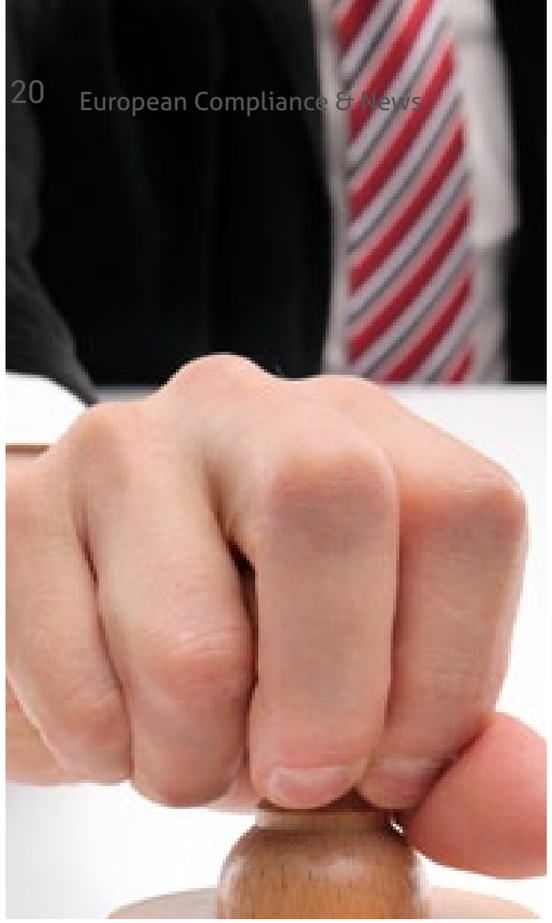


El análisis y la gestión de los riesgos conforme a ISO 31000:2009

Francisco Menéndez Piñera
CEO de Contein XXI y de SIGEA

El análisis y la gestión de los riesgos conforme a ISO 31000:2009

El análisis de riesgos de una organización se ha convertido, en los últimos años, en uno de los aspectos más importantes de la gestión de las organizaciones.

La aparición en 2009 de la ISO 31000, supuso la unificación de los criterios para la realización de análisis de riesgos de los diferentes aspectos de una organización bajo una única metodología. Hasta entonces, nada tenía que ver la metodología utilizada para analizar los diferentes tipos de riesgos (financieros, medioambientales, la seguridad en la cadena de suministro o los relacionados con la seguridad de los sistemas de información, por ejemplo).

Antes de la ISO 31000

Para cada tipo de riesgo existían diferentes metodologías, más o menos complejas, muy especializadas en ese tipo de riesgo. Sin duda, se trataban de metodologías muy desarrolladas y que proporcionaban una gran cantidad de información para el análisis.

Cojamos, por ejemplo, las metodologías para el análisis de riesgos en seguridad de la información. Las había más o menos complejas y que analizaban más o menos factores, pero todas tenían en común que iban de abajo hacia arriba, partiendo de cada activo individual y teniendo en cuenta una serie de elementos para cada uno de ellos como amenazas, vulnerabilidades, impacto en diferentes aspectos de la organización, dependencias entre activos, tiempo de exposición a la amenaza, etc. que hacía el análisis muy laborioso pero muy completo. El riesgo de un proceso se calculaba acumulando los riesgos de los activos implicados en el mismo.

Sin embargo, todos los que nos dedicamos a realizar análisis de riesgos nos fuimos dando cuenta de que, a nivel práctico, tanto trabajo y detalle resultaba totalmente prescindible; ya que, si se procedía a simplificar el análisis, los resultados eran muy similares. Esto se debía a que unos pocos activos concentraban la mayor parte del riesgo.

La unificación de criterios con la aparición de la ISO 31000

La aparición de la ISO 31000:2009 supuso un gran cambio en la forma de entender el análisis de riesgos. Este estándar, orienta el análisis de riesgos al negocio en su conjunto y establece una metodología que permite unificar los criterios y comparar los diferentes riesgos. Por ello, todas las últimas versiones de los diferentes estándares parten de la estimación del riesgo y hacen referencia explícita a la ISO 31000 para la realización de esta estimación.

> *“La clave de esta nueva metodología, consiste en agrupar diferentes riesgos, que anteriormente se analizaban uno a uno, en escenarios de riesgos”.*

En este caso, el análisis se realizada desde arriba, desde la perspectiva de los objetivos de la organización. El cumplimiento de estos objetivos, definidos por los órganos de gobierno y que reflejan los intereses de las partes interesadas, puede verse en peligro por la posible materialización de una serie de riesgos.

La clave de esta nueva metodología consiste en agrupar diferentes riesgos, que anteriormente se analizaban uno a uno, en escenarios de riesgos. Por ejemplo, un escenario podría ser la no disponibilidad de la información necesaria para la operativa diaria de la organización, ¿qué más nos da que esa indisponibilidad esté motivada por fallos en el suministro eléctrico, en los servidores o en las comunicaciones?. Desde el punto de vista de negocio, lo único relevante es que no tenemos acceso a la información que necesitamos, con el correspondiente impacto en la organización. Por lo tanto, muchos riesgos que antes se analizaban por separado, ahora se agrupan y se analizan bajo un único escenario. Además, se reducen también los parámetros a analizar, pasando a solamente dos: probabilidad y consecuencia.

“El riesgo asociado al escenario será el resultado de combinar probabilidad y consecuencia”

Resumiendo, el proceso de análisis de riesgos bajo ISO 31000 sería el siguiente:

Bajo el término “probabilidad” se resume el conjunto de elementos que se analizaban en metodologías anteriores (amenaza, vulnerabilidad, frecuencia de la amenaza, etc.); y, ciertamente tenemos que tener todos estos elementos en cuenta para estimar el valor que le otorgamos a la probabilidad de que un escenario de riesgo se materialice; pero ya no necesitamos recurrir a cálculos complejos de abajo hacia arriba. Incluso, para muchos escenarios, podremos recurrir a estadísticas y datos históricos, tanto propios como externos.

Respecto a la consecuencia (antes se utilizaba la palabra “impacto”), resulta mucho más sencillo aplicarla a un escenario de riesgo que a una serie de amenazas sobre diferentes activos. De esta forma, estimaremos la consecuencia que tendría para la organización el que un escenario de riesgo se materializase. Evidentemente, existen varios tipos de consecuencias si se materializa un escenario de riesgo (operativas, económicas, reputacionales, penales, etc.); pero, de nuevo, tendremos que sintetizar todos esos impactos en un único valor de consecuencia.

Existen diferentes formas de calcular estos valores de probabilidad y consecuencia para cada uno de los escenarios, aunque lo más habitual es seleccionar el mayor de los que hayamos obtenido.

Por ejemplo, en una escala de 1 a 5, si la probabilidad de que la información no esté disponible por un fallo eléctrico es de 3 y por un fallo en las comunicaciones es de 5, el valor de probabilidad para nuestro escenario será 5; y si la consecuencia reputacional es 3 y la operativa 4, el valor de consecuencia para nuestro escenario será 4.

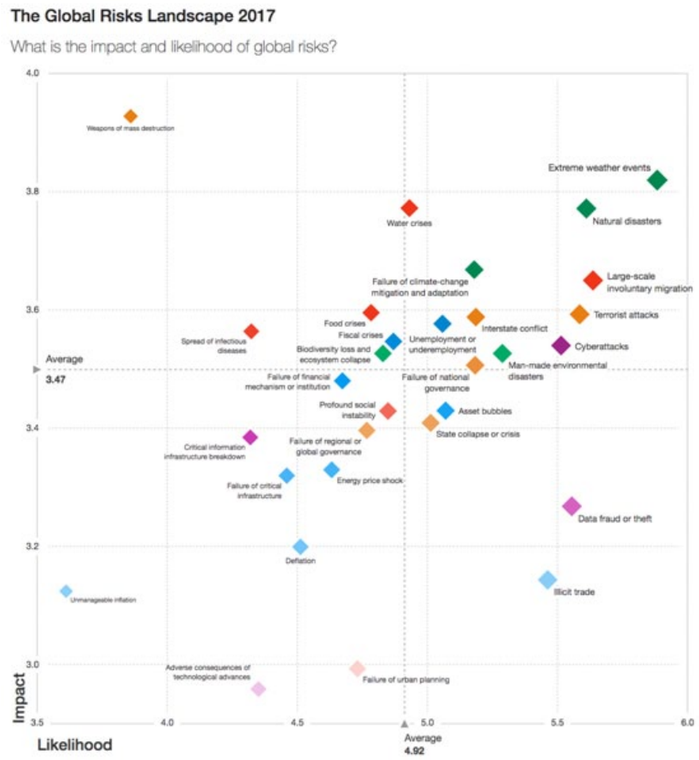
A partir de aquí, el riesgo asociado al escenario será el resultado de combinar probabilidad y consecuencia. Lo que se hace es multiplicar los valores, por lo que el riesgo del escenario analizado será 20 (de un rango entre 1 y 25).

Una vez que tengamos todos los escenarios de riesgos analizados, la dirección deberá establecer el umbral de riesgo tolerable; es decir, aquel a partir del cual será necesario tomar acciones para tratar el riesgo y reducirlo hasta un nivel aceptable. En este sentido, hay una máxima que siempre se debe cumplir, y es que las acciones que se tomen para reducir el nivel de riesgo nunca deben suponer un coste superior al que supondría la consecuencia de la materialización de dicho riesgo. O sea, que no debemos matar moscas a cañonazos; algo que muchas veces no se tiene en cuenta.

Una vez que se ha determinado qué riesgos deben ser tratados, tendremos que establecer un Plan de Tratamiento de Riesgos, estableciendo diferentes medidas que permitan reducir el nivel de riesgo. Estas medidas pueden ser de diferente tipo (organizativas, técnicas, legales) y con diferente perspectiva a la hora de tratar el riesgo (evitarlo, reducirlo, transferirlo, etc).

En el siguiente análisis de riesgos que efectuemos, todas estas medidas habrán tenido su impacto en la reducción del riesgo, y harán que el valor de probabilidad y/o consecuencia varíen (con seguridad más la probabilidad que la consecuencia). Pero como vivimos en un entorno cambiante, aparecerán nuevos riesgos o la probabilidad de que nos afecten, lo que nos llevará a un nuevo plan de tratamiento de riesgos, y así sucesivamente. Por ello, es importante contar con una herramienta que nos ayude a gestionar el análisis de riesgos, a realizar un seguimiento de la implantación del plan de tratamiento, y a comparar la evolución en el tiempo.

Utilizando esta misma metodología para diferentes escenarios relacionados con diferentes aspectos, podremos llegar a comparar los diferentes riesgos de la organización. Mostramos, a continuación, y a modo de ejemplo, la representación gráfica de los riesgos mundiales estimados para 2017 por el World Economic Forum.



Conclusiones

La ISO 31000:2009 nos ofrece las pautas para gestionar de forma adecuada los riesgos de nuestra organización desde una perspectiva de negocio; nos enseña que la responsabilidad de la gestión de riesgos debe partir de los órganos de gobierno e involucrar a toda la organización; y nos permite evaluar todo tipo de riesgos bajo una única metodología, mostrándonos una imagen global del mapa de riesgos de la organización y suministrando información importante para la toma de decisiones estratégicas.