances como la computación cuántica, el omnipresente Internet de las Cosas y el metaverso prometen cambios igualmente fundamentales.

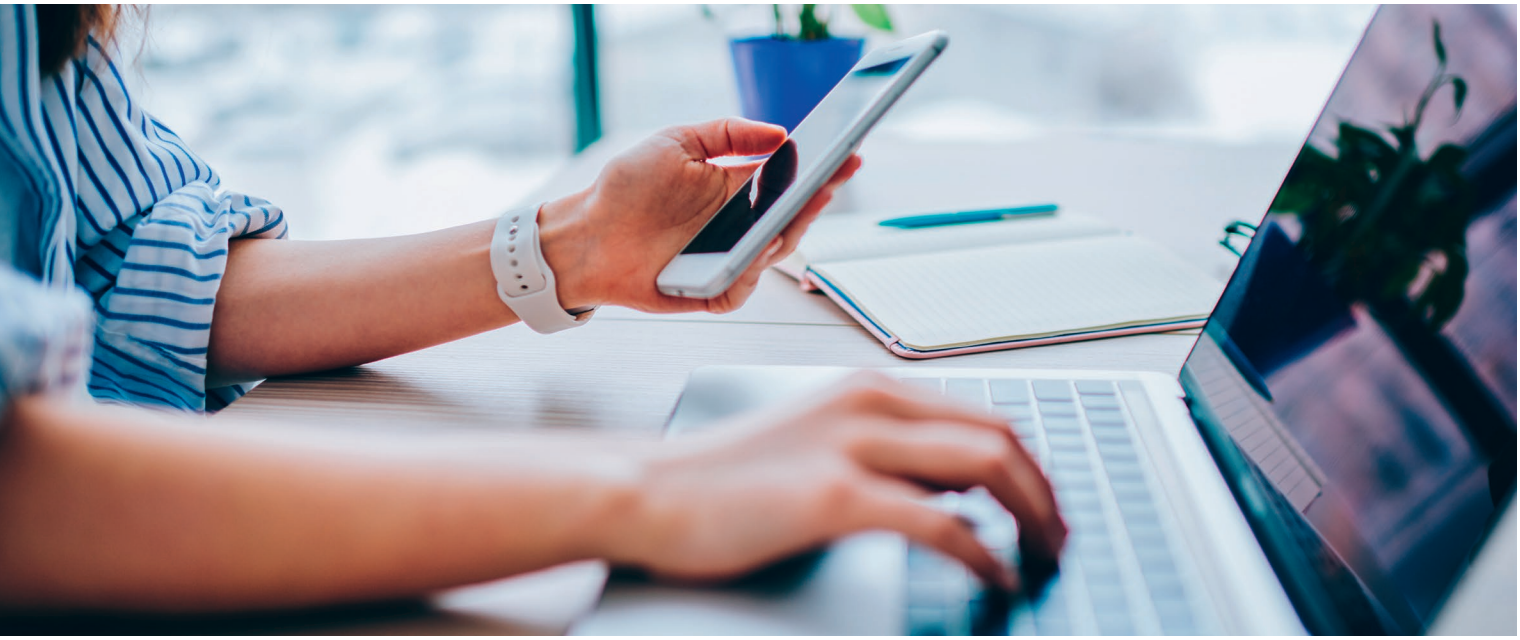
En términos generales, la revolución digital ha tenido un triple impacto en la gestión de riesgos de las organizaciones: los riesgos surgen de forma más repentina y se propagan con mucha más rapidez; los datos, su almacenamiento, transmisión e interpretación, se han convertido en un ingrediente valioso de las operaciones; y, si bien la digitalización ha creado nuevas áreas de riesgo, también ha dado lugar a nuevas herramientas para afrontarlos.

Cuando la información viaja a la velocidad de la luz a través de una red digital global, las cosas cambian más rápido de lo que un ser humano puede reaccionar. Como las computadoras toman cada vez más decisiones por los humanos, los procesos pueden avanzar a través de numerosas iteraciones antes de que se detecte un error o un resultado no deseado. Con clientes, socios y consumidores conectados a los medios de comunicación globales, la reputación de una marca puede encontrarse frente al tribunal de la opinión pública antes de que los ejecutivos de la organización hayan asimilado plenamente lo que está ocurriendo.

Referente a la IA generativa, estamos viendo surgir un nuevo riesgo cibernético potencial. El ritmo de su adopción ha dejado tras de sí a la sociedad, y los responsables políticos y reguladores — y los pioneros creadores de la tecnología — con un gran esfuerzo para mantener el ritmo. Los gestores de riesgos no saben a quién recurrir para recibir el mejor asesoramiento en esta fase inicial de lo que podría resultar tan disruptivo para los modelos empresariales como lo fue Internet. «¿Quién tiene experiencia en riesgos en relación con el camino hacia donde se dirige la IA generativa?» — se pregunta Fishman. «¿Qué métodos sofisticados podemos adoptar para controlar mejor la concentración de información en la nube? Teniendo en cuenta cómo cambia el panorama cibernético, ¿cómo podemos seguir integrando la resistencia en nuestras infraestructuras y procesos?».

Este ámbito plantea cuestiones urgentes y retos complejos a los gestores de riesgos y los negocios. En esos momentos, empezar por lo básico es un buen punto de partida. Sigue siendo primordial que las organizaciones se centren en tres áreas de riesgo principales a la hora de gestionar sus activos digitales:

- Gobernanza de datos: garantizar la exactitud, la coherencia y la accesibilidad de la información.
- Seguridad de los datos: proteger la información del acceso, el uso, la divulgación, la alteración, la modificación o la destrucción no autorizada.
- Privacidad de los datos: proteger la privacidad de las personas, controlando cómo se recopilan, utilizan y comparten sus datos personales.



Los mismos principios de proactividad y exploración del horizonte siguen vigentes, pero con más urgencia que antes. Del mismo modo, garantizar el cumplimiento es aún más difícil en un panorama normativo tan cambiante e incierto, pero no por ello menos vital.

Los resultados de la encuesta indican que las organizaciones han mostrado dedicación y coherencia en sus esfuerzos por mitigar los riesgos relacionados con los datos y la ciberseguridad a través de diferentes medidas. En los últimos tres años, el 49 % de las organizaciones invirtió en planes de recuperación en caso de catástrofe/continuidad de la actividad para sistemas digitales y el 48 % invirtió en servicios/almacenamiento en la nube y supervisión y prevención continuas de riesgos y amenazas cibernéticas. Durante el mismo periodo, el 46 % de los ejecutivos encuestados también han informado de inversiones en talento de TI y ciberseguridad, y en formación informática/técnica.

Mientras tanto, los gestores de riesgos deberían interesarse por la evolución de la IA, no sólo como fuente de riesgo, sino también como medio para mitigarlo. El 43 % de nuestros encuestados destaca que usa tecnologías cognitivas e IA en los procesos de gestión de riesgos. Si se entrena y dirige adecuadamente, la IA puede identificar patrones extraños, identificar tendencias, trazar escenarios y detectar áreas de riesgo que los analistas humanos podrían no ver.

Pocas organizaciones están libres de riesgos cibernéticos, pero algunos sectores son más propensos que otros. Por ejemplo, tanto el sector sanitario como el financiero recopilan enormes cantidades de datos confidenciales de los clientes. Sacar el máximo partido de esta información, sobre todo para calcular el riesgo para el cliente o la organización, sin dejar de protegerla, es una tarea gigante. Los costos del fracaso pueden ser devastadores. No es de extrañar que, entre todos los sectores, el sanitario fuera el que mayor porcentaje de encuestados obtuvo, con un 83 %, lo que indica la creciente importancia de los indicadores tecnológicos en los últimos tres años. Entre ellos, el tiempo de actividad de la red, los incidentes de ciberseguridad y los errores de software.

El sector energético también se basa en los datos para racionalizar sus operaciones, mientras que el Estado moderno se apoya en gran medida en la información de los ciudadanos para prestar servicios públicos con la máxima eficiencia. En el caso de los gobiernos, los costos de reputación de un fracaso pueden ser especialmente perjudiciales, ya que enfrentan directamente a los políticos y sus partidos con quienes votan por ellos.

Sostenibilidad

La industrialización le ha aportado a la humanidad ventajas que hubieran resultado inimaginables para nuestros antepasados preindustriales. Sin embargo, al quemar combustibles fósiles para impulsarla, hemos puesto en peligro la sostenibilidad de nuestro estilo de vida — y nuestras propias vidas. Los gases de efecto invernadero (GEI) liberados a la atmósfera, en gran parte debido a nuestra actividad económica, están elevando la temperatura media mundial. Los efectos serán potencialmente catastróficos en las próximas décadas, pero no tenemos por qué esperar tanto. Aumentan los fenómenos meteorológicos extremos, sube el nivel del mar y la biodiversidad está bajo amenaza.

Esto afecta a las organizaciones de dos maneras. Primeramente, las operaciones y las cadenas de suministro son vulnerables a las perturbaciones provocadas por fenómenos meteorológicos extremos y otros efectos medioambientales difíciles de prever. Los sucesos de los últimos tres años han hecho que el 47 % de las organizaciones encuestadas se centre en mantener redes de cadenas de suministro diversas y flexibles. En segundo lugar, las partes interesadas de las organizaciones, desde los clientes a los inversionistas, pasando por los empleados, esperan, con razón, que las entidades hagan lo que les compete a la hora de abordar el agotamiento de los recursos, la degradación del medio ambiente y las emisiones de GEI.

Por ahora, la segunda es más urgente para los gestores de riesgos (aunque la primera es una amenaza creciente). Los grupos activistas señalan rápidamente a los que consideran infractores atroces de las prácticas sostenibles, con un arsenal cada vez mayor de medios creativos para llamar la atención del público. Las empresas petroleras y energéticas, y los inversionistas y bancos que las financian, han sido objeto de ataques continuos. Estas campañas pueden perturbar directamente el funcionamiento de las empresas, pero pueden tener un impacto más serio al socavar la reputación de una organización y su «licencia social» para operar.

La importancia de los indicadores de riesgo de reputación entre los ejecutivos ha aumentado en los últimos años debido a la creciente complejidad de los entornos operativos y a la necesidad de que las empresas sean más transparentes, rindan cuentas y sean socialmente responsables. Un significativo 80 % de los encuestados determinó que los indicadores de riesgo de reputación eran los más cruciales en cuanto a la importancia creciente para la supervisión de riesgos.

Al igual que ocurre con la ciberseguridad, la sostenibilidad y las áreas asociadas de política social y gobernanza (ESG – Política Ambiental, Social e de Gobernanza) constituyen un panorama de riesgos en rápida evolución. La preocupación por el medio ambiente ha ganado protagonismo en la agenda pública y las organizaciones responden emitiendo declaraciones en las que anuncian sus credenciales «verdes». No obstante, estas declaraciones se suelen tachar de «*greenwashing*» o «ecoblanqueo» e insuficientes para proteger a las organizaciones de la indignación pública. Las declaraciones de intenciones ecológicas se sustituyen cada vez más por promesas de lograr «cero emisiones netas» de gases de efecto invernadero, acompañadas de rutas que muestran cómo se conseguirá.

Para las grandes empresas, esto ya no es suficiente. Los ciudadanos presionan para que las empresas y el sector público adopten una postura «positiva para la naturaleza» y las organizaciones se ven obligadas a presentar planes para devolver el medio ambiente a su estado preindustrial o, al menos, para que los indicadores climáticos vuelvan a situarse dentro de límites compatibles con una economía sostenible. Heading apunta a «un cambio en la gestión de riesgos, que ha pasado de observar únicamente el cumplimiento normativo, en concreto, de ser un mero ejercicio burocrático, a una función mucho más estratégica, que incorpora valores sociales como ESG».

Nuestra encuesta refleja el hecho de que ESG figura actualmente en los registros de riesgos de las organizaciones. Casi la mitad de las organizaciones encuestadas dedicó más recursos a las iniciativas ESG, mientras que un número similar se centró en la elaboración de informes de rendimiento ESG — exigidos por los reguladores en algunas jurisdicciones.

Eficiencia operativa

Lo más familiar para las organizaciones y sus gestores de riesgos son sus operaciones internas. La mayoría puede hacer poco para influir en lo que pasa al otro lado de sus paredes, físicas o virtuales, pero lo que ocurre dentro está, en su mayor parte, bajo su control directo. Ya sean las personas, los procesos o los requisitos normativos, la eficacia del funcionamiento interno de una organización es la diferencia entre el éxito y el fracaso. Y está plagado de riesgos: el personal puede no rendir como se espera, verse defraudado por los equipos de los que depende o caer en la vulnerabilidad de los procesos diseñados para hacerlos colectivamente productivos.

La protección frente a tales riesgos ha sido una característica central de la gestión de riesgos desde los primeros días de esta disciplina. Como tales, los gestores de riesgos pueden caer fácilmente en la vieja percepción de ser poco más que un policía interno que pone obstáculos a otros departamentos. Por tanto, la función de riesgos llega a considerarse un centro de costos y una carga para el impulso emprendedor de las verticales «lucrativas». Esta percepción era (y, a veces, sigue siendo) una piedra en el zapato para los gestores de riesgos, pero las cosas están cambiando. Los gestores de riesgos han mejorado en la medición de los costos de los fallos operativos y su comparación con el costo de mantener una función de riesgos adecuada. En comparación con la suspensión de las operaciones para restablecer un proceso defectuoso, una considerable sanción reglamentaria por gestionar mal los datos de los clientes o la pérdida de negocio debido a un fallo ético que ha salido a la luz, el costo de una función ágil de gestión de riesgos es menos molesto.

No hay dos organizaciones iguales, por lo que no existe un modelo para lograr la eficiencia operativa. De hecho, lo que se entiende por «operaciones» puede variar mucho dentro de una misma empresa y entre ellas. El sector energético se centra en los equipos y procesos, ya que la perforación petrolífera o la extracción de minerales requieren mucho capital y sus fallos pueden provocar catástrofes humanas y medioambientales. El sector financiero tiene muchos datos y es vulnerable a los fallos de su personal por incumplimiento ilegal de políticas y funciones, mala ejecución, falta de formación y comportamiento poco ético. Esto puede dar lugar a pérdidas directas, así como a costos reglamentarios, jurídicos y de reestructuración. El cumplimiento de la legislación y la normativa es especialmente importante, lo que se complica por el hecho de que muchos bancos e instituciones financieras operan en múltiples jurisdicciones legales. Otros sectores varían en el enfoque de su gestión del riesgo operativo — uno de los muchos factores que complican el trabajo de los gestores de riesgos.

La encuesta refleja la importancia del riesgo operativo para las organizaciones, con una clara sensación de que la inversión en este ámbito mejora el rendimiento y los resultados financieros. En particular, el 42 % de los encuestados señala una mejora del rendimiento

derivada de la aplicación de buenas prácticas de gestión en la planificación de instalaciones y espacios físicos de trabajo. Un porcentaje similar señala una mejora significativa de la eficiencia operativa de su organización. Sin embargo, dos tercios de los encuestados reconocen que se trata de una apuesta a largo plazo y que la inversión en gestión de riesgos perturba las operaciones a corto plazo.

Henisz afirma que es fundamental reconocer la conexión entre inversión y rendimiento. «Podemos monetizar el impacto del riesgo calculando los días de parada y la producción perdida», afirma. «Traducir los datos al lenguaje de las finanzas o las operaciones es valioso. De lo contrario, la función de gestión de riesgos sólo se verá como un costo mientras todos los demás generan ingresos».

Desafíos para la gestión de riesgos

La profesión de la gestión de riesgos se ha hecho más influyente y sofisticada con el tiempo y está integrada en la cultura y la estructura de la mayoría de las grandes organizaciones. A pesar de eso, su papel y sus metodologías están sometidos a una presión continua para mantenerse al día en un entorno de riesgo en constante cambio. Se ha tendido a considerar suficiente una estrategia de riesgo capaz de afrontar todas las amenazas registradas en el pasado, pero el pasado suele ser un mal indicador de cómo se manifestará el riesgo en el futuro. En respuesta, la gestión de riesgos debe evolucionar constantemente a medida que aparecen nuevas amenazas y disruptores. En particular, la profesión debe seguir avanzando desde la reacción a la anticipación, creando resiliencia frente a las amenazas venideras en lugar de limitarse a responder a las ya conocidas.

A este respecto, la encuesta muestra algunos avances, pero sugiere que aún queda mucho por hacer. Una abrumadora mayoría de los ejecutivos encuestados confía en que las iniciativas de gestión de riesgos aplicadas por sus organizaciones sean suficientes para mitigar o prevenir los daños derivados de los mismos. Esto apunta a un exceso de confianza por parte de las organizaciones que podría dejarlas más expuestas de lo que piensan. Para subsanar este déficit potencial, hay que centrarse en tres áreas principales: medición, recursos y coordinación.

Medición

El seguimiento de los resultados en la gestión de riesgos es intrínsecamente complicado. Si se produce un fallo en ellas, los costos incurridos pueden imputarse al programa de riesgos. Esto parece claro, pero determinar qué porcentaje de los costos debe asignarse a la función no es nada sencillo. La gestión de riesgos crediticio es aún más difícil cuando las cosas van bien. Existe la tendencia a considerar que esto no es más que «lo de siempre» y a negar por completo la contribución de los gestores de riesgos. Incluso cuando se hace algún esfuerzo por reconocer el mérito de la función, resulta difícil cuantificar lo que debe introducirse en la columna «positivo».

¿Debe esperarse que la función de riesgos contabilice las inversiones realizadas en previsión de riesgos que nunca llegaron a materializarse? ¿Debería responsabilizarse de los cisnes negros (difíciles de predecir, pero que retrospectivamente parecían inevitables) que no superaron el umbral de atención? Tras la crisis financiera mundial de 2008-2009, considerada en general como un cisne negro, la disciplina del riesgo (incluidas las agencias de calificación crediticia) se vio sacudida hasta sus cimientos. Sin duda, la crisis crediticia fue un indicio del fracaso en la comprensión y gestión de riesgos, pero los errores políticos y la imprudencia pública también tuvieron parte de la culpa. En tales circunstancias, es difícil llevar a cabo una contabilidad forense de los resultados de tal gestión con una mínima pretensión de precisión.

La gestión de riesgos también comparte la dificultad experimentada en muchas áreas operativas de justificar la inversión a corto plazo para obtener beneficios a largo plazo. «Inviertes en algo hoy y puede que no veas la compensación hasta dentro de cinco o diez años, o puede que la veas dentro de tres meses», dice Heading. «Dependiendo de lo que se intente controlar, puede ser muy difícil articular ese tipo de costo-beneficio, de forma que los ejecutivos lo entiendan fácilmente».

Los ejecutivos reconocen los retos que plantea la medición de los resultados de la gestión de riesgos. Alrededor de tres cuartas partes de los encuestados coinciden en que la falta de parámetros de evaluación normalizados para medir el riesgo dificulta la demostración de los avances.

«Es esencial establecer parámetros que vinculen los riesgos a los objetivos de la organización y garantizar que estén claros, desde el trabajo sobre el terreno hasta el consejo de administración y la dirección ejecutiva», afirma Fishman. «Las herramientas pueden ayudar, pero la estructura de medición de los riesgos directamente ligados a las actividades y su impacto es fundamental. Es necesario no sólo observar el impacto, sino comprender los factores causales. Por ejemplo, aunque medir los cibereventos es importante, igual de importante es medir la eficacia con que los procesos y sistemas corrigen las vulnerabilidades y garantizan la continuidad de los negocios».

Recursos

Pocos departamentos se consideran adecuadamente financiados, pero el caso de los gestores de riesgos es particularmente sólido. Esto se debe en parte a que las organizaciones tienden a financiar la función para reflejar el panorama de riesgos del pasado en lugar de equiparla para prepararse para el futuro. El alcance y complejidad de los riesgos a los que se enfrentan las organizaciones no han dejado de aumentar a medida que las cadenas de suministro se alargan y racionalizan y que la tecnología acelera el ritmo del cambio. Del mismo modo, las organizaciones pueden recurrir a un conjunto cada vez mayor de herramientas para supervisar los riesgos y aumentar la resiliencia, pero exigen un gran desembolso inicial y, como ya se ha dicho, el calendario y la magnitud del rendimiento de la inversión son difíciles de cuantificar.

Los encuestados reflejan la sensación de que los departamentos de riesgos carecen de recursos suficientes. Los ejecutivos creen que los recursos financieros, tecnológicos y humanos de su organización dedicados a la gestión de riesgos son insuficientes, y casi dos tercios afirman que su organización necesita mejorar en esta área.

Parte del reto consiste en que, a medida que las organizaciones se vuelven cada vez más digitales, los gestores de riesgos deben tener un ámbito de conocimientos más amplio. Esto significa que, incluso para mantener un nivel constante de protección, las organizaciones deben gastar más para atraer los conjuntos de aptitudes necesarios para la función de gestión de riesgos. «Los gestores de riesgos son un producto de primera necesidad», afirma Fishman. «Incluso con los despidos masivos en los sectores financiero y tecnológico, es difícil encontrar buenos gestores de riesgos».

Con avances como la inteligencia artificial, la automatización y la robótica acaparando toda la atención, es probable que esta situación empeore. Junto con el acercamiento de tecnologías como la computación cuántica y la tecnología de registro contable distribuida a escala, no habrá lugar para la complacencia en el sector de la gestión de riesgos en un futuro previsible.

Coordinación

Como hemos comentado, un requisito fundamental de la gestión de riesgos en los próximos años será la capacidad de llevar la mentalidad del riesgo a todos los rincones de la empresa. Los flujos ascendentes del proceso de información deben coordinarse en toda la organización, y los gestores de riesgos deben implementar las normas y herramientas que tienen que utilizar todos los departamentos y empleados. El liderazgo general (*Top-down leadership*) debe marcar la pauta para que el papel central de la creación de resiliencia frente a amenazas conocidas y desconocidas impregne la cultura organizacional. Hay que incluir en la red a socios, proveedores y clientes, ampliando el radar de riesgos de la organización mucho más allá de sus paredes. Todo el aparato de gestión de riesgos debe centrarse en lo que ocurre en la organización día a día, pero también, y de forma crítica, en lo que podría ocurrir en el futuro dadas las tendencias emergentes. Las organizaciones con más éxito serán aquellas en las que este esfuerzo esté diseñado y coordinado por gestores de riesgos de alto nivel, dotados de los conocimientos y recursos que exige un entorno en rápida evolución y con el apoyo de los más altos ejecutivos.

La trayectoria de la gestión de riesgos aún no ha concluido, pero la dirección que toma es prometedora.

Conclusión

La gestión de riesgos ha recorrido un largo camino desde su primera manifestación como función organizativa diferenciada. Ha pasado de ser una disciplina limitada principalmente a la banca, donde la solución consistía en construir colchones financieros más generosos para garantizar la liquidez durante la evolución adversa de los mercados, a una pieza central de la gestión moderna. Los gestores de riesgos ocupan un lugar destacado en organizaciones de todos los sectores, tanto públicos como privados. Captan y cuantifican las amenazas a través de una amplia gama de factores, que surgen tanto dentro de la organización como más allá de sus paredes, donde hay menos visibilidad y control. La gestión de riesgos se ha adoptado en niveles cada vez más altos de la organización y muchos gestores de riesgos operan hoy en día en la alta dirección (*C-suite*), con acceso al CEO o al consejo de administración. Esta ha sido la dirección adoptada durante algunas décadas, y la función sigue integrándose cada vez más.

Aunque están surgiendo nuevos retos y los antiguos se están transformando a medida que la tecnología, la geopolítica y el cambio social afectan al entorno operativo. La gestión de riesgos siempre ha sido una disciplina dinámica, pero la necesidad de cambio es cada vez más urgente. Este nuevo siglo ha arrojado una sucesión de problemas globales. Desde la crisis financiera mundial de 2008-2009 y la subsiguiente crisis de confianza en la democracia liberal, hasta la pandemia de la COVID-19 y la invasión rusa de Ucrania, los movimientos tectónicos en los asuntos mundiales han multiplicado la incertidumbre. Esto ha sucedido en el contexto de una transición iniciada desde hace tiempo, pero que se acelera hacia un panorama digital, así como de preocupaciones medioambientales que afectan a las empresas, la sociedad, la política y la economía mundial.

La aceleración de la adopción digital, ejemplificada por la aparición de grandes modelos lingüísticos generativos preentrenados, conlleva tanto promesas como amenazas. A pesar de que promete crear una nueva generación de herramientas para ayudar a las organizaciones a controlar y responder a los riesgos, acarrea la amenaza de dotar a los agentes maliciosos de armas igualmente innovadoras para robar o corromper datos valiosos. Los nuevos modelos de trabajo, en particular el crecimiento del teletrabajo, amplían y disuelven la primera línea digital de la organización, abriendo nuevas vías a las ciberamenazas.

Los gestores de riesgos prosiguen el viaje emprendido hace décadas, incorporando a toda la organización un enfoque de las operaciones basado en el riesgo. Se enfrentan a la naturaleza cada vez más contingente del mismo, donde un suceso en un rincón remoto de la cadena de suministro puede producir ramificaciones imprevistas en otros lugares.

También, están pasando de una actitud reactiva a una proactiva. El primer enfoque se centra en aumentar la resiliencia frente a las amenazas previstas y responder a ellas cuando se materializan. En este último, los gestores de riesgos dedican recursos y esfuerzos en el análisis del horizonte en busca de amenazas no reflejadas en el registro de riesgos, preparándose para escenarios que pueden parecer improbables y se consideran un alto potencial de daño.

Reajuste del riesgo: pasar de la reacción a la anticipación

En la constante transformación del panorama actual de riesgos, más amplio, variable y complejo que nunca, adoptar un enfoque proactivo puede ser la medida más eficaz que la disciplina de gestión de riesgos puede adoptar para prepararse para el futuro.

ECONOMIST IMPACT

LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

900 Third Avenue
New York, NY 10022
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com