

Risk Management

LA CLAVE...

Y TRES LÍNEAS DE REFLEXIÓN

Con motivo de la puesta en marcha del proceso de certificación de los risk managers, no está de más recordar algunos principios básicos que sientan la base de un Risk Management competente. Añadiremos algunas líneas de reflexión que pueden hacer de caldo de cultivo para la puesta en marcha de una gestión sistemática de los riesgos. El Risk Management es una misión de gran relevancia dentro de cualquier organización, pero como en cualquier misión importante se impone una visión previa. El presente artículo tiene como objeto desarrollar esta visión en proceso de evolución.



FRANÇOIS SETTEMBRINO
GERENTE DE RIESGOS
FERMA

Hace más de medio siglo, los inventores del *Risk Management* se aventuraron a establecer las bases del sistema. No existía nada sobre la materia y les hizo falta valor para salir de los tópicos. Lo más difícil fue perder la costumbre de considerar únicamente materia prima los riesgos asegurados o asegurables. El tiempo

les ha dado la razón, ya que los «nuevos riesgos» percibidos a lo largo del tiempo no están asegurados en su totalidad y algunos incluso no lo están de ninguna manera.

Vamos a centrar nuestra atención en algunos principios en torno a los cuales, desde el punto de vista de los pioneros, se articula ineludiblemente el éxito del *Risk Management*:

- El *top management* tiene que involucrarse desde el principio hasta el fin del proceso que hay que implementar. Él es el que tiene la iniciativa y proporciona los recursos adecuados y a él le corresponde mantenerlo. Se trata de un proceso tan vital que no se puede desatender y dejar a su libre albedrío ya que hay que alimentarlo constantemente para lograr que sobreviva.

- En función del tamaño de la empresa, de su sistema organizativo, de su localización geográfica, de sus objetivos y de sus procesos operativos, el *Risk Management* estará más o menos centralizado.

- Para simplificar, en la bibliografía al uso se habla casi siempre de *risk manager*. En realidad, convendría más hablar de la entidad de *Risk Management*, ya que en las organizaciones de gran tamaño no basta con involucrar a una sola persona. Partiendo de esta idea, seguiremos utilizando el término de *risk manager* para facilitar la comprensión.

- Hay que encontrarle un sitio en la estructura empresarial. Los pioneros han entendido rápidamente que, desde el momento en que los integraban en el organigrama de la empresa, por ejemplo, en el departamento financiero, perdían toda libertad de acción. Por ello, optaron por una función *staff*, la única



ILLUSTRATION STOCK

que les permitía relacionarse de forma completamente autónoma con el *top management*. Lo que sorprende hoy en día es que este puesto era fácil de lograr... antaño. Pero en la actualidad pocas empresas lo tienen en cuenta. Lo que descoloca a muchos dirigentes es el hecho de tener que tolerar que, en su propia organización, alguien tenga el derecho y la obligación de formular críticas y advertencias. Este planteamiento entra en conflicto con el egocentrismo larvado o incluso conquistador que se produce con frecuencia en las altas esferas.

■ Había que investir a los ejecutantes de cierta autoridad para que pudieran actuar. Por tanto, nuestros pioneros debían tener derecho a informarse a todos los niveles de la organización y a obtener respuestas a todas sus preguntas. Desde el principio, ya se sabía que el estudio de muchas problemáticas abarcaba varias disciplinas al mismo tiempo y que la mejor manera de abordarlas era formando grupos multidisciplinares bajo la supervisión del *risk manager*. En ambos casos, al margen de las conclusiones de sus investigaciones o de sus discusiones, éstas se sometían al *top management* o al *board*, que tomaba las decisiones o que encomendaba tareas adicionales. Por supuesto, son ellos los que toman las decisiones importantes dado que, en lo referente al *Risk Management*, son los dirigentes los que dirigen, y son ellos los que tienen que asumir las responsabilidades.

■ Uno de los papeles encomendados al *risk manager* o a la entidad de *Risk Management* es el de encargarse de la formación interna sobre la materia. Cuando esta tarea se ejercía sobre los cuadros de alto nivel, generalmente no planteaba ningún problema. Como

LO QUE DESCOLOCA A MUCHOS DIRIGENTES ES EL HECHO DE TENER QUE TOLERAR QUE, EN SU PROPIA ORGANIZACIÓN, ALGUIEN TENGA EL DERECHO Y LA OBLIGACIÓN DE FORMULAR CRÍTICAS Y ADVERTENCIAS

hemos dicho anteriormente, ellos habían puesto en marcha el proceso y conocían y admitían de entrada toda la importancia que revestía. Los profesionales del día a día estaban más familiarizados con los verdaderos problemas y solicitaban al mismo tiempo información y formación, demostrando, por tanto, un gran interés. Los más refractarios eran por lo general los que ocupaban un puesto en el *middle-management*, bloqueados entre sus objetivos y el mayor rendimiento posible. Por lo tanto, estos últimos son los que había que controlar más de cerca, con seminarios y boletines informativos. Asimismo, las tecnologías, en evolución continua, han brindado un gran apoyo al respecto. Una de las consecuencias indirectas consistía en la obligación del *risk manager* y de su equipo de formarse continuamente y sin pausa, para no quedarse atrás.

Si eliminamos cualquiera de los elementos citados anteriormente, resulta prácticamente imposible sentar los cimientos de un verdadero *Risk Management*, y es precisamente esto lo que ha ocurrido. Cuando los pioneros han abandonado el terreno han sido esporádicamente sustituidos por homólogos. Los equipos directivos empezaron a interesarse únicamente por el precio de mercado de su organización, las fusiones y absorciones han suscitado el interés de los inversores y se ha prestado mucha menos atención a los riesgos, ya que todo se centraba en las operaciones financieras. Los riesgos seguían estando presentes, a pesar de que los dirigentes se hacían los sordos y los ciegos, riesgos que todos recuerdan. Desde Enron hasta Fukushima, pasando por las *subprime*, la lista es desastrosa e increíblemente larga e impresionante.



Ahora hay que invertir a toda costa el proceso y volver a las buenas costumbres, como en los comienzos. Los esfuerzos encaminados a certificar esta función van en el buen sentido. Asimismo, será necesario volver a formar a los dirigentes porque nada será posible sin ellos. Queda mucho por hacer.

Cada organización es «una» y, por lo tanto, única. Por ello, no hay ni habrá nunca un modelo único de *Risk Management* que se pueda aplicar en todos los casos, hacia y contra cualquier circunstancia. Partiendo de los principios anteriormente expuestos, que constituyen el esquema de una «clave» correctamente estructurada, cada organización tendrá que adaptarlos a su plantilla, a sus procedimientos, a sus limitaciones financieras, políticas y geográficas, así como a su propia cultura. Es un proceso a largo plazo que no tiene fin y que hay que plantearse y replantearse constantemente. Por esta razón, la profesión de *Risk Manager* es apasionante.

**NO HAY NI HABRÁ
NUNCA UN MODELO
ÚNICO DE RISK
MANAGEMENT QUE
SE PUEDA APLICAR
EN TODOS LOS
CASOS, HACIA Y
CONTRA
CUALQUIER
CIRCUNSTANCIA**

Por otro lado, resultará útil estudiar las posibilidades de formación y las disponibilidades para evitar un alto grado de dispersión.

Veamos ahora tres ejemplos que pueden servir de líneas de reflexión y facilitar una mayor comprensión de los fenómenos que se producen. Cada una de estas líneas reflexivas merecería, para llegar a ser exhaustiva, un análisis en profundidad con la dedicación de especialistas en la materia. Los siguientes párrafos no tienen esta ambición, pero pueden suscitar interés y servir, en cierto modo, de introducción o incitación para investigar más ampliamente.

- Para empezar, analicemos el concepto de ciberriesgo. De manera constante se están produciendo ataques en todo el mundo, no sólo a empresas y entidades diversas, sino también a cada uno de nosotros. Nosotros, pequeños individuos insignificantes, somos víctimas de ataques en la misma medida que las grandes organizaciones, ya sea para seguir la pista de nuestros hábitos de compra, de nuestras relaciones íntimas, de nuestra situación financiera, de nuestras relaciones bancarias. Todo, en definitiva. Y esto se produce entre la mayor indiferencia. Casi todo el mundo conoce los peligros de las redes sociales, pero casi todos nos acomodamos y provocamos riesgos que descubriremos demasiado tarde. Por no mencionar a las empresas o a los gobiernos, ya que todos los días descubrimos que ninguno ha sido capaz de implementar protecciones suficientes ni eficaces. El ingenio de los delincuentes es tal que siempre llevan ventaja en lo relativo a la sofisticación de sus víctimas. Su ventaja llega a tal extremo que son capaces de instalar en secreto un dispositivo permanente en el interior de los ordenadores que han intervenido, lo que les permite estar al tanto de todo lo que pasa en

ellos y tienen la opción de elegir el momento o la víctima de un ataque sorpresa. ¿Hay que quedarse de brazos cruzados? De ningún modo, antes al contrario, hay que verificar de forma permanente los mecanismos de defensa, ya que darse cuenta de una intrusión con rapidez a menudo permite reaccionar con más celeridad. La formación de los usuarios es primordial, ya que hay que evitar que se cansen y que olviden las normas de seguridad que ralentizan su trabajo. No se trata en absoluto de un fenómeno puramente informático. Desde que existe el teletrabajo, la confusión frecuente entre trabajo y redes sociales, la proliferación de tarjetas inteligentes, las puertas de acceso se encuentran donde menos lo esperamos y los documentos confidenciales son a veces tan poco secretos que conseguirlos es demasiado fácil. Nos encontramos en una esfera típica del *Risk Management*, donde el problema debe ser analizado entre todos y donde el *top management* tiene que preocuparse por la estrategia a adoptar y las acciones a desarrollar. Todo el mundo conoce la existencia de las *backdoors* que han sido previstas subrepticamente en los sistemas operativos de cualquier ordenador. Cualquiera que tenga las claves puede entrar en ellos. Google, Outlook y compañía no son tampoco una excepción. Pero hay cosas mucho peores, como la entrega anónima del *darknet*. Este facilita la comunicación a escondidas de cualquier ordenador que vigile, espíe o intercepte las comunicaciones. Ha tenido gran acogida por parte de los internautas censurados, demandados o simplemente frustrados por algunos poderes despóticos. Es la única manera que tienen de contar lo que les ocurre y comunicar con libertad. Pero también se trata de una ganga para todas las redes mafiosas, que pueden ejercer sus actividades con total impunidad. Hasta ahora, este



darknet ha sido impenetrable y los cifrados han sido infranqueables. Lo más trágico de este rompecabezas es que va a dejar obsoleta una parte de los espionajes famosos que se han realizado con una gran complejidad técnica y de los que acabamos de tener noticia en multitud de titulares. Ir por lana y volver trasquilado... Pero en este campo, los riesgos se han convertido en incontrolables porque no conseguimos dar con quienes han alimentado el *darknet*, ni lo que sucede a espaldas de todos: secretos de fabricación, inventarios de cualquier tipo, clientes, proveedores, productos estratégicos, etc... No sabemos aún cómo poner freno a esto, pero... habrá que hacerlo. Aunque, ¿quién se encargará de ello? *That is the question.*

● La segunda línea de reflexión reside en la atención que hay que prestar al capital humano y a las «personas» que lo componen.



**EL RISK
MANAGEMENT DEL
OTRO LADO DEL
ATLÁNTICO HA IDO
INCORPORANDO
TÍMIDAMENTE EN EL
PROCESO LA
PREOCUPACIÓN DE
LOS STAKEHOLDERS,
ESTO ES, «LAS
PARTES
INTERESADAS»**

Este capital está a menudo infravalorado o maltratado. Resulta curioso haber confiado su suerte a los especialistas de «recursos humanos». Esta terminología se parece demasiado a los demás recursos de las empresas, como las materias primas, las energías, las subcontrataciones, etc... Si es muy caro, o complicado o muy difícil de manejar, lo cambiamos todo. Por esto mismo, al personal se le trata como al carbón: si es muy caro, lo sustituimos o lo desplazamos a otros lugares, sin tener en cuenta los problemas humanos que pueden derivarse de ello. Prueba de ello son las Bolsas, que han reaccionado sin piedad, siempre a favor de cualquier reestructuración/externalización. Es entonces cuando el responsable de recursos humanos deja de ser el vínculo entre la dirección y el personal para convertirse en un mero ejecutor de las grandes obras, y deberá apañárselas para que esto cueste lo menos posible, con planes so-

ciales que son como entierros. ¿Para qué preocuparse por el personal y protegerlo con arreglo a la normativa y la legislación, si externalizándolo o subcontratándolo podemos ahorrarnos todas esas limitaciones tan onerosas?

El *Risk Management* del otro lado del Atlántico ha ido incorporando tímidamente en el proceso la preocupación de los *stakeholders*, a saber, «las partes interesadas». Estas incluyen principalmente al personal, pero también a los sindicatos, a los clientes, a los socios, a los proveedores, a los contratistas y subcontratistas, inversores y acreedores, sin olvidar el fisco o el medio ambiente. Además de las que se han citado, ya numerosas de por sí, se encuentran también los competidores. Todos ellos, o cada uno en particular, pertenecen a diferentes clases de vulnerabilidad, como las expectativas de las personas, las pérdidas de información, las pérdidas de recursos, los daños materiales, etc. Todos ellos merecen atención y cuidados permanentes. Son muchos los medios para hacerles frente. Si reflexionamos sobre ello, nos damos cuenta rápidamente de que esta segunda línea recorre todo el tejido empresarial y, además, la gobernanza vuelve a ocupar la posición de responsabilidad que no tendría que haber abandonado nunca. A raíz de ello, el *Risk Management* se está familiarizando de nuevo con los principios de precaución y prevención. Sólo podemos hacer prevención teniendo en cuenta los riesgos que tienen una probabilidad mensurable, mientras que la precaución sólo puede aplicarse cuando no se puede calcular la amplitud ni la probabilidad del evento. Cualquier *risk manager* tiene que navegar de uno a otro y, cuando se estanca, sólo le queda la capacidad de resistir... Resulta relevante que la legislación belga del bienestar haya ampliado sus hori-

zontes, pasando de abarcar los accidentes laborales a cubrir también los asuntos organizativos, de relación, de acoso, y entrar así también en el área psicosocial. Más revelador aún es el hecho de que el asesor responsable sólo pueda relacionarse directamente con la cúspide de la empresa, sin intermediarios, y que en su función no tenga que someterse a nadie más. Ocuparse de este modo del capital humano de la empresa es un ejemplo legal y obligado del modo según el cual el *Risk Management* debería funcionar, accediendo directamente a la cúspide de la empresa.

● La tercera línea de reflexión es un nido de víboras ya que abarca todo lo referente a la «reputación», esta cara aparente de la imagen de marca. Todos los manuales lo dicen: este valor es irremplazable y hay que protegerlo y defenderlo adecuadamente. Pero es tan frágil que un simple rumor puede deteriorarla y hay que reconstruirla, una tarea ardua y a veces imposible. En las mentes de mucha gente sigue sembrándose la pequeña o gran sospecha de que «cuando el río suena, agua lleva...». El problema lo constituye el hecho de que los dirigentes siguen siendo por lo general los protagonistas, pero también los más vulnerables. Se trata de un aspecto ineludible de buena gobernanza, que destaca de igual manera el papel clave que desempeña el concepto de *Risk Management*. Volviendo la vista atrás, el caso *Perrier* es representativo de cómo las cosas pueden deteriorarse. La contaminación del agua se gestionó bien gastando mucho dinero en reclamar cantidades industriales de botellas, pero ha sido la actitud errática de los administradores la que ha provocado más daños a la imagen de marca, y, consiguientemente, el valor de marca de la firma se ha desmorona-

OCUPARSE DEL CAPITAL HUMANO DE LA EMPRESA ES UN EJEMPLO LEGAL Y OBLIGADO DEL MODO SEGÚN EL CUAL EL RISK MANAGEMENT DEBERÍA FUNCIONAR: ACCEDIENDO DIRECTAMENTE A LA CÚSPIDE DE LA EMPRESA

do y ésta ha sido comprada a buen precio por otro grupo.

Lo que hace que la gestión de este riesgo sea prácticamente imposible en la actualidad es el hecho de que los dirigentes falsean el mensaje. En 1976, Emmanuel Todd emitió el juicio siguiente con respecto al bloque del este: «...una sociedad especializada en la que la técnica ya no está al servicio del bienestar y de la seguridad de sus ciudadanos no puede perdurar...». Sin embargo, es exactamente lo que ocurre hoy en día bajo el falaz estandarte de la globalización, que hace que todo esté permitido: se da lugar a una esclavitud larvada mediante la externalización; la invasión de todos los productos, sobre todo los de la industria agroalimentaria, con aditivos y compuestos cuyo peligro y nocividad se ven infravalorados o incluso negados; el retroceso de la biodiversidad; el *efecto invernadero* incontrolado... No faltan ejem-



plos, pero se están comenzando tímidamente a tratar gracias a algunos valientes a quienes todavía no han conseguido silenciar. Los más conocidos son la piscicultura, el artificio de la cadena alimenticia, desde los productos falsos, como el queso artificial, hasta la sustitución de carnes en los circuitos de platos preparados, los complementos alimenticios cuya inocuidad está por demostrar pero cuyos efectos perniciosos se deben en gran parte a la omnipresente comida basura, etc. Los grandes grupos industriales, que son los principales responsables de estos monstruosos desajustes, no tienen miedo absolutamente a nada. Son tan potentes que organizan ellos mismos su propia impunidad. A los medios que emplean se les llama *lobbies*, sin escrúpulos, todo con tal de que rinda el mayor beneficio, científicos sinvergüenzas, mentiras omnipresentes, todo ello para alimentar simultáneamente y de forma artificial las

LO QUE HACE QUE LA GESTIÓN DEL RIESGO DE REPUTACIÓN SEA PRÁCTICAMENTE IMPOSIBLE EN LA ACTUALIDAD ES EL HECHO DE QUE LOS DIRIGENTES FALSEAN EL MENSAJE

opiniones que se desacreditan entre sí. Las autoridades sanitarias están inundadas de teorías tan contradictorias que ya no desempeñan su papel de perro guardián. ¿Cómo quieren aplicar los principios del *Risk Management* en un contexto como éste? Si la ética de los industriales no vuelve a ser la de antes, es decir, honesta y transparente, ¿por qué quieren que se corrijan los riesgos que ellos mismos han creado y que atraen fortunas, y cuyos efectos nocivos se dejarán ver mucho más adelante?

Dejemos la última palabra a Stéphane Foucart, ya que expresa muy bien el creciente desasosiego de los que creen en el *Risk Management*: «...se duda de los conocimientos acumulados que son discutidos mediante simulacros de metodología científica o manipulados por las industrias a las que molestan... El proyecto científico consiste en comprender el mundo, si bien el proyecto técnico consiste en sacar partido de él...»¹. Sin embargo, desde que podemos someter la ciencia a la técnica marcamos las cartas, provocando con ello la desaparición de la idea de principio de precaución. No se trata de que un diagnóstico científico se interponga en cualquier actividad industrial. La industria se las arreglará para hacerlo desaparecer entre la confusión seudocientífica artificial, fábrica de incertidumbre y de ignorancia. ¿Podrá el *Risk Management* hacer frente a este desafío? El tiempo nos dará la respuesta. |

¹ La Fabrique du Mensonge. Comment les industriels manipulent la science et nous mettent en danger. [La Fábrica de la Mentira. Como los industriales manipulan la ciencia y nos ponen en peligro.] Stéphane Foucart, éd. Denoël Impacts, 2013, páginas 17 y 18.

